

Cisco and F5 Deployment Guide: ISE Load Balancing using BIG-IP

Secure Access How-To Guides Series

Author: Craig Hys, Cisco Systems

Date: December 2014

Table of Contents

Introduction	6
What is Cisco Identity Services Engine?.....	6
What are F5 BIG-IP Local Traffic Manager and Global Traffic Manager?	6
About This Document.....	7
Scenario Overview	8
Topology.....	8
Components	8
Topology and Traffic Flow	10
Deployment Model	10
Physically Inline Traffic Flow	10
Logically Inline Traffic Flow	10
Topology and Network Addressing	11
Configuration Prerequisites	14
F5 LTM Configuration Prerequisites	14
Verify Basic F5 LTM Network Interfaces Assignments, VLANs, IP Addressing, and Routing.....	14
Optional: Verify LTM High Availability	15
Cisco ISE Configuration Prerequisites	16
Configure Node Groups for Policy Service Nodes in a Load-Balanced Cluster	16
Add F5 BIG-IP LTM as a NAD for RADIUS Health Monitoring.....	19
Configure DNS to Support PSN Load Balancing.....	22
Configure Certificates to Support PSN Load Balancing	22
IP Forwarding for Non-LB traffic	29
Load Balancing RADIUS	32
NAT Restrictions for RADIUS Load Balancing.....	32
RADIUS Persistence.....	33
Sticky Methods for RADIUS	33
Sticky Attributes for RADIUS	33
Example F5 BIG-IP LTM iRules for RADIUS Persistence.....	34
Fragmentation and Reassembly for RADIUS.....	36
Persistence Timeout for RADIUS	37
NAD Requirements for RADIUS Persistence	37
RADIUS Load Balancing Data Flow.....	40
RADIUS Health Monitoring	40

F5 LTM Monitor for RADIUS	40
RADIUS Monitor Timers	41
User Account Selection for RADIUS Probes	42
ISE Filtering and Log Suppression	42
RADIUS Load Balancing: F5 LTM Configuration Details	44
RADIUS CoA Handling	50
Network Access Device Configuration for CoA	50
Source NAT for RADIUS CoA	51
RADIUS CoA SNAT: F5 LTM Configuration Details	52
Load Balancing ISE Profiling	55
Introduction	55
What is ISE Profiling?	55
Why Should I Load Balance Profiling Traffic?	55
Which Profiling Data Should Be Load Balanced?	56
Load Balancing RADIUS Profiling Data	56
Health Monitors for Profiling Services: DHCP, SNMP, and NetFlow	56
Load Balancing DHCP Profiling Data.....	57
DHCP Profiling Data Flow	58
DHCP Profiling Persistence.....	58
Load Balancing SNMP Trap Profiling Data	59
Load Balancing Netflow Profiling Data.....	60
Profiling Load Balancing: F5 LTM Configuration Details.....	61
Load Balancing ISE Web Services	66
URL-Redirected Web Services	66
URL-Redirection Traffic Flow	66
Shared PSN Portal Interface for URL-Redirected Portals	67
Dedicated PSN Portal Interface for URL-Redirected Portals	67
Direct-Access Web Services.....	69
Web Portal Load Balancing Traffic Flow	69
Load Balancing Sponsor, My Devices, and LWA Portals	70
Shared PSN Portal Interface for Direct-Access Portals.....	70
Dedicated PSN Portal Interface for Direct-Access Portals	70
ISE Web Portal Interfaces and Service Ports	71
Virtual Servers and Pools to Support Portal FQDNs and Redirection.....	73
LWA Configuration Example for Cisco Wireless Controller	73

HTTPS Persistence for Direct-Access Portals	74
HTTPS Health Monitoring	74
F5 LTM Monitor for HTTPS	75
HTTPS Monitor Timers	75
User Account Selection for HTTPS Probes	75
HTTPS Load Balancing: F5 LTM Configuration Details	76
Global ISE Load Balancing Considerations	82
General Monitoring and Troubleshooting.....	86
Cisco ISE Monitoring and Troubleshooting.....	86
Verify Operational Status of Cisco Components	86
ISE Authentications Live Log.....	90
ISE Reports	91
ISE Packet Capture using TCP Dump.....	91
Logging Suppression and Collection Filters	92
F5 BIG-IP LTM Monitoring and Troubleshooting	92
Verify Operational Status of F5 LTM Components	92
Health Monitors	93
Persistence Records	94
iRule Debug and View Local Traffic Logs.....	96
Packet Capture using TCP Dump	97
Network Topology, Routing, and Addressing Review	97
Appendix A: F5 Configuration Examples.....	98
Example F5 BIG-IP LTM Configurations.....	98
Full F5 LTM Configuration	98
Example F5 iRules for DHCP Persistence.....	109
DHCP Persistence iRule Example: dhcp_mac_sticky.....	109
Appendix B: Configuration Checklist.....	114

Configuration Tables

Table 1. F5 and Cisco Components	9
Table 2. Network Addressing Scheme	12
Table 3. LTM Forwarding IP Configuration	29
Table 4. RADIUS Attributes for Cisco Catalyst Switches	38
Table 5. LTM RADIUS Load Balancing Configuration	44
Table 6. LTM RADIUS CoA SNAT Configuration	53
Table 7. LTM Profiling Load Balancing Configuration.....	61
Table 8. LTM HTTPS Load Balancing Configuration	76
Table 9. Configuration Checklist	114

Introduction

What is Cisco Identity Services Engine?

Cisco Identity Services Engine (ISE) is an all-in-one enterprise policy control product that enables comprehensive secure wired, wireless, and Virtual Private Networking (VPN) access.

Cisco ISE offers a centralized control point for comprehensive policy management and enforcement in a single RADIUS-based product. The unique architecture of Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. The administrator can then use that information to make proactive governance decisions. Cisco ISE is an integral component of Cisco Secure Access.

Cisco Secure Access is an advanced Network Access Control and Identity Solution that is integrated into the Network Infrastructure. It is a fully tested, validated solution where all the components within the solution are thoroughly vetted and rigorously tested as an integrated system.

Unlike overlay Network Access Control solutions the Cisco Secure Access utilizes the access layer devices (switches, wireless controllers, etc.) for enforcement. The access device itself now handles functions that were commonly handled by appliances and other overlay devices, such as URL redirection for web authentications.

The Cisco Secure Access not only combines standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control, it also has many more advanced identity and enforcement capabilities such as flexible authentication, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), device profiling, guest and web authentications services, posture assessments, and integration with leading Mobile Device Management (MDM) vendors for compliance validation of mobile devices before and during network access.

What are F5 BIG-IP Local Traffic Manager and Global Traffic Manager?

F5 Local Traffic Manager (LTM) and Global Traffic Manager (GTM) are part of F5's industry-leading BIG-IP Application Delivery Solutions.

