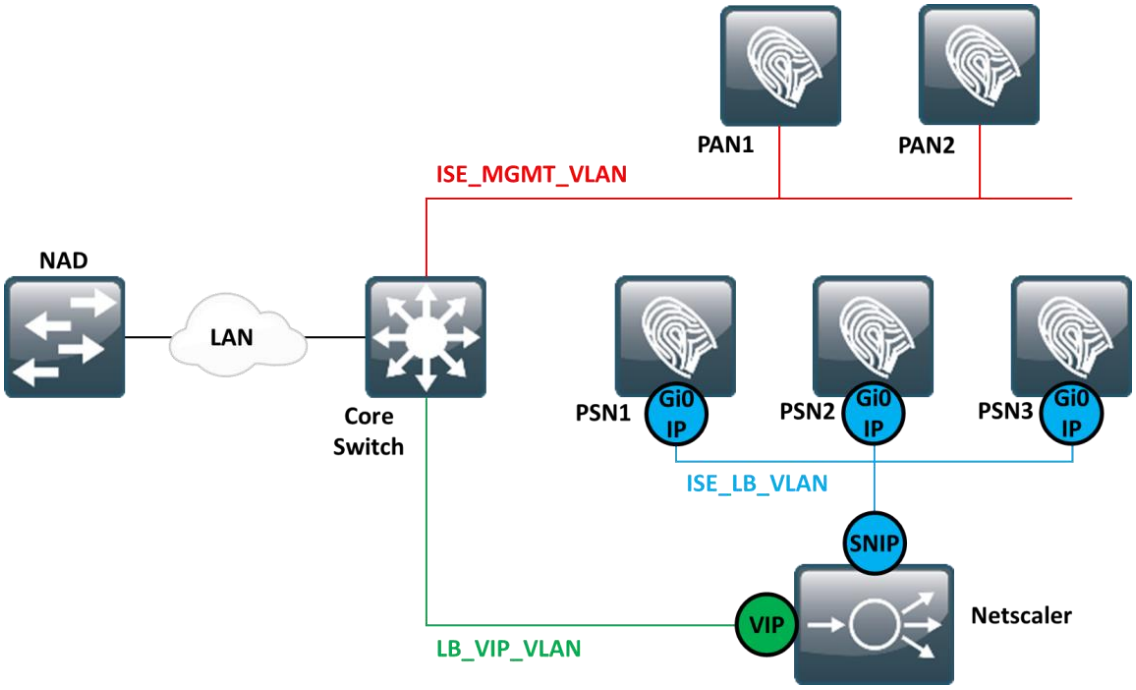
Cisco ISE

ISE Policy Service Node PSN Appliances run the following services (some services are restricted to a particular appliance interface):

ISE PSN Service	Appliance Interface
Administration	**GigabitEthernet 0 only**
Replication an Synchronization	**GigabitEthernet 0 only**
Clustering (Node Group)	**GigabitEthernet 0 only**
CA PKI	GigabitEthernet 0 only
Device Administration	**Any**
Monitoring	**Any**
Logging (outbound)	**Any**
Session (RADIUS)	**Any**
External Identity Sources and Resources	**Any**
Web Portal Services	Any
Posture	Any
Bring Your Own Device	Any
Mobile Device Management (MDM)	Any
Profiling	**Any**

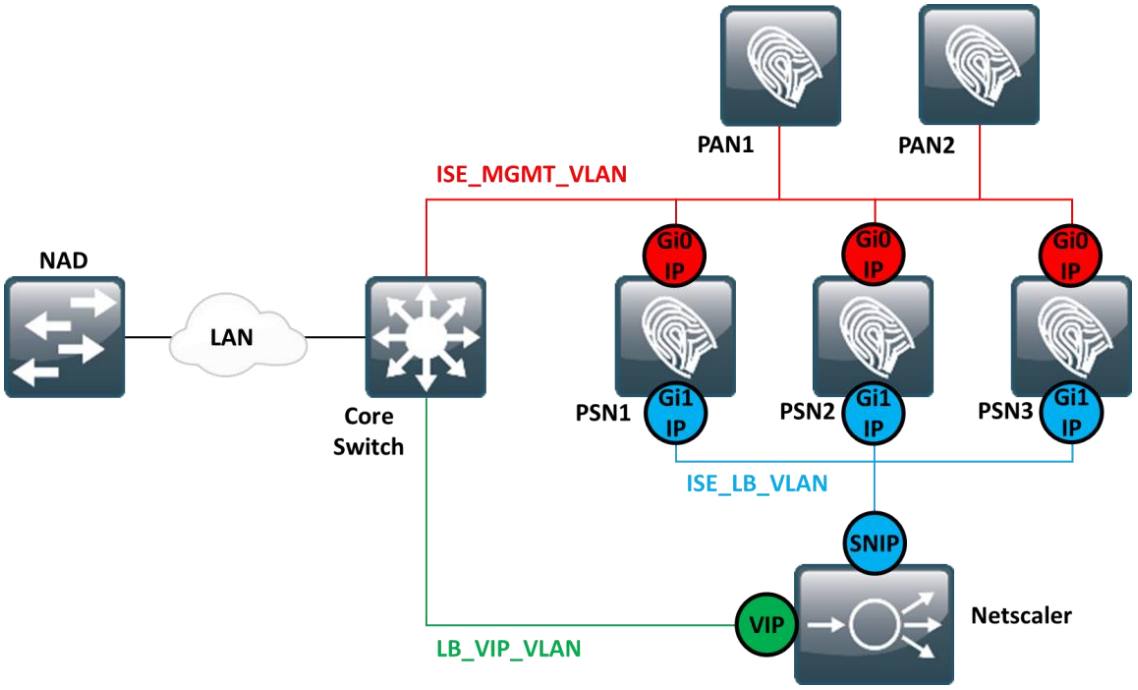
This document looks at the options for loadbalancing Session services (RADIUS Authentication, Accounting and CoA) using a Citrix Netscaler while supporting the other services highlighted in green.

