SD-WAN Compliance

Credential management

Q **Does the Cloud Service Platform (CSP) support Single Sign On (SSO) for all human users (standard/privileged)?**

A Yes, we support SAML 2.0-based integration, including support for 2FA. RADIUS- and TACACS-based integrations are also supported.

Q **Is the solution using any certificates for authentication? Describe how they are used in the solution and certificate characteristics?**

A Yes, the solution makes extensive use of certificates in the solution. Please refer to the detailed section on certificates at http://cs.co/sdwanbook.

Q **Are there any root users in the system? If there are any local users, how are they created? Can the local users be removed?**

A There are no root users in the system. Initial admin and read-only accounts are created by Cisco. These can be removed once the service is configured by the customer.

Q **Does the CSP have any integration/service accounts? Does it list them and the credentials used?**

A No, third-party integrations in the solution. The service by Cisco for Software-Defined WAN (SD-WAN) is a standalone service. Any third-party integrations are commissioned by the customer using REST APIs.

Access provisioning

Q **Are standard users only provisioned within customer the Identity Provider (IDP)?**

A If IDP is set up, then yes. Otherwise, local user accounts can be created if not using an IDP.

Q **How are users provisioned/deprovisioned, etc.?**

A Users are controlled via the SSO. In this case, a user can be provisioned/deprovisioned at IDP. If not using an SSO, the users can be added/removed via an administrative account. The vManage service provides APIs to control all aspects of the users in the solution.

Q **How are user roles and entitlements configured within the CSP?**

A Role management is provided through the dashboard. SD-WAN user groups can be integrated via SAML to the IDP inside a customer environment. These roles are tunable to all aspects of the solution. Cisco cannot modify these since they reside within the vManage service and only the customer can control them.

Q **Describe how CSP supports administrators that can access customer data or how applications are provisioned? (This should be provisioned by customer IDP or the process should be explained.)**

A By default, when the service is initially created, Cisco creates two accounts in the service to help with onboarding customers. These accounts can be removed/modified by the customer once the service is commissioned. Cisco does not have the ability to modify anything in the service. Customers must explicitly provide administrative controls to Cisco to be able to modify the service or any aspect within.

Q **What are the roles in the Software-as-a-Service (SaaS) environment?**

A Please see the vManage Usergroup section under Administration.

Authentication and authorization

Q **How does the CSP support IP restrictions and what is the process to put IP restrictions in place?**

A All Cisco® SD-WAN services are IP restricted. Currently the only way to whitelist IP space is to open a service request, and only a license administrator from the customer can submit the request.

Q **If tenant/root administration accounts are publicly available explain whether Multifactor Authentication (MFA) is in use for these accounts and what method (OTP, SMS, etc.) is used?**

A MFA is available via integration into IDP services. No public root or tenant administrative accounts exist in the solution.

Q **How do users authenticate to lower environments/ sandbox environment? Is separation provided?**

A A sandbox environment can be created but it will be a separate VM. Each customer receives a dedicated environment that is separated at layer 3 through layer 7. Access to the environments is restricted based on SSO as well as IP restrictions.

Q **Describe any part of the CSP customer environment that has connections to other CSPs or services and describe the characteristics/relationship with the other CSP or service.**

A Services are physically hosted in Amazon Web Services (AWS) and Azure. No other integrations exist. The Cisco SD-WAN service only uses the AWS/Azure environment to provide virtualization for the actual Cisco service.

Q **How do systems or services authenticate to the CSP environment?**

A All systems accessing the customer's SD-WAN environment must authenticate against the system. This authentication is again able to use an SSO via an IDP or be provided a local user account with a token that it must use to access the service.

Application security

Q **Has the SaaS gone through any third-party security testing? When did the last third-party testing occur? Please provide testing results and proof of remediation if testing has findings (artifact is listed in requested doc).**

A On roadmap.

Q **How and when does the CSP perform internal application security testing or code review and at what frequency?**

A Pen Test is done against SD-WAN before every release. Detail can be found at https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html.