BIG-IP Local Traffic Manager provides intelligent traffic management for rapid application deployment, optimization, load balancing, and offloading. LTM increases operational efficiency and ensures peak network performance by providing a flexible, high-performance application delivery system. With its application-centric perspective, BIG-IP LTM optimizes your network infrastructure to deliver availability, security, and performance for critical business applications.

BIG-IP Global Traffic Manager is a global load balancing solution that improves access to applications by securing and accelerating Domain Name resolution. Using high-performance DNS services, BIG-IP GTM scales and secures your DNS infrastructure during high query volumes and DDoS attacks. It delivers a complete, real-time DNSSEC solution that protects against hijacking attacks. BIG-IP GTM improves the performance and availability of your applications by intelligently directing users to the closest or best-performing physical, virtual, or cloud environment. In addition, enables mitigation of complex threats from malware and viruses by blocking access to malicious IP domains.

About This Document

This document is the result of a joint effort on behalf of Cisco and F5 to detail best practice design and configurations for deploying BIG-IP Local Traffic Manager with Cisco Identity Services Engine. This is a validated solution that has undergone thorough design review and lab testing from both Cisco and F5. This document is intended to serve as a deployment aid for customers as well as support personnel alike to ensure a successful deployment when integrating these vendor solutions.

Many features may exist that could benefit your deployment, but if they are not part of the tested solution they may not be included in this document. Other configurations are possible and may be working successfully in your specific deployment, but may not be covered in this guide due to insufficient testing or confidence for a stable deployment. Additionally, many features and scenarios have been tested, but are not considered a best practice, and therefore may not be included in this document (Example: Transparent mode load balancing).

Note: Within this document, we describe the recommended method of deployment, and a few different options depending on the level of security and flexibility needed in your environment. These methods are illustrated by examples and include step-by-step instructions for deploying an F5 BIG-IP LTM-Cisco ISE deployment as prescribed by best practices to ensure a successful project deployment.

Scenario Overview

Topology

The figure depicts a basic end-to-end Cisco ISE deployment integrated with an F5 BIG-IP Load Balancer. The figure includes key components of the deployment even though they may not be directly involved with the load balancing process. These components include other ISE nodes such as the Policy Administration node (PAN), Monitoring and Troubleshooting node (MnT) and supporting servers and services like Microsoft Active Directory (AD), Lightweight Directory Access Protocol (LDAP), Domain Name Service (DNS), Network Time Protocol (NTP), Simple Mail Transport Protocol (SMTP), and external Sysloggers.

This document focuses on the load balancing of the following ISE Policy Service Node (PSN) services:

- RADIUS Authentication, Authorization, and Accounting (AAA) requests from network access devices (NADs) as well as RADIUS Change of Authorization (CoA) from ISE PSNs to NADs.
- Profiling data sent by NADs and other network infrastructure and security devices.
- Web services for Sponsors (ISE Guest Services) and My Devices (ISE Device Registration Services)

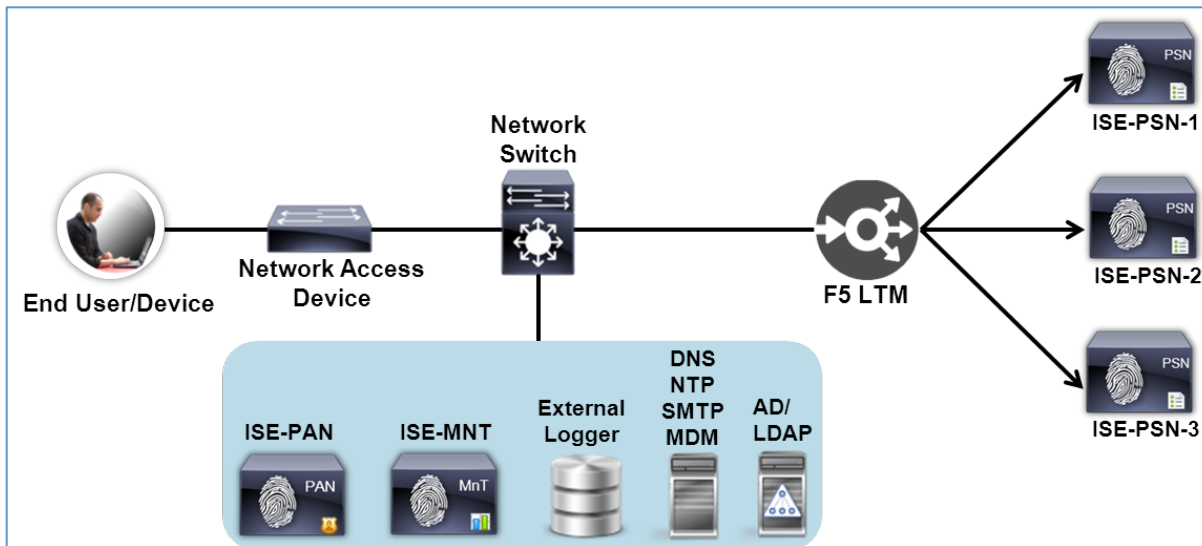


Figure 1. Topology Overview

For simplicity, three ISE PSNs are depicted in the sample topology, although a load-balanced group of PSN nodes could constitute two or more appliances.

Components

The table includes the supported hardware as well as versions tested in this guide. Other platforms and versions may also work but can be subject to specific limitations. Platform and version specific caveats and issues are noted as best possible within the guide.

Table 1. F5 and Cisco Components

Component	Supported Hardware/Virtual Platforms	Recommended Software Releases
F5 BIG-IP Local Traffic Manager (LTM)	Refer to SOL9476: The F5 hardware/software compatibility matrix for list of supported F5 platforms and software versions.	F5 BIG-IP LTM 11.4.0 hotfix HF6 and above F5 BIG-IP LTM 11.4.1 hotfix HF5 and above
Cisco Identity Services Engine (ISE)	Any supported appliance: 1121/3315, 3355, 3395, SNS-3415, SNS-3495, VMware. Refer to Release Notes for Cisco Identity Services Engine for list of supported ISE hardware and virtual appliances by software version.	Cisco ISE 1.2.0 and above
Cisco Catalyst Series Switch	Refer to the Cisco Identity Services Engine Network Component Compatibility Guide for list of supported Cisco switch platforms and recommended software versions for ISE. The configurations in this guide should work with many switch platforms but actual support will be depend on the capabilities of the network access device and support for specific RADIUS features and attributes.	
Cisco Wireless LAN Controller (WLC) Series Wireless Services Module (WiSM)	Refer to the Cisco Identity Services Engine Network Component Compatibility Guide for current list of supported Cisco wireless platforms and recommended software versions for ISE. The configurations in this guide should work with many wireless platforms but actual support will be dependent on the capabilities of the network access device and support for specific RADIUS features and attributes.	

Note: For F5 BIG-IP LTM, the minimum recommended software release is 11.4.1 hotfix HF5 or 11.4.0 hotfix HF6. Additionally, 11.6.0 HF2 incorporates performance enhancements that can improve RADIUS load balancing performance.