Option 1- Fully Inline



- Single PSN interface (Gi0) used for all services (all traffic flows through Netscaler)
- PSNs configured with Netscaler SNIP as the default-gateway
- Core switch configured with a static route for ISE_LB_VLAN (next hop is Netscaler)

Option 2- Fully Inline (Multiple PSN Interfaces)



- Multiple PSN interface used:
  - Gi1 used for loadbalanced Session services (RADIUS Authentication, Accounting and CoA)
  - Gi0 used for all other services (including profiling)
- PSN routing:
  - PSN Appliances configured with the default-gateway of the ISE_MGMT_VLAN (i.e. Gi0 preferred)
  - PSN Appliances configured with a static default route (next hop is Netscaler SNIP) to allow traffic received on Gi1 to return via that interface
  - For CoA, PSN Appliances configured with a static default route (next hop is Netscaler SNIP) for all NAD management subnets

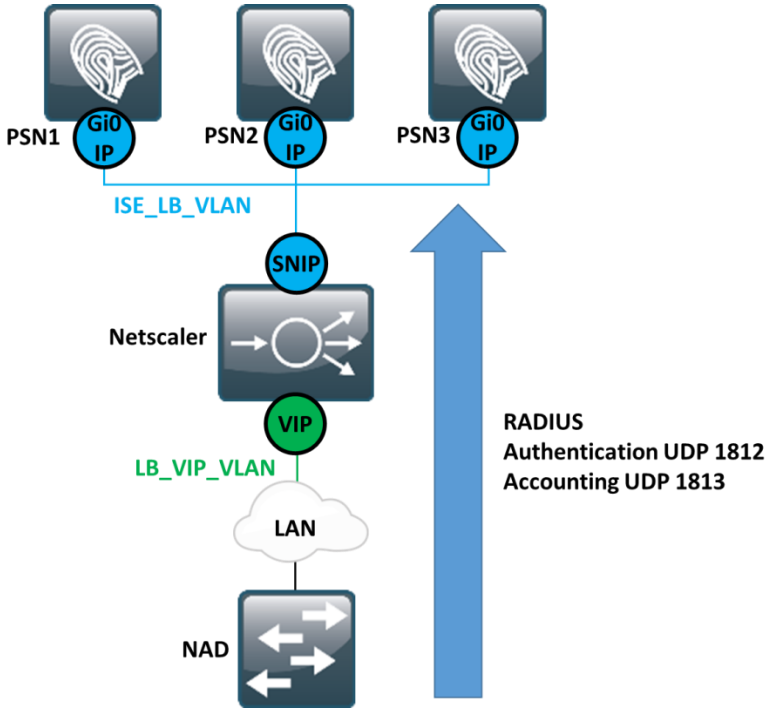
NAD Configuration

NAD configuration excerpt:

```
aaa group server radius ISE-RADIUS
 server name ise-vip
!
aaa authentication dot1x default group ISE-RADIUS
aaa authorization network default group ISE-RADIUS
aaa accounting identity default start-stop group ISE-RADIUS
!
aaa server radius dynamic-author
 client <NETSCALER_VIP> server-key <RADIUS_KEY>
!
radius server ise-vip
 address ipv4 <NETSCALER_VIP> auth-port 1812 acct-port 1813
 key <RADIUS_KEY>
!
```

- Netscaler VIP listed as the sole IP address for RADIUS and CoA (dynamic author)

Netscaler Configuration (RADIUS Authentication/Accounting)



