Example Configuration for Cisco Catalyst SD-WAN Remote Access, RADIUS, and AnyConnect

Example Configuration for SD-WAN Remote Access, RADIUS, and AnyConnect

This example describes the configuration of the following:

- SD-WAN RA headend device
- RADIUS server
- AnyConnect remote access client

The following remote access connection details apply to the example:

- Remote access client type: Cisco AnyConnect
- Remote access client authentication type: AnyConnect-EAP user authentication
- CA server with SCEP-based certificate enrollment
- RADIUS server configured with following profiles and attributes:
  - User profile name: user1@example.com
  - User password: user1-passwd
  - Group profile name: example.com
  - Group profile attributes: VRF, ip unnumbered interface, IP pool name, server subnets

Before You Begin

- In Cisco SD-WAN Manager, configure the following using a feature template:

    - VRF for the SD-WAN RA service VPN
    - Public IP on the TLOC interface used for SD-WAN RA

- Ensure that the RADIUS server and CA server are reachable in the SD-WAN RA service VPN.

SD-WAN RA Headend Device Configuration

This example provides a generic template for configuring a Cisco IOS XE Catalyst SD-WAN device to function as an SD-WAN RA headend. The template uses variables that prompt you for details specific to your network, at runtime when you apply the template.

The following table describes the variables used in the template.

Table 1: CLI Template Variables

Variable	Description
SDRA_POOL_START_IP	First IP address of the private IP pool configured on the SD-WAN RA headend
SDRA_POOL_END_IP	Last IP address of the private IP pool configured on the SD-WAN RA headend
SDRA_UNNUM_INTF_IP	Private IP address to use on the SD-WAN RA unnumbered interface, preferably in the same subnet as private IP pool. The SD-WAN RA headend uses this interface as the source IP for communication with the RADIUS server. Configure this interface IP address as the SD-WAN RA headend IP on the RADIUS server.
SDRA_SERVICE_VPN	Service VPN in which the CA and RADIUS servers must be reachable. By default, the SD-WAN RA headend places a remote access user into this service VPN unless the RADIUS-based user and group policy specifies a different service VPN.
SDRA_RADIUS_IP	IP address of the RADIUS server reachable in the SDRA_SERVICE_VPN
SDRA_RADIUS_ENCR_KEY	Encryption key to use with the RADIUS server. This key must match the key configured on the RADIUS server.
SDRA_RADIUS_SOURCE_INTF	The interface in the SDRA_SERVICE_VPN to be used as source interface for RADIUS communication. The IP address configured on the SDRA_RADIUS_SOURCE_INTF must be configured on the RADIUS server for authorization.
SDRA_AUTHOR_RADIUS_PASSWD	The password used with the group authorization request to the RADIUS server. The group authorization name and password must match the group profile name and password configured on the RADIUS server.

Variable	Description
SDRA_CA_SERVER_IP	IP address of the CA server reachable in the SDRA_SERVICE_VPN
SDRA_CA_CERT_FINGERPRINT	Fingerprint of the CA certificate
SDRA_HEADEND_SUBJECT_NAME	Subject name to use in the SD-WAN RA headend certificate

Use the following in a CLI add-on template:

```
ip local pool SDRA_IP_POOL {{SDRA_POOL_START_IP}} {{SDRA_POOL_END_IP}}
!
aaa new-model
!
aaa group server radius SDRA_RADIUS_SERVER
server-private {{SDRA_RADIUS_IP}} key {{SDRA_RADIUS_ENCR_KEY}}
ip radius source-interface {{SDRA_RADIUS_SOURCE_INTF}}
ip vrf forwarding {{SDRA_SERVICE_VPN}}
!
no ip http secure-server
!
aaa authentication login SDRA_AUTHEN_MLIST group SDRA_RADIUS_SERVER
aaa authorization network SDRA_AUTHOR_MLIST group SDRA_RADIUS_SERVER
aaa accounting network SDRA_ACC_MLIST start-stop group SDRA_RADIUS_SERVER
!
crypto pki trustpoint SDRA_TRUSTPOINT
enrollment url http://{{SDRA_CA_SERVER_IP}}:80
fingerprint {{SDRA_CA_CERT_FINGERPRINT}}
revocation-check none
rsakeypair SDRA_TRUSTPOINT 2048
subject-name cn={{SDRA_HEADEND_SUBJECT_NAME}}
auto-enroll 80
auto-trigger
vrf {{SDRA_SERVICE_VPN}}
!
crypto ikev2 proposal SDRA_IKEV2_PROPOSAL
encryption aes-cbc-256
integrity sha256
group 19
!
crypto ikev2 policy SDRA_IKEV2_POLICY
proposal IKEV2_PROPOSAL
!
crypto ikev2 profile SDRA_IKEV2_PROFILE
match identity remote any
authentication local rsa-sig
authentication remote anyconnect-eap aggregate
pki trustpoint SDRA_TRUSTPOINT
aaa authentication anyconnect-eap SDRA_AUTHEN_MLIST
aaa authorization user anyconnect-eap cached
aaa authorization group anyconnect-eap list SDRA_AUTHOR_MLIST name-mangler
SDRA_NAME_MANGLER_DOMAIN password {{SDRA_AUTHOR_RADIUS_PASSWD}}
aaa accounting anyconnect-eap SDRA_ACC_MLIST
virtual-template 101 mode auto
reconnect
!
crypto ikev2 name-mangler SDRA_NAME_MANGLER_DOMAIN
eap suffix delimiter @
!
crypto ipsec transform-set SDRA_IPSEC_TS esp-gcm 256
mode tunnel
!
crypto ipsec profile SDRA_IPSEC_PROFILE
```

```
set ikev2-profile SDRA_IKEV2_PROFILE
set transform-set SDRA_IPSEC_TS
!
interface Loopback 65515
no shutdown
vrf forwarding {{SDRA_SERVICE_VPN}}
ip address {{SDRA_UNNUM_INTF_IP}} 192.168.0.1
!
interface Virtual-Template101 type tunnel
no shutdown
vrf forwarding {{SDRA_SERVICE_VPN}}
tunnel mode ipsec ipv4
tunnel protection ipsec profile SDRA_IPSEC_PROFILE
exit
!
```

RADIUS Server Configuration

The following is an example user profile:

```
user1@example.com  Cleartext-password := "user1-passwd"
 Service-Type = NAS-Prompt-User,
```

The following is an example group profile:

```
example.com   Cleartext-password := "group-passwd"
 Service-Type = NAS-Prompt-User,
 cisco-avpair+="ip:interface-config=vrf forwarding 20",
 cisco-avpair+="ip:interface-config=ip unnumbered Loopback 65515",
 cisco-avpair+="ipsec:addr-pool=IP_LOCAL_POOL",
 cisco-avpair+="ipsec:route-set=prefix 192.168.1.0/24",
 cisco-avpair+="ipsec:route-set=prefix 192.168.2.0/24"
```

AnyConnect Remote Access Client Configuration

The AnyConnect client connects to an SD-WAN RA headend similarly to how it connects to any other remote access headend. However, AnyConnect uses SSL by default, and SSL is not supported by SD-WAN RA, so it is necessary to change the mode to IKEv2/IPsec.

In this brief example, the AnyConnect client does not download the profile from the SD-WAN RA headend, but instead uses a locally defined profile.

Note the following points of AnyConnect configuration for this scenario:

- Disable AnyConnect profile download.

  In the AnyConnect local policy file, configure the **BypassDownloader** variable to **TRUE**.

- Specify IKEv2/IPsec mode

  ```
  PrimaryProtocol: IPsec
  ```