Cisco SD-WAN NCSC Cloud Security Principles Assertions

Purpose

A wide variety of customers across a large base of the UK Government are guided by numerous frameworks and principles documents. One specific framework authored by the National Cyber Security Centre (NCSC) gives the readers 14 Principles to consider when assessing cloud based services. The aim of the 14 Principles is to provide customers with a framework against which they can assess the security capabilities of a cloud service in order to build assurance that it is in alignment with their data handling needs.

The principles are not intended to indicate a right or wrong approach and are instead focussed on a specific set of outcomes. Each organisation assessing the NCSC Cloud principles will have different security needs and therefore the importance of each principle will vary accordingly.

This document aims to provide the reader an assertion against each of the 14 Principles in the context of the cloud hosted elements of the Cisco SD-WAN solution.

Audience

Oriented towards readers who are looking to assess the Cisco SD-WAN cloud hosted solution and wish to understand the service and security provisions. It is expected that readers have an understanding of the overall Cisco SD-WAN architecture and its components. A brief overview is included to aid this understanding.

Scope

The document aims to provide sufficient information relating to the cloud hosted elements of the Cisco SD-WAN solution. Cisco utilise 3rd party cloud providers to host the SD-WAN solution. Customers can choose to have their service hosted on either Amazon AWS or Microsoft Azure. In some areas, the security capabilities of the chosen cloud provider are utilised and therefore some Principles are addressed by the native hosting environment. In these instances the reader will be referred to the respective 3rd party security materials.

More Information

The table within this document outlines how a Cisco hosted SD-WAN orchestration environment aligns to the NCSC Cloud Security Principles. As noted above, since Cisco utilises either Amazon Web Services or Microsoft Azure, a number of the principles are addressed via the inherent capabilities of the chosen provider. Both Amazon and Microsoft have published extensive responses to the NCSC Cloud Security Principles and these documents are available at:

Amazon Web Services – https://d1.awsstatic.com/whitepapers/compliance/AWS_CESG_UK_Cloud_Security_Principles.pdf

Microsoft Azure – https://gallery.technet.microsoft.com/14-Cloud-Security-Controls-670292c1

Within the evidence column of the table, there are references to the CAIQ Cloud Control Matrix. This document provides additional evidence against the various principles and is available upon request but requires an NDA to be in place.