Topology and Traffic Flow

Deployment Model

There are many ways to insert the F5 BIG-IP LTM load balancer (LB) into the traffic flow for ISE PSN services. The actual traffic flow will depend on the service being load balanced and the configuration of the core components including the NAD, F5 BIG-IP LTM, ISE PSNs, and the connecting infrastructure. The method that has been most tested and validated in successful customer deployments is a fully inline deployment.

In a fully inline deployment, the F5 BIG-IP-LTM is either physically or logically inline for all traffic between endpoints/access devices and the PSNs. This includes RADIUS, direct and URL-redirected web services, profiling data, and other communications to supporting services.

Physically Inline Traffic Flow

The figure below depicts the “physically inline” scenario. The F5 BIG-IP LTM uses different physical adapters for the internal and external interfaces to separate the PSNs from the rest of the network; all traffic to/from the PSNs must pass through the load balancer on different physical interfaces.

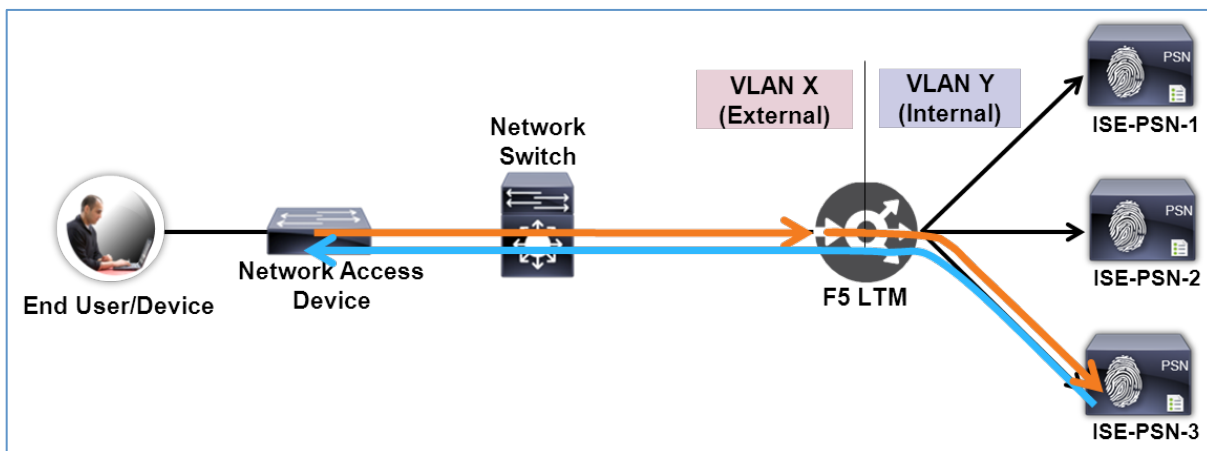


Figure 2. Physically Inline Traffic Flow

Logically Inline Traffic Flow

The figure below depicts the “logically inline” or “on-a-stick” deployment scenario. Like the physically inline case, the PSNs are on a separate network from the rest of the network and all traffic to/from the PSNs must pass through the load balancer. The difference is that only a single physical adapter is configured with VLAN trunking; network separation for the PSNs is provided using *logical* internal and external interfaces.

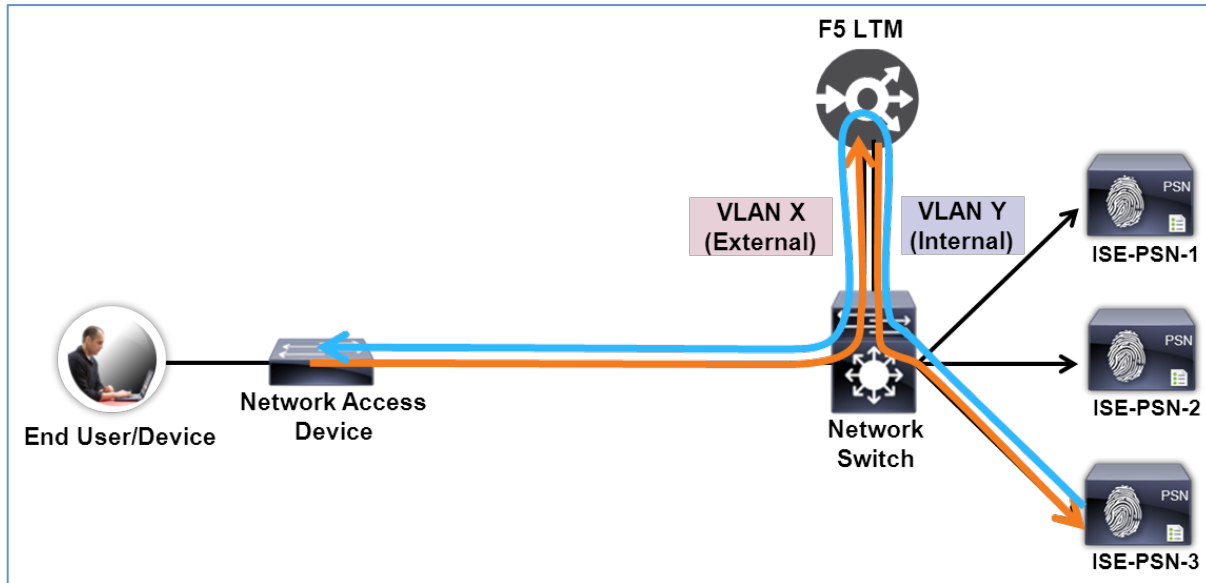


Figure 3. Logically Inline Traffic Flow

In both cases routes must be configured to point to the F5 external interface to reach the PSNs on the internal interface. Additionally, the PSNs must have their default gateway set to the F5's internal interface.

Both of the above inline deployment models are valid and the one chosen is primarily one of customer preference. Some customers prefer physical separation and more intuitive traffic paths using different network adapters while other customers opt for the simplicity of a single interface connection.

Note: For very high traffic volume, a single connection using the inline deployment model will incur higher per-interface utilization. Separate physical interfaces can be used to increase interface bandwidth capacity.

Topology and Network Addressing

The sample topology below will be used to illustrate the load-balancing configuration of ISE PSN services using an F5 BIG-IP appliance. The diagram includes the network-addressing scheme used in the detailed configuration steps. Notice in the following illustration that the F5 BIG-IP LTM is deployed fully inline between the ISE PSNs and the rest of the network.