Q **Is SDLC (Secure Software) Software Development Lifecycle (SDLC) followed for the CSP environment?**

A Yes.

Q **What options are there for customer to test the app security environment using on-premises tools and what is the process to enable this testing?**

A A customer can scan against their own environment. They must however notify Cisco and schedule a window to allow for security assessment scans against their own cloud service. They may not scan, audit, or investigate Cisco at an organizational level. This is to ensure the security checks in place against scans are lifted against the customer environment alone.

Q **List any certifications the SaaS solution has achieved.**

A The certification to achieve FedRAMP Moderate is on the roadmap.

Infrastructure security

Q **Where is the SaaS hosted? Is it primary to the CSP or third party?**

A AWS and Azure.

Q **List all certifications for the CSP environment.**

A Refer to AWS and Azure certification.

Q **Is the environment multitenant?**

A By default no. Multitenancy as an option is available.

Q **Describe segregation of data in the multitenant environment (multiple applications/customers in the same cloud).**

A All data is segregated from layer 3 through layer 7. This means each customer has their own private networking and dedicated firewalls and IP addressing that is not shared with anyone. Similarly all data storage is stored in a distinct storage space and uniquely encrypted at rest. Each customer can host a multitenant system, where the data is segregated at the tenant level.

Q **Describe segregation of data between lower environments and production.**

A Same rules as above.

Q **Does the SaaS have any on-premises or system-level agents that will be deployed on-premises or in other customer cloud environments?**

A No. NA (Not Applicable).

Q **Provide a diagram and description of the CSP system environment.**

A NA (Not Applicable).

Q **Please provide any independent assessments of the Infrastructure controls that have been completed, including the results and if this is an ongoing activity.**

A The independent assessment for the solution is in progress for the FedRAMP certification.

Q **What is the operating availability tier of the CSP/hosting environment?**

A The SaaS provides a 4 nines level of availability to the SD-WAN control plane infrastructure.

Data security

Q **What is the data type? Public, confidential–internal distribution, confidential–restricted, confidential–high restricted including Network Provider Identifier (NPI), Peripheral Component Interconnect (PCI)? Note: If the data type changes during or AFTER the review, the CSP will be required to go through a new suitability evaluation and third-party risk analysis.**

A Confidential–internal distribution.

Q **Describe the encryption in transit between customer and the CSP.**

A Transport Layer Security (TLS) 1.2 using AES-256.

Q **Describe how encryption at rest is supported. What is the method for objects such as files? File Manager (FM) required for all NPI/and protected data types).**

A AES-256 is the encryption algorithm used to encrypt at rest for all data stored in the service.

Q **Describe how data in the CSP environment is protected between application components?**

A The application components connect only through an internal API layer. This API layer is not accessible externally. The only access is through the vManage webpage.

Q **Describe your encryption management including a key management solution to the customer.**

A Simplified encryption management is in fact one of the major aspects of the solution. It provides a more efficient and secure propagation mechanism for key exchanges to allow for TLS and IPSec establishment.

Q **How are encryption keys stored and managed? (Ensure that key material does not persist remotely in storage.)**

A Encryption keys are not stored on disk. All encryption keys are locally generated on the components and stored in inaccessible parts of memory in a protected keystore.

Q **If the CSP is managing encryption keys, how often are they rotated and who has access to them? Please provide a Standard Operating Procedure (SOP).**

A Encryption keys are managed via the solution itself. Customers have access to the vManage dashboard controller, where they can control the certificates and the timers associated with the environment. The keys themselves are inaccessible. Only the customers have access to the vManage dashboard in an administrative capacity, unless they explicitly permit Cisco or a third party to access it. The keys themselves have fast rekey enabled by default, with a default 24-hour rekey.

Q **Describe database and disk-level encryption used.**

A Databases used are ElasticSearch and Neo4j. Encryption used is AES-256.