- RADIUS packets sourced from the NAD will not be NAT'd by the Netscaler. RADIUS packets received by the PSNs will be sourced from the NAD management IP Address:
    - PSNs will have the NAD listed as an AAA device
- PSNs configured with a default-gateway of the Netscaler SNIP
- Netscaler will use USIP (Use Client IP) for RADIUS 1812/1813 so that PSNs will see the NAD management IP Address
- Netscaler RADIUS 1812/1813 Persistence will be done using the RADIUS attributes Framed-IP-Address and Calling-Station-Id
- Netscaler will monitor PSN availability using a RADIUS authentication monitor with a test username/password:
    - PSNs will have the Netscaler SNIP listed as an AAA device for this monitor

Netscaler Configuration

The following Netscaler configuration is for RADIUS authentication

Monitor

add lb monitor ISE-RADIUS-MONITOR RADIUS -respCode 2 -userName <TEST_USER_ACCOUNT> -password <TEST_USER_PASSWORD> -encrypted -radKey <RADIUS_KEY> -encrypted -radNASip <NETSCALER_SNIP> -LRTM DISABLED -deviation 0 -interval 5 -resptimeout 2 -downTime 30 -destPort 1812

Monitor ***ISE-RADIUS-MONITOR RADIUS*** sends authentication requests to PSNs with Test user account details (sourced from Netscaler SNIP). Monitor is successful if access-accept is reurned (response code 2)

ISE Service Group

add serviceGroup GROUP-ISE-PSN-AUTH RADIUS -maxClient 0 -maxReq 0 -cip DISABLED -usip YES -useproxyport NO -cltTimeout 120 -svrTimeout 120 -CKA NO -TCPB NO -CMP NO

RADIUS Service group ***GROUP-ISE-PSN-AUTH RADIUS*** has USIP (Use Client IP) enabled

ISN PSN Servers

bind serviceGroup GROUP-ISE-PSN-AUTH <ISE-PSN1-IP> 1812
bind serviceGroup GROUP-ISE-PSN-AUTH -monitorName ISE-RADIUS-MONITOR

All PSN servers are added to service group ***GROUP-ISE-PSN-AUTH RADIUS*** and bound to the monitor ***ISE-RADIUS-MONITOR RADIUS***

ISE Persistence Rule

add policy expression ISE_RADIUS_PERSISTENCE "CLIENT.UDP.RADIUS.ATTR_TYPE(8)+CLIENT.UDP.RADIUS.ATTR_TYPE(31)"

Persistence rule ***ISE_RADIUS_PERSISTENCE*** matches on RADIUS attributes 8 (Framed-IP-Address) and 31 (Calling-Station-Id)

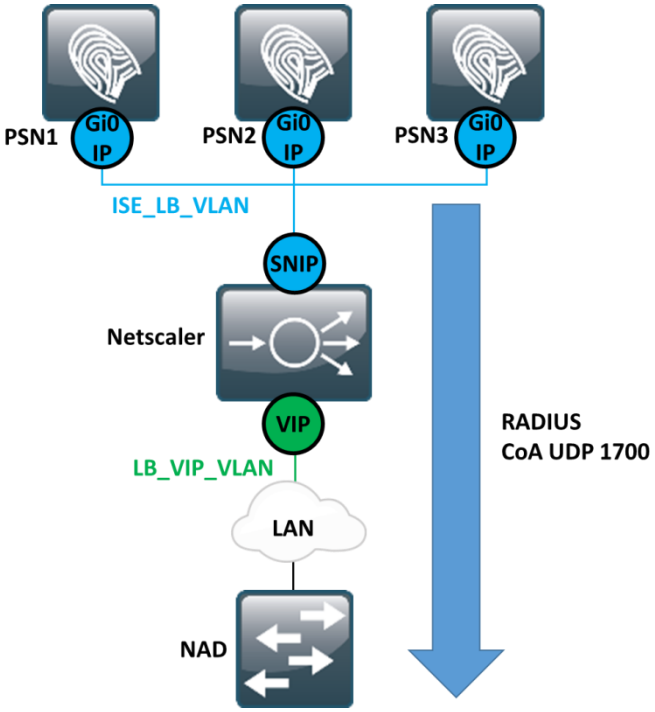
ISE VIP

add lb vserver VSRV-ISE-RADIUS-AUTH RADIUS <NETSCALER_VIP>1812 -rule ISE_RADIUS_PERSISTENCE -cltTimeout 120

set lb group GROUP-ISE-PSN-AUTH -persistenceType RULE -rule ISE_RADIUS_PERSISTENCE

VIP ***VSRV-ISE-RADIUS-AUTH*** created and bound to server group ***GROUP-ISE-PSN-AUTH RADIUS*** with persistence rule ***ISE_RADIUS_PERSISTENCE***

Netscaler Configuration (RADIUS CoA)



- RADIUS CoA packets sourced from the PSNs must be RNAT's so that the NAD sees the source as being the Netscaler VIP

CoA RNAT

```
add ns acl ISE_COA ALLOW -srcIP = <ISE_PSN_IP_ADDRESSES> -destPort = 1700 -protocol UDP
set rnat ISE_COA -natIP <NETSCALER_VIP>
```