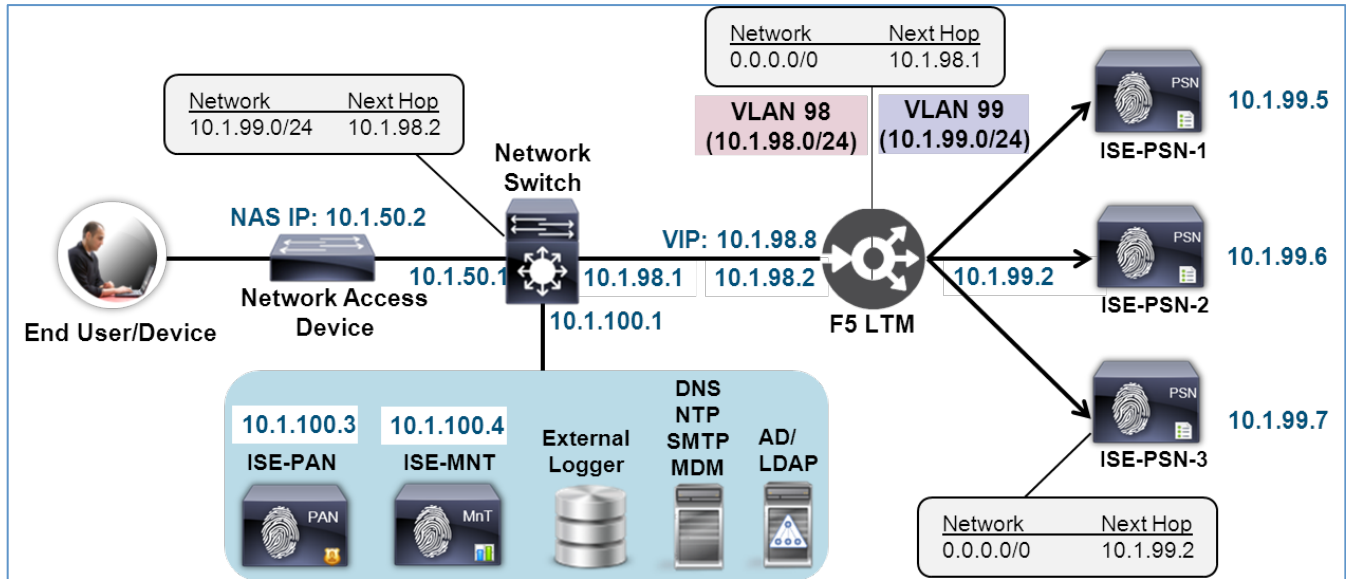


Figure 4. Sample Topology Network Addressing Scheme

The PSNs are on a dedicated VLAN 99 (subnet 10.1.99.0/24). Each PSN has a default gateway to the F5 LTM load balancer’s internal interface with Self IP 10.1.99.2. The virtual IP (VIP) for load balanced services (10.1.98.8) is on a separate VLAN 98 (subnet 10.1.98/24). The F5 BIG-IP LTM has a default gateway to the upstream network switch at 10.1.98.1. Since the F5 LTM is not advertising internal routes, it is necessary that the network switch be configured with a static route to the 10.1.99.0/24 network with a next hop set to the Self IP for the F5 LTM’s external interface at 10.1.98.2. The table displays the network addressing scheme for the sample topology.

Table 2. Network Addressing Scheme

Device	Interface	VLAN	Subnet	IP Address	Routing
ISE-PAN	GE0	100	10.1.100.0/24	10.1.100.3	DFG: 10.1.100.1
ISE-MNT	GE0	100	10.1.100.0/24	10.1.100.4	DFG: 10.1.100.1
ISE-PSN-1	GE0	99	10.1.99.0/24	10.1.99.5	DFG: 10.1.99.2
ISE-PSN-2	GE0	99	10.1.99.0/24	10.1.99.6	DFG: 10.1.99.2
ISE-PSN-3	GE0	99	10.1.99.0/24	10.1.99.7	DFG: 10.1.99.2
F5-BIG-IP	Internal	99	10.1.99.0/24	10.1.99.2	
F5-BIG-IP	External	98	10.1.98.0/24	10.1.98.2	DFG: 10.1.98.1
Network Switch/Router	F5 LTM-Facing	98	10.1.98.0/24	10.1.98.1	10.1.99.0/24: Next Hop 10.1.98.2
Network Switch/Router	NAD-Facing	50	10.1.50.0/24	10.1.50.1	
Network Switch/Router	Server-Facing	100	10.1.100.0/24	10.1.100.1	
Network Access Device	RADIUS Source	50	10.1.50.0/24	10.1.50.2	DFG: 10.1.50.1

Best Practice: A well-documented topology with network addressing and routing information is a critical step in ensuring a successful ISE deployment using load balancers. One of the top issues that cause load-balancing issues is failure to understand the path traffic is taking through or around the load balancer. This includes the ingress and egress interfaces/VLANs for all devices as well as route next hops and source/destination IP addresses/port numbers for all traffic in the end-to-end flow.

Configuration Prerequisites

F5 LTM Configuration Prerequisites

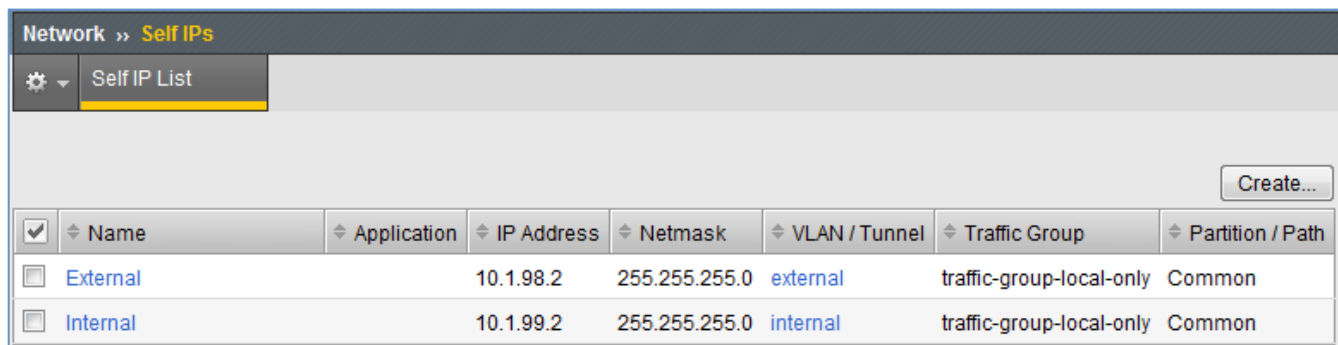
This section includes items that are assumed to be pre-configured or setup prior to the primary load balancing configuration. These include:

- Validate IP addressing for Internal and External interfaces
- Validate correct VLAN assignments
- Verify routes are properly configured to forward traffic
- Optional: Verify LTM High Availability

Verify Basic F5 LTM Network Interfaces Assignments, VLANs, IP Addressing, and Routing

Verify Self IP address and interface settings

Step 1 From the F5 LTM web-based admin interface, navigate to **Main > Network Self IPs** and check the IP address and interface assignments as shown:

