CloudOps Frequently Asked Questions

Security

What are the standard cloud security measures implemented to protect both Cisco and its customers within the AWS cloud environment?

AWS provides network-level protections, including DDoS protection shields, that are enabled for all Cisco SD-WAN production fabrics. These protections help mitigate volumetric and application-layer attacks. Additionally, AWS security groups (whitelists) control user access to cloud resources.

What happens if someone tries to brute force the SD-WAN Manager infrastructure?

Brute force attempts from unauthorized IPs are detected by the cloud provider's security monitoring systems. Upon detection, alerts are sent to the Cisco SD-WAN CloudOps team for immediate action. This proactive monitoring helps prevent unauthorized access and protects the integrity of the SD-WAN Manager controllers.

How does Cisco view the risk of customers accessing SD-WAN Manager without Single Sign-On (SSO), and what mitigations exist?

While many customers globally access SD-WAN Manager without SSO, we have not observed security issues to date. We encourage you to adopt SSO, which is supported in all models except SD-WAN Cloud (formerly CDCS), to enhance security. For non-SSO customers, we offer a custom VPC option that places private IP interfaces of cloud-hosted controllers within your on-premises network, allowing secure access via TACACS, RADIUS, or AAA servers, bypassing public IP exposure.

What security measures does Cisco use beyond AWS security groups to protect Internet-facing SD-WAN controllers?

We employ multiple layers of security including Web Application Firewalls (WAF) and application-level DDoS protection. Data is protected both in transit and at rest. The publicly accessible SD-WAN models are safeguarded by WAF and integrated DDoS protections to prevent attacks and unauthorized access.

Is there security monitoring to detect brute force or other attacks?

Yes. Cloud providers monitor for security breaches and suspicious activities 24x7. Any detected compromises or brute force attempts trigger notifications to Cisco CloudOps, which follows incident management protocols. Our Security and Trust Organization (STO) also performs periodic vulnerability scans on production deployments, with reports published on the Cisco Trust Portal. Basic DDoS protection and WAF are enabled by default for cloud deployments and publicly accessible portals 1.

How is access controlled for Cloud and Cloud-Pro environments?

Access is restricted to authorized customers and Cisco SD-WAN support teams. Authentication and authorization span multiple components including Day Zero Servers, SD-WAN Validator, and SD-WAN Manager. Role-based access control and Access Control Lists (ACLs) are enforced both on SD-WAN Manager and in the cloud environment to ensure secure access.

How can customers request penetration testing (pen test) for Cisco SD-WAN cloud controllers?

- AWS: You can conduct your own penetration tests on Cisco SD-WAN overlay controllers hosted in AWS without prior approval, following AWS's penetration testing policy: https://aws.amazon.com/security/penetration-testing/
- Azure: Similarly, you can perform penetration testing on Azure-hosted controllers without approval, adhering to Microsoft's rules of engagement: https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement

Can CloudOps provide security certifications or audit reports?

Yes. we provide direct access to the Cisco Trust Portal, which contains security compliance documents, industry certifications (such as SOC, ISO, FedRAMP, and PCI DSS), privacy data sheets, penetration test attestations, and whitepapers. For NDA-protected content, you can register for access. For questions not covered by the Trust Portal, the Customer Information Clearinghouse (CIC) team offers vetted responses. CIC can be engaged via the CIC Request Tool on Salesforce: http://go2.cisco.com/stocic