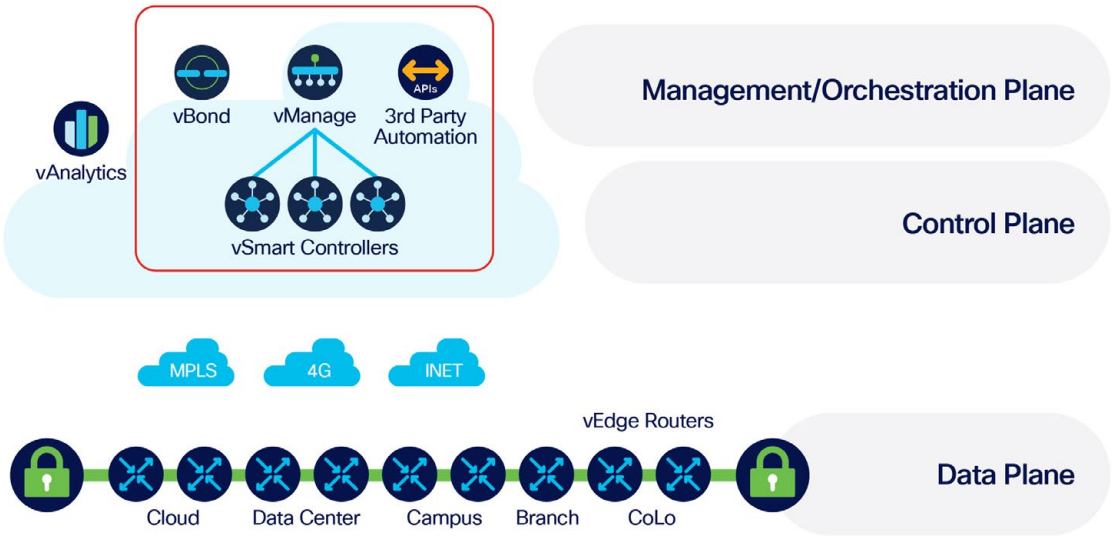
Cisco SD-WAN | Overview

Whilst a full description of the Cisco SD-WAN solution is beyond the scope of this paper, it is important to highlight that the Cisco SD-WAN solution is comprised of a number of components described below.

- **vBond** – The vBond controller or the policy controller determines if the edge device is part of the network. It helps onboard the device. The Zero touch provisioning process provides the address of the vBond to the edge device on boot up and in turn the vBond on-boards the device to the vManage.
- **vSmart** – The vSmart device is the control plane controller, that provides the best path to take for a device from branch to branch and branch to cloud. It provides the smartness to switch between paths depending on the configured application level latency requirements. The vSmart in the cloud is configured as an active active geo located cluster.
- **Edge** – The Edge routers sit at the perimeter of a site (such as remote offices, branches, campuses, data centres) and provide connectivity among the sites. They are either hardware devices or software, called a vEdge Cloud/CSR1000v router, that runs as a virtual machine. Edge routers handle the transmission of data traffic.
- **vManage** – The vManage or the NMS service provides the interface to onboard all devices. It also provides workflows to configure the RBAC for network administrators and for configuring the network topology. While the vSmart and vBond are stateless devices the vManage is stateful.
- **vAnalytics** (Optional) – vAnalytics platform is a SaaS service hosted by Cisco as part of the SD-WAN solution. vAnalytics platform provides graphical representations of the performance of the entire overlay network over time enabling drill down to the characteristics of a single carrier, tunnel, or application at a particular time.

All SDWAN edge devices and controllers are FIPS 140-2 compliant. All ISR and ASR edge devices are DOD APL STIG and Common Criteria Certified.

The figure below illustrates how each of these components are deployed. It is important to note that many of the components are software-only, i.e. are deployed as a virtual machine. In addition, whilst the vEdge remains a physical router, there is also the option to deploy a virtual instance of this platform into the cloud or on to models of the Cisco ENCS, ASR 1000, ISR 4000 and ISR 1000 series router platforms.



The Cloud instances that are in-scope for the remainder of this document are encompassed above in red.

Cisco SD-WAN | Cloud Operations

Cisco provide cloud hosted controllers for SD-WAN customers. These controllers will be automatically instantiated as part of the ordering process. The instantiation and maintenance of the controllers are the responsibility of the Cisco SD-WAN CloudOps team.

- Bring up a complete controller set with options for building redundant controllers in a single or across multiple AWS VPCs (preferred and standard) or Azure VNETs
- Orchestration process includes certificate signing / installation process with DigiCert certificates, Cisco certificates or customer enterprise certificates.
- Control channels brought up automatically when controllers are functional.
- Any number of controllers across any number of VPCs and Availability Zones can be created (technically, rights reserved depending upon fabric size). Controllers can be added at any time into an existing setup, horizontally scalable without interruption. The solution 'spin-up' is orchestrated by Internal Cisco tools, to ensure a consistent deterministic instantiation of cloud controllers is provided.

Advantages of Cloud Provision include:

Currently Cisco cloud deployments are "In Process" of FedRamp moderate, a US Federal government security evaluation process to incorporate CISCO SDWAN into the Federal network.

- Cisco hosts controllers for the customer in the cloud, providing space, hardware, CPU, memory, cabling and connectivity, cooling, geographic redundancy in different availability zones for fault tolerance.
- Cisco is responsible for server health, monitoring and uptime.