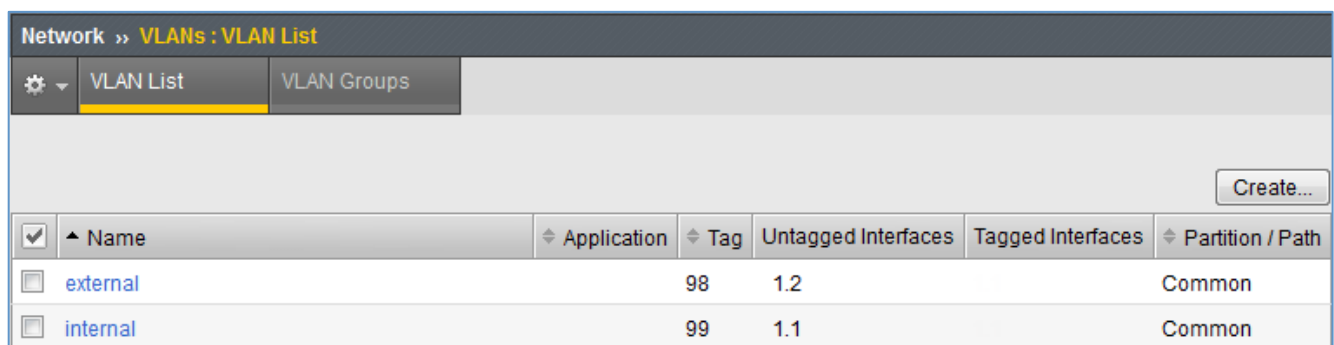


The screenshot shows the 'Network >> Self IPs' configuration page. It features a 'Self IP List' table with columns for Name, Application, IP Address, Netmask, VLAN / Tunnel, Traffic Group, and Partition / Path. There are two entries: 'External' and 'Internal'. A 'Create...' button is visible in the top right corner.

<input checked="" type="checkbox"/>	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
<input type="checkbox"/>	External		10.1.98.2	255.255.255.0	external	traffic-group-local-only	Common
<input type="checkbox"/>	Internal		10.1.99.2	255.255.255.0	internal	traffic-group-local-only	Common

Figure 5. LTM Self IP Configuration

Step 2 Navigate to **Main > Network > VLANs > VLAN List** and check interfaces for correct VLAN assignment, tagging and physical interface mapping as shown:



The screenshot shows the 'Network >> VLANs : VLAN List' configuration page. It features a 'VLAN List' table with columns for Name, Application, Tag, Untagged Interfaces, Tagged Interfaces, and Partition / Path. There are two entries: 'external' and 'internal'. A 'Create...' button is visible in the top right corner.

<input checked="" type="checkbox"/>	Name	Application	Tag	Untagged Interfaces	Tagged Interfaces	Partition / Path
<input type="checkbox"/>	external		98	1.2		Common
<input type="checkbox"/>	internal		99	1.1		Common

Figure 6. : LTM VLAN Configuration for Untagged Interfaces

In the above example, the first available interface 1.1 is mapped to *internal* and associated with VLAN 99. Interface 1.2 is mapped to *external* and associated to VLAN 98. Since both interfaces are dedicated network connections (no trunking), each are configured as “Untagged”.

The diagram below shows an example of how to configure a single trunked interface for virtual network separation.

<input type="checkbox"/>	Name	Application	Tag	Untagged Interfaces	Tagged Interfaces	Partition / Path
<input type="checkbox"/>	external		98		1.1	Common
<input type="checkbox"/>	internal		99		1.1	Common

Figure 7. LTM VLAN Configuration for Tagged Interfaces

Note that only one single interface is used (1.1) and separate VLANs assigned using tagged interfaces. The connecting switch will need to be configured for 802.1Q trunking for the specified VLANs (example: 98 and 99).

Step 3 Navigate to Main > Network > Routes and confirm that a default route exists for the upstream Layer 3 gateway.

<input type="checkbox"/>	Name	Application	Destination	Netmask	Route Domain	Resource Type	Resource	Partition / Path
<input type="checkbox"/>	external_default_gateway	Default IPv4			Partition Default Route Domain	Gateway	10.1.98.1	Common

Figure 8. LTM Default Gateway Configuration

In the example, the default gateway for the F5 LTM appliance is the upstream network switch at 10.1.98.1 off the external interface.

Note: For simplicity, the example configuration uses the Common partition for load balanced virtual servers and services. It is up to customer discretion whether the need for a separate partition is deemed necessary for the ISE load-balancing configuration.

Optional: Verify LTM High Availability

F5 BIG-IP LTM may be configured in Active-Standby and Active-Active high availability modes to prevent single points of failure with the load balancing appliance. Configuration of LTM high availability is beyond the scope of this guide. For additional details on Active-Standby configuration, refer to F5 product documentation on [Creating an Active-Standby Configuration Using the Setup Utility](#). For additional details on Active-Active configuration, refer to [Creating an Active-Active Configuration Using the Setup Utility](#).

When configured for high availability, default gateways and next hop routes will point to the floating IP address on the F5 appliance, but health monitors will be sourced from the locally-assigned IP addresses.

Cisco ISE Configuration Prerequisites

This section includes items that are assumed to be pre-configured or setup prior to the primary load balancing configuration. These include:

- Node groups configured for any LB cluster
- Adding the BIG-IP LTM(s) as a NAD for RADIUS health monitoring
- DNS properly configured
- Certificates properly installed

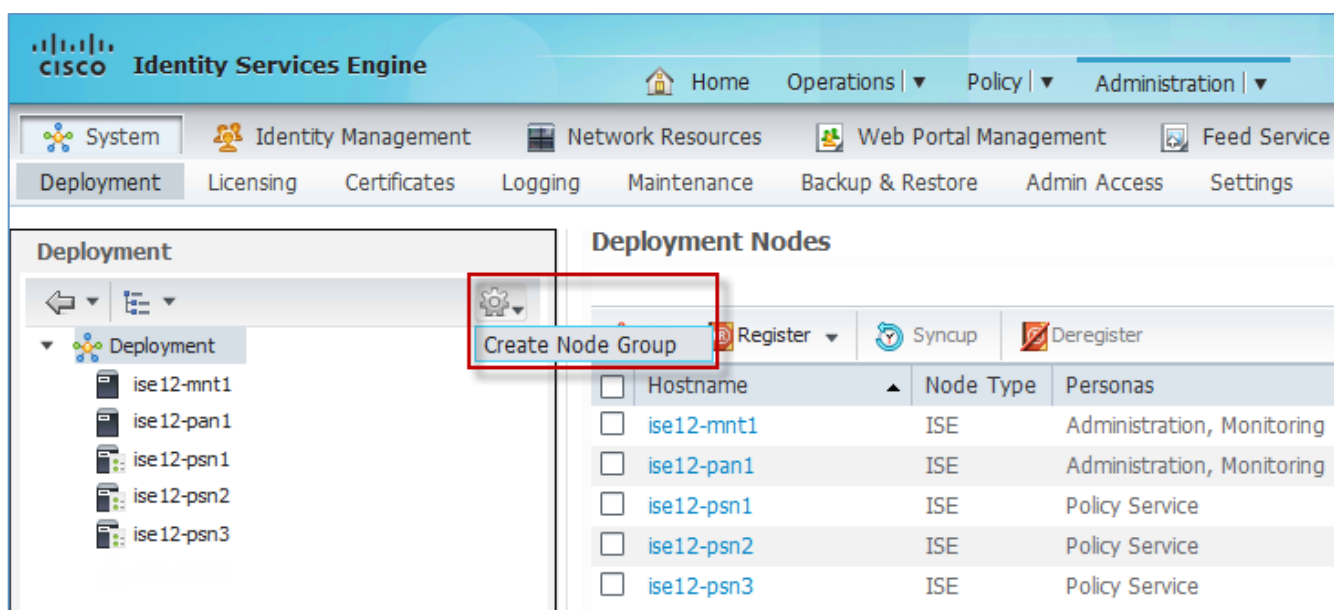
Configure Node Groups for Policy Service Nodes in a Load-Balanced Cluster