Q **Describe how backups are encrypted?**

A The backup snapshots are stored in the cloud as compressed and encrypted (using AES-256) files.

Security monitoring

Q **Please provide the CSP's incident response plan, or process for addressing incidents, where unauthorized access (or attempted unauthorized access) to customer data may have occurred, including prompt and reasonable reporting, escalation procedures, etc.**

A Alerts are generated and sent whenever an incident is detected.

Q **Who is the customer Point of Contact (POC) from the CSP in case of a security event?**

A Product Security Incident Response Team (PSIRT)—Details can be found at www.cisco.com/c/en/us/about/trust-center.html.

Q **Provide a copy of any incident handling procedures or guides.**

A Details regarding procedure to handle incidents can be found at www.cisco.com/c/en/us/about/trust-center.html.

Q **Describe the security and operational monitoring that is provided.**

A Monitoring dashboard is available on the vManage.

Q **Provide information on what security logs are captured, what events are logged, and how long they are stored in the CSP environment?**

A All security, events, and audit logs are stored on vManage for seven days.

Q **How does a customer obtain these logs and what format are they available in?**

A A customer can access these logs either using vManage dashboard, or accessing the control plane. Also, a customer can configure a log server to receive these logs from vManage.

Q **How long are logs stored in the CSP environment and how are they protected?**

A The logs are stored for seven days in the vManage. These logs are accessible only to the users that can log in to the vManage. They are not available outside of the CSP. The customer can however choose to ship the logs to an external server for auditing.

Q **Describe any SIEM integration that is possible with the CSP.**

A Yes, available via APIs and syslog export.

Operations security

Q **Describe how customer data is backed up—disaster recovery (describe method and RPO)—or if the CSP is a high-availability state that (reference any documented plans you have and provide them to us)?**

A Disaster recovery is done using periodic snapshot.

Q **How do you inform customers when maintenance is performed or a new release is published?**

A Code releases of new software versions are sent via Cisco's release process. This includes email notifications and Cisco website notifications.

Q **How is security included in release management?**

A All Cisco SD-WAN software upgrades natively also have security components, and the release notes include all aspects that relate to security services as well.

Q **How does CSP personnel perform remote administration of the CSP environment (to perform operations support)?**

A Remote users that are employees of Cisco cannot access the CSP environment without using VPN with Duo Multifactor authentication to access the Cisco network. From the Cisco network, only authorized Cisco users with the appropriate privileges may access the Cisco cloud infrastructure in AWS and Azure—again requiring 2FA authentication.

Project-level questions

Q **What is the data type? Public, confidential-internal distribution, confidential-restricted, confidential-high restricted (including NPI), PCI? Note: If the data type changes during or AFTER the review, the CSP will be required to go through a new suitability evaluation and third-party risk analysis.**

A Confidential-internal distribution.

Q **How can we back up our data outside of the CSP (in a format the customer can use if we terminate a contract) to avoid vendor lock-in?**

A All raw configurations, events, and logs can be extracted via API, as well as other standard formats like XML, JSON, NETCONF YANG, SYSLOG, and NETFLOW IPFIX to ensure openness.

Additional questions-compliance baseline for-potential reciprocity

Q **When has the vendor conducted a security self-assessment (process to validate security controls for the cloud infrastructure and application against a specific industry standard such as CSA CCM, FedRAMP, nist)?**

A FedRAMP.

Q **Please provide any third-party security assessment (process to validate security controls for the infrastructure and application against a specific industry standard such as CSA CCM, FedRAMP, nist).**

A FedRAMP.

Q **Describe how the vendor routinely publishes changes (in how controls are implemented) that are relevant to the security controls provided in the IaaS, PaaS, or SaaS in a manner that allows the subscriber to include evaluate the controls for implementation - self assessment-continuous monitoring?**

A Code releases of new software versions are sent via Cisco's release process. This includes email notifications and Cisco website notifications.

Q **Does the cloud service provider utilize any other cloud service providers in order to deliver the contracted services?**

A No.

C67-742712-00 08/19