- Cisco will provide assistance for software upgrades.
- Cisco TAC can have limited read visibility to controllers for monitoring and troubleshooting purposes.
- Control plane will never see any customer data that traverses the data plane.
- Control plane only has control information and network statistics.
- Connectivity to the controllers from the edge routers are PKI authenticated and secured with AES-256 bit encryption (DTLS).
- Admin connectivity to the controllers are secured with security group whitelisting for only the customer's IP address space and limited Cisco IP addresses. This incorporates (https/ssh or SD-WAN GW) and is at the customer's discretion.

Summary

For more information of the roles and responsibilities of Cisco SD-WAN CloudOps, please refer to the following link

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/knowledge-base/cloudops.html#id_119894

For more information in regard to the Cloud Provision - Service Description, please refer to the following link

https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/cisco_sd_wan_offer_description.pdf

Cisco SD-WAN | Cloud Perimeter Security

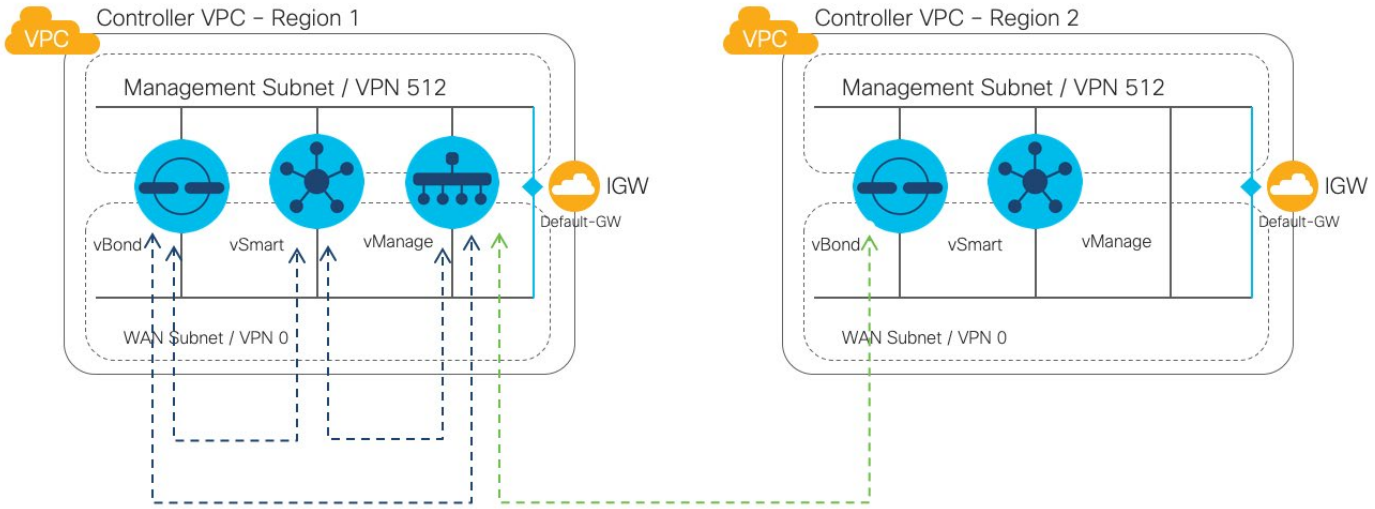
The following security boundaries are not directly applicable to the cloud principles, but do help readers comprehend the wider solution.

At a generic high level, the perimeter security of the Cloud Controllers can be categorised into two sections.

Cloud Inherent

The CISCO cloud VPC or vNet are only open to white listed IPs as specified by the customer, these rules help to prevent of DDOS attacks and Man in the middle attack vectors from IPs outside the range specified.