When multiple Policy Service nodes are connected through high-speed LAN connections, it is a general best practice to add them to the same ISE Node Group. ISE Node Groups optimize the replication of endpoint profiling data amongst PSNs and also offer recovery of Posture Pending sessions in the event of a node failure. Although node groups do not require members to be part of a load-balanced group, it makes sense that if multiple PSNs are part of a locally load-balanced server group, they most likely satisfy requirements for node group membership.

In ISE 1.2 and earlier, node groups use multicast to exchange information. If LB node members are not Layer 2 adjacent, then it may be necessary to ensure L3 multicast is supported and enabled on the connecting Layer 3 switch. In ISE 1.3, the use of multicast is removed and all communications occur over TCP using SSL.

Define a Node Group

Step 1 From the ISE admin interface, navigate to Administration > System > Deployment. From the left panel, click the gear icon in the upper right corner as shown to display the **Create Node Group** option:



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The left sidebar shows 'System', 'Identity Management', 'Network Resources', 'Web Portal Management', and 'Feed Service'. The main content area is titled 'Deployment Nodes' and contains a table of nodes. A red box highlights the 'Create Node Group' option in the upper right corner of the table.

Hostname	Node Type	Personas
<input type="checkbox"/> ise12-mnt1	ISE	Administration, Monitoring
<input type="checkbox"/> ise12-pan1	ISE	Administration, Monitoring
<input type="checkbox"/> ise12-psn1	ISE	Policy Service
<input type="checkbox"/> ise12-psn2	ISE	Policy Service
<input type="checkbox"/> ise12-psn3	ISE	Policy Service

Figure 9. Add ISE Node Group

Step 2 Click **Create Node Group** and complete the form and click **Submit** when finished. The below figure shows an example node group configuration.

Create Node Group

* Node Group Name:

Description:

* Multicast Address:

Example: 228.10.11.12. Please make sure you are not using a reserved/already-used multicast IP Address.

Note: Please make sure that all of the Session Services nodes that would be part of this Node Group can communicate over IP multicast. Typically, these nodes are connected to the same switch and are in the same VLAN.

Figure 10. ISE Node Group Configuration

Per the note, be sure the selected multicast address (ISE 1.2.x and earlier) is not being used in the network where the PSNs are deployed. Starting in ISE 1.3.0, multicast is no longer required for node group configuration.

Step 3 Verify the node group now appears in the list of nodes in the left panel.

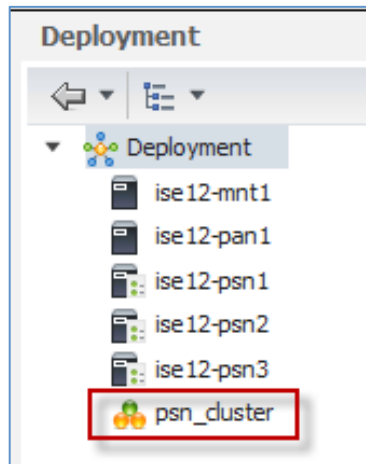


Figure 11. Display New ISE Node Groups

Add Load-Balanced PSNs to the Node Group

Add all PSNs that are part of the same local load-balanced server farm to the same node group. If there are multiple load-balanced PSN server groups, such as in separate data centers, then they will be added to their own unique group. A key criterion for node group membership is LAN proximity.

Step 1 Add a PSN to a node group by clicking the name of the PSN from either the left or right panel:

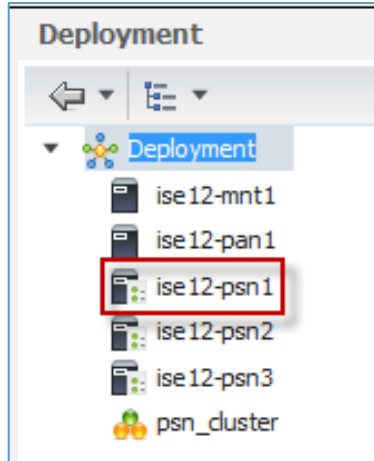


Figure 12. Select PSN for ISE Node Group Assignment

Step 2 Under the Policy Services section, click the drop down next to Include Node in Node Group box and select the name of the node group created for the load-balanced PSNs. Click **Save** to commit the changes:

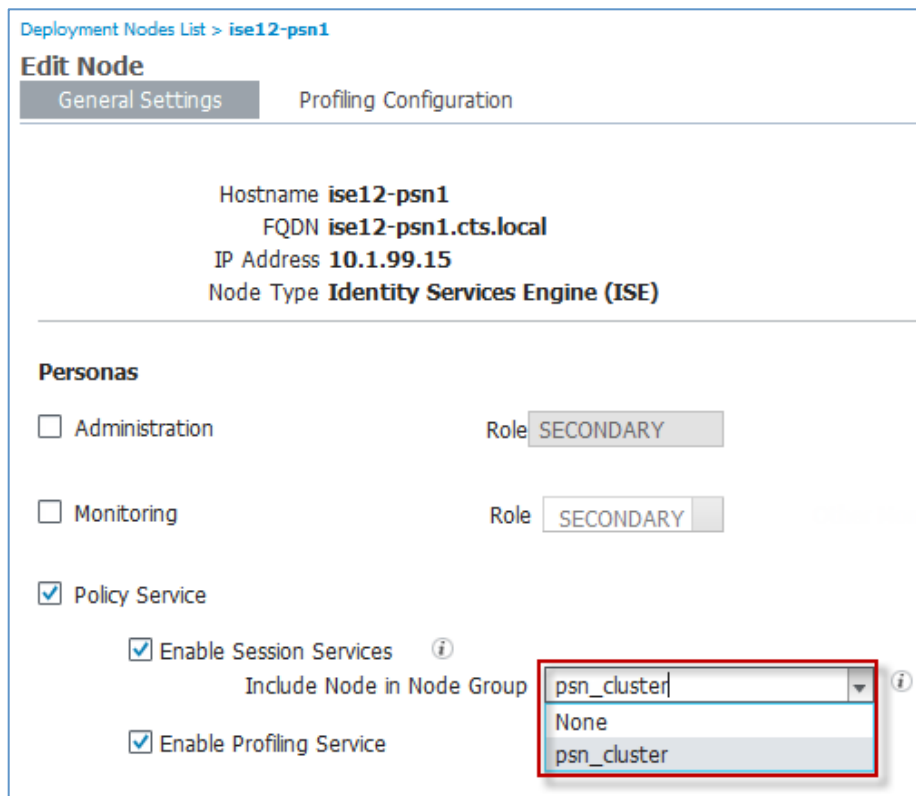


Figure 13. Assign PSN to ISE Node Group

Step 3 Repeat the steps for each PSN to be added to the node group.

Step 4 When complete, all selected PSNs should appear under the node group:

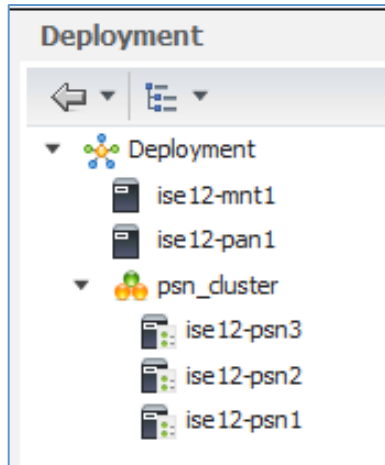


Figure 14. Verify ISE Node Group Members

Add F5 BIG-IP LTM as a NAD for RADIUS Health Monitoring

When load balancing services to one of many candidate servers, it is critical to ensure the health of each server before forwarding requests to that server. In the case of RADIUS, the F5 BIG-IP LTM includes a health monitor to periodically verify that the RADIUS service is active and correctly responding. It performs this check by simulating a RADIUS client and sending authentication requests to each PSN (the RADIUS Server) with a username and password. Based on the response or lack of response, the BIG-IP LTM can determine the current status of the RADIUS auth service. Therefore, ISE must be configured to accept these requests from the BIG-IP LTM. This section covers the steps to add the BIG-IP LTM as a Network Device (RADIUS client) to the ISE deployment.

Configure BIG-IP LTM as a Network Device in ISE

Step 1 From the ISE admin interface, navigate to Administration > Network Resources > Network Devices and click **Add** from the right panel menu.

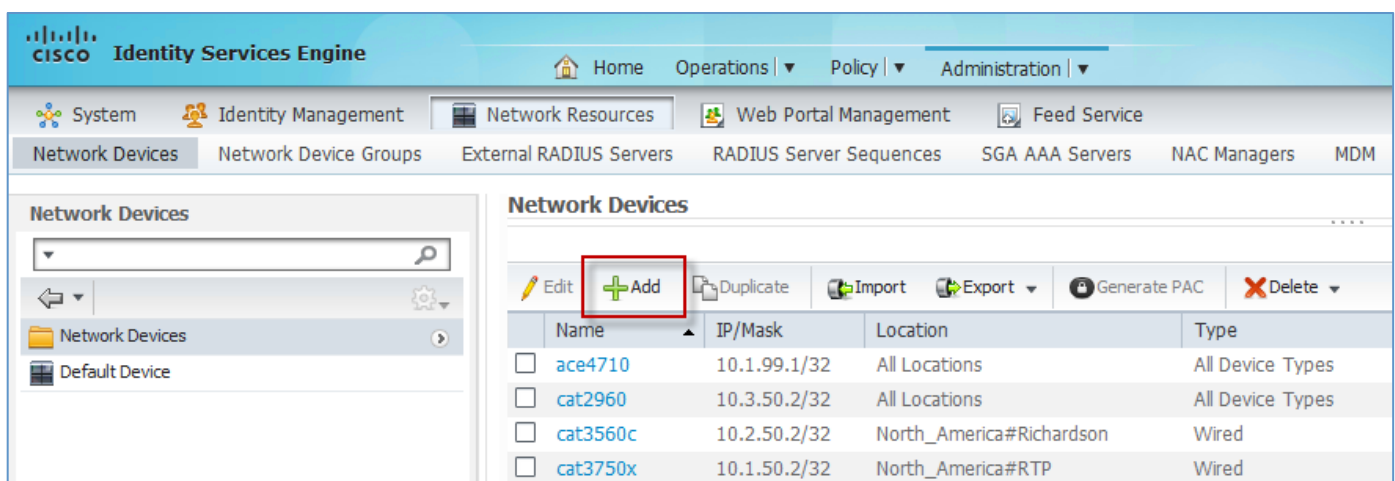
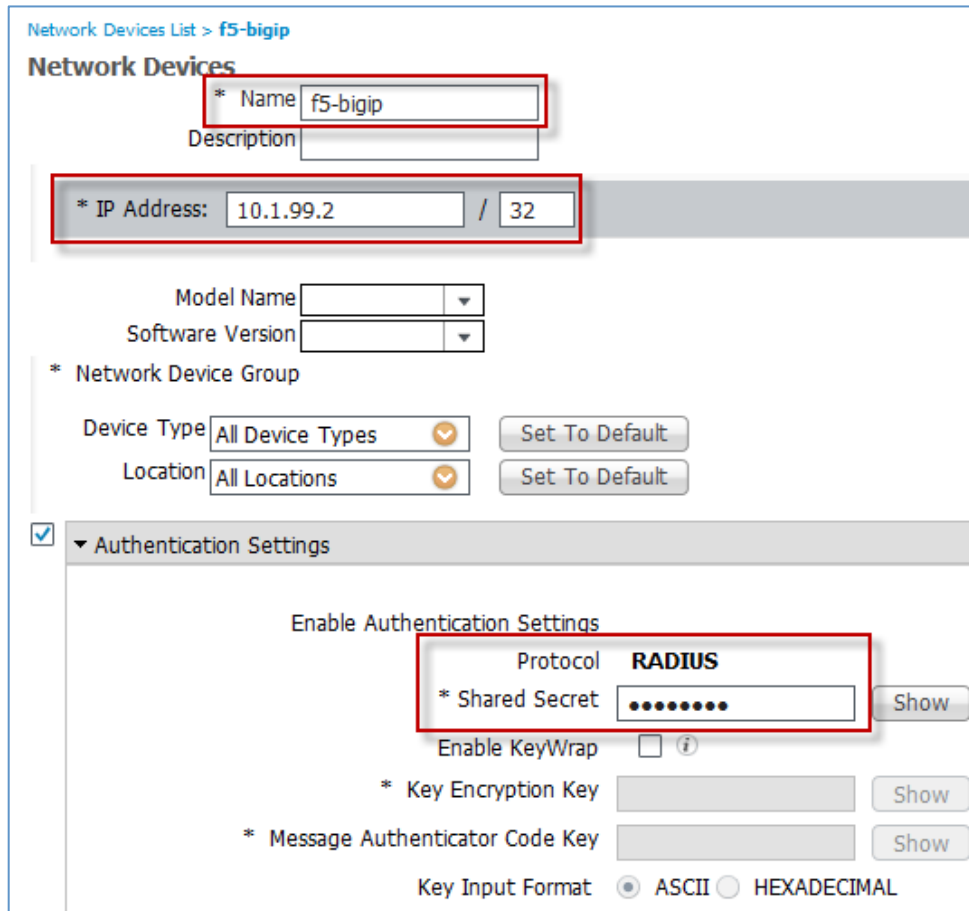


Figure 15. Add LTM as ISE Network Access Device

Step 2 Complete the form and click **Submit** when finished. Key fields that need to be completed include the following:

- a. Enter a name (such as the hostname) of the F5 BIG-IP LTM.
- b. Enter the forwarding IP address (Self IP) of the BIG-IP LTM's Internal interface. This is the source IP address of RADIUS request as seen by the ISE PSN.
- c. Click the checkbox for the Authentication Settings section and enter a shared secret. This is the password used to secure RADIUS communications between the BIG-IP LTM and the ISE PSN.