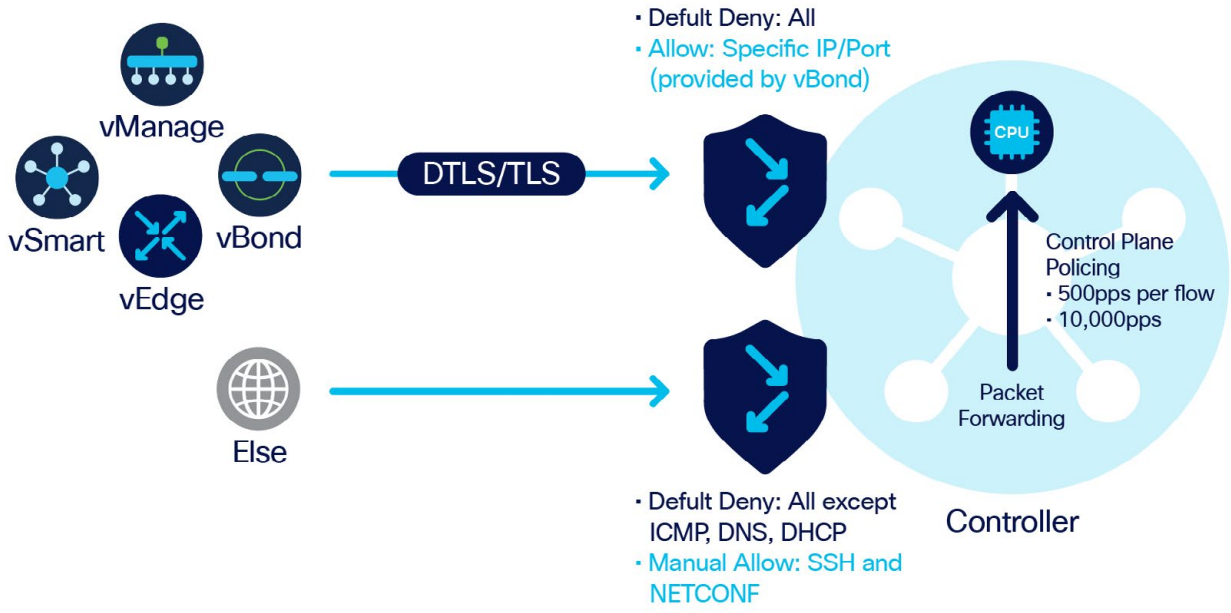
The automated process mentioned also includes the leveraging of inherent security features provided by the Cloud provider (AWS/Azure). Whitelists limit administrative connectivity (HTTPS) to certain IP address ranges and all other connectivity is limited to permit only the protocols required to establish the control-plane elements.



Controller Inherent

The Controllers also have their own protection mechanisms to mitigate certain vectors of threat. The components that comprise the SD-WAN solution have a default automated mechanism to dis-allow traffic that isn't specifically originating from another SD-WAN element. Due to the vBond orchestrator and on-boarding mechanisms of the devices, the fabric distributes only permitted IP/Protocol combinations to all SD-WAN components.

Cisco SD-WAN Cloud Controller Information



Cisco SD-WAN | NCSC Principles

NCSC PRINCIPLE	DESCRIPTION	CISCO RESPONSE	EVIDENCE SOURCE
1. Data in transit protection	User data transiting networks should be adequately protected against tampering and eavesdropping.	All connectivity into and between Cloud instances can be categorised into two parts **User Interaction (Management Plane):** User connections to the SD-WAN Cloud solution are protected using TLS v1.2. Web service authentication is performed using self-signed certificates by default. Certificates can be replaced by the customers' own certificate for authentication of the web service (workflow provided). The offered suites by the webserver can be found using the Evidence source link **Component Interaction (Control Plane): Connectivity from SD-WAN device** to and between cloud instances are encrypted and mutually authenticated with (D)TLS v1.2 using AES-256. Again, customers can deploy their own Enterprise Certificates should they wish. The most recent versions of Cisco SD-WAN software will utilise the following cipher suite for the control plane. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 Finally for more information around NCSC's TLS guidance, see the following link https://www.ncsc.gov.uk/guidance/tls-external-facing-services	- **SD-WAN Compliance** - **SD-WAN Web Server Ciphers** - **CCM v3.01 – EKM-03** - **FedRAMP**