Network Devices List > f5-bigip

Network Devices

* Name

Description

* IP Address: /

Model Name

Software Version

* Network Device Group

Device Type

Location

Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

Figure 16. LTM Network Access Device Properties

- d. Write down and save the shared secret in a safe place, because it will be needed later for the F5 Monitor configuration.

Optional: Define an Internal User for F5 LTM RADIUS Health Monitor

F5 BIG-IP LTMs have the ability to treat a failed authentication (RADIUS Access-Reject) as a valid response to the RADIUS health monitor. The fact that ISE is able to provide a response indicates that the service is running. If deliberately sending incorrect user credentials, then an Access-Reject is a valid response and the server is treated as healthy.

If it is desired to have the LTM send valid credentials and receive a successful authentication response (RADIUS Access-Accept), then it is necessary to configure the appropriate Identity Store—either internal or external to ISE—with the username and password sent by the BIG-IP LTM.

This procedure shows an example of creating an ISE Internal User account for this purpose.

Note: Refer to the “RADIUS Health Monitoring” section of this guide for a detailed discussion on RADIUS Monitor considerations and F5 LTM configuration. This procedure has been included here to streamline the ISE configuration steps to support RADIUS monitoring.

Step 1 From the ISE admin interface, navigate to Administration > Identity Management > Identities > Users and Click **Add** from the right panel menu.

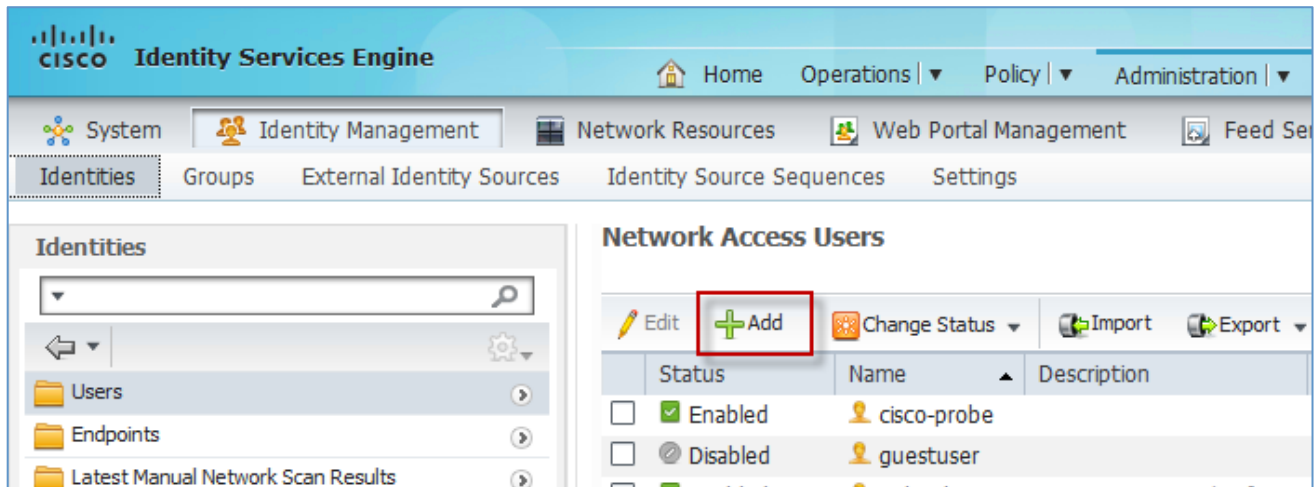


Figure 17. Add LTM RADIUS Health Monitor as ISE Internal User

Step 2 Complete the form and click **Submit** when finished. Required information includes Name and Password:

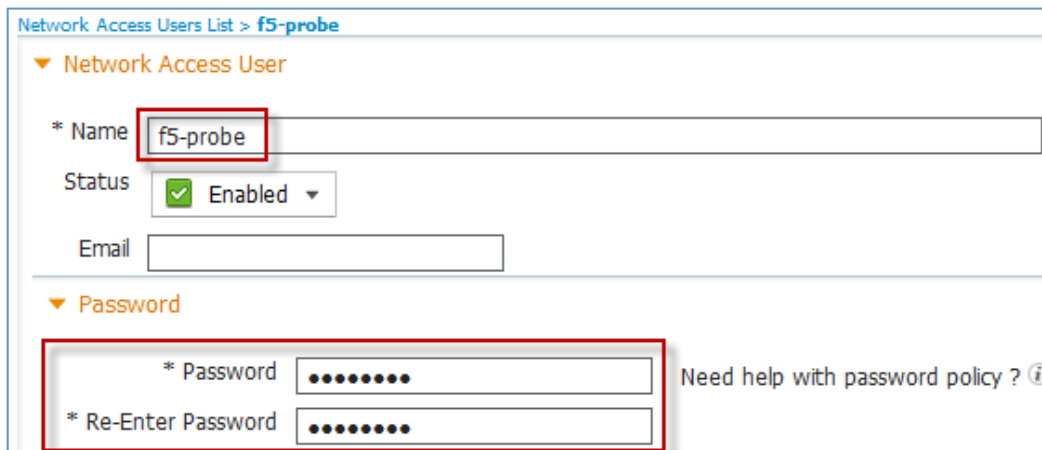


Figure 18. RADIUS Health Monitor Internal User Properties

Step 3 Write down and save the user credentials in safe place as they will be needed later for the F5 Monitor configuration.

Note: Be sure to include the identity store used for validating F5 RADIUS credentials in the Authentication Policy Rule used to authenticate the F5 monitor. In this example, the identity store InternUsers must be included as the ID store for matching load balancer requests.

Best Practice: To ensure that the F5 Monitor account is not used for other purposes that may grant unauthorized access, lock down the ability to authenticate using this account and restrict access granted to this account. As a health probe, no real network access needs to be granted.

Example: Create ISE Authorization Policy Rule that matches specifically on the F5 IP address or parent ISE Network Device Group and the specific F5 test username and return policy that denies network access such as ACL=deny ip any any.

Configure DNS to Support PSN Load Balancing

DNS plays an important role in load balancing ISE web portal services such as the Sponsor Portal and My Devices Portal. Each of these portals can run on every PSN. In order to provide high availability and scaling for these portals, we can deploy F5 LTM to load balance requests to