NCSC PRINCIPLE	DESCRIPTION	CISCO RESPONSE	EVIDENCE SOURCE
2. Asset protection and resilience	User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.	**Location:** All cloud data locations are requested at initial provisioning time as part of the ordering process. Customers can stipulate the locations of all controllers (within the boundaries of enabled zones – a full list can be provided) and also where backup (snapshots) are stored. Outside of these agreed locations, data will not be moved unless consulted and agreed or mandated by law. In all cases, customers will be notified of a transfer. **Data at Rest:** All data at rest is encrypted. Cisco leverage the cloud providers' capabilities to enable this; Encrypted Files Systems (EFS). More on AWS EFS, here. **Data Sanitisation:** Cisco relies upon the data sanitisation procedures offered by the underlying cloud provider. These are outlined in the guidance linked above for AWS and Microsoft Azure. **Resilience:** The control plane capability is highly resilient at an application level (see SD-WAN Book reference for more detail). Resilience can be further enhanced by locating controllers in diverse Cloud environments. **Availability:** During each Measurement Period, the Availability Percentage will be 99.99% or greater, for both control and management plane. Please See Service Description for more detail.	- **SD-WAN Compliance** - **SD-WAN Book** - **AWS CAIQ DSI-07.1/2** - **CCM v3.01 - DCS-04** - **CCM v3.01 – EKM-03.1**

NCSC PRINCIPLE	DESCRIPTION	CISCO RESPONSE	EVIDENCE SOURCE
3. Separation between Users	A malicious or compromised user of the service should not be able to affect the service or data of another.	**Tenant Separation:** 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. Separation is supported by the mechanisms inherent to the customer's chosen cloud provider, namely AWS Virtual Private Cloud (VPC) and Azure VNET. **Penetration-Test:** As part of Fedramp Cicso SDWAn does penetration tests multiplet times a day. The Ciso SDWAN also includes a FIM codebase built in that detects any anomaly within the customers controllers deployed. Penetration testing is performed against SD-WAN releases at regular intervals, more information here. Customers can perform their own penetration tests, under agreement from Cisco.	- **SD-WAN Compliance**

NCSC PRINCIPLE	DESCRIPTION	CISCO RESPONSE	EVIDENCE SOURCE
4. Governance framework	The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.	Cisco has a mature and effective governance framework that ensures procedural, personnel, physical and technical controls are well defined and executed across the organisation. In addition to complying with our stringent internal standards, Cisco continues to pursue numerous external third-party validations to demonstrate our commitment to information security. Cisco Services has received certification for ISO27001 Cisco is in the process of undertaking such certification activity for the hosting of the SD-WAN management and orchestration components. This effort will initial be focussed on FedRAMP with SOC2 and PCI-DSS as committed follow-on targets. Cisco is currently estimating completion of FedRAMP certification by late 2020 Cisco SD-WAN has a Chief Security Officer / Global ISSO that acts as the “Security Assurance Manager”. That role is independent from the delivery team who are responsible for delivery of SD-WAN services. The Chief Security Officer reports, on a monthly basis, to senior management regarding the risk-posture of the product. Finally, the underlying cloud providers’ security and compliance certifications should also be considered as part of the wider scope of the service.	- **SD-WAN Compliance** - **AWS Compliance** - **Azure Compliance**

NCSC PRINCIPLE	DESCRIPTION	CISCO RESPONSE	EVIDENCE SOURCE
5. Operational security	The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.	With regards to the four main points that underpin this principle, the below provides a summary of the approach taken. **Configuration and change management** Cisco implements a number of processes and controls for change management purposes, which follow robust practices. It should be noted that consumers have full control of the configuration and of their SD-WAN solution and so change control over these aspects of the service are within their control. **Vulnerability management** The Product Security Incident Response Team (PSIRT) governs potential new threats, vulnerabilities and exploitation techniques which could affect any Cisco product or service including SD-WAN. Policy link provided. **Protective monitoring** Cisco use a multitude of internal and external tools to ensure the continual operation, integrity and security of the solution. Additionally, the customer has a number of monitoring touchpoints to enable them to monitor the solution. All security, events, and audit logs are stored on vManage and can be exported to a customer's own event management system. **Incident monitoring** The CSIRT Incident Response Playbook defines the criteria that is used to extract security events of interest from the data that is collected and generally define the processes. Details regarding procedure to handle incidents can be found at https://www.cisco.com/c/en/us/about/trust-center.html.	- **SD-WAN Compliance** - **Vulnerability Policy** - **Trust Centre** - **CCM v3.01 CCC 01-04**

NCSC PRINCIPLE	DESCRIPTION	CISCO RESPONSE	EVIDENCE SOURCE
6. Personnel security	Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.	Pre-employment background checks are conducted on all employees. Cisco uses a third-party agency to conduct background checks to verify the accuracy of the information provided by the applicant during the selection process. Typical checks will include criminal history, prohibited parties, verification of education and previous employment history checks. Cisco complies with all applicable local laws within the countries it operates in. It should also be noted that access by Cisco staff to the orchestration elements can be removed such that the only access available for Cisco staff is to the underlying hosting environment. If access is granted to Cisco staff, the level of access granted is under the complete control of the customer.	- **CCM v3.01 CCC 02.1**
7. Secure development	Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.	Cisco maintain an extensive and comprehensive secure development lifecycle (SDL) which is compliant with ISO 27034. CSDL has been audited by BSIMM (2017). The Cisco SDL (CSDL) covers all aspects of product development from product design through development, in life management and end-of-life activities. CSDL also includes critical gates that product teams must pass before products are allowed to be released. CSDL includes an automated testing framework ensures that critical security baselines requirements are met prior to product shipment.	- **Cisco CSDL** - **CCM v3.01 AIS 01.1**

NCSC PRINCIPLE	DESCRIPTION	CISCO RESPONSE	EVIDENCE SOURCE
8. Supply chain security	The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.	Cisco recognizes the important role of supply chain security in a comprehensive Cisco cybersecurity strategy. Under that strategy, Cisco deploys and maintains a capability that continually assesses, monitors, and improves the security of the Cisco supply chain. For providers of cloud services, Cisco puts in place multiple mechanism to ensure security controls are maintained including: • Master Data Protection Agreement – This agreement is put in place between Cisco and its suppliers and contains a wide range of security related obligations. • Cloud Approval to Operate (CATO) – CATO is an internal process which all Cisco cloud services must follow. The process validates that Cisco's cloud-based service offers meet a minimum set of requirements prior to being offered to customers. In the context of delivering cloud hosting for the management and orchestration components of the SD-WAN solution, Cisco has chosen to partner with two highly respected organizations, each of whom hold extensive evidence of their respective commitments to security. Both Microsoft and Amazon hold ISO 27001 certificates for their cloud platforms and have published their own responses demonstrating how the NCSC Cloud Security Principles are being met. In regards to customer information (inclusive of Supply chain), all data is subject to the Privacy Data Sheet for SD-WAN. Of particular relevance to this principle is section 7, 'Third Party Service Providers (Sub-processors)'.	- **Cisco Supply Chain Security** - **Cisco SD-WAN Privacy Data Sheet**

9. Secure user management	Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data.	User management within the orchestration and management functions is entirely within the control of the customer. User(s) and their associated roles are defined in the vManage dashboard and customer administrators can assign read-only and read-write privileges on a wide range of configuration options. SD-WAN user groups can be integrated via SAML to an identity provider inside a customer environment, or via RADIUS/TACACS. As described in principle 1, management interfaces to the vManage appliance are protected using TLS v1.2. All requests for support of the SD-WAN cloud service utilise Cisco's standard procedures and are delivered via the Cisco Technical Access Assistance (TAC). Customers access Cisco TAC via the Cisco website, e-mail and telephone. To access Cisco TAC services, customers must have a Cisco.com user ID which is linked to a valid support contract. The support contract must include the serial number of the device for which support is required. Cisco TAC do not have direct administrative access to the cloud hosted SD-WAN components. Customer must grant explicit access (which can be limited to read-only if required) to Cisco TAC as and when required.	- **SD-WAN Compliance** - **CCM v3.01 IAM 12**
10. Identity and authentication	All access to service interfaces should be constrained to authenticated and authorised individuals.	All interfaces presented to customers require authentication prior to granting access. Customers have full control over who has access and the roles they are assigned to. Authentication can be performed 'on-box' via the local database or be linked to existing identity databases via SAML or RADIUS/TACACS. Two-Factor authentication mechanisms are also available for increased security. Examples of how to configure the RADIUS protocol and SAML are provided in the evidence source.	- **SD-WAN Compliance** - **RADIUS configuration** - **SAML Configuration using 3rd Party Provider** - **CCM v3.01 IAM 12**

11. External Interface Protection	All external or less trusted interfaces of the service should be identified and appropriately defended.	All Internet accessible interfaces are protected in two ways. Firstly, access is restricted using the cloud native access-control functions which ensures only those services required are exposed. In addition, the hosted components themselves also implement their own, more stringent access-control limiting both the service exposed and the source IP address from which connections can be made from. These IP addresses are captured from the SD-WAN fabric configuration and applied automatically to the inbound interfaces of the management and orchestration components.	- **Cisco SD-WAN | Cloud Perimeter Security section**
12. Secure Service Administration	Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.	The hosted systems are under the full administrative control of the customer. Cisco access to the vManage, vBond and vSmart components is not necessary for service operation. Cisco personnel will have access and will administer the underlying cloud environment (either AWS or Azure). Access to this underlying platform if only available to authorised personnel from the SD-WAN CloudOps team and is only available from within the Cisco network. Authorised administrators are required to utilize fully-managed Cisco assets for administration which will include standard security controls such as end-point anti-malware, data-at-rest encryption. Two-factor authentication is required for authorised users to access the cloud provider administration interface. Cisco enforces the rule of least privilege through access restriction based on roles and job functions. Cisco has an account administration application that provides a central access point to request and perform administrative functions for account requests across multiple platforms. This includes accounts for applications, hosts, databases, and responsibilities. In addition, Cisco conducts ongoing security awareness campaigns and training that details need-to-know guidelines in association with the Cisco Data Protection Policy. The most applicable NCSC designation for the system administration architecture would be “Direct Service Administration”	- **NCSC Admin Arch**

13. Audit information of Users	You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.	The proposed solution provides a native auditing capability. All security and system events and audit logs are stored on the vManage for seven days. From mid-2020, audit information from vManage will be exportable via syslog, to facilitate customers in their respective monitoring regimes. Currently the log can be exported via the GUI in a CSV format. The Audit log records many actions ranging from successful/failed authentication attempts to certificate install events and configuration changes (template/policies). The API is available on any installed instance for more information.	- **SD-WAN Compliance** - **SD-WAN Audit log Documentation**
14. Secure use of the Service	The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.	Secure use of the Cisco cloud hosted orchestration and management service is dependent on a number of factors: Security of the management environment/ system used to access the hosted components. If the integrity of the customer management system is compromised, then an attacker may be able to steal administrative credentials which could then be used to maliciously modify the SD-WAN configuration. This threat is partially mitigated through being able to whitelist the source IP addresses from which management sessions can be established however there is a clear responsibility on the customer to maintain the security of the device from which they administer the service.	- **Cloud Ops White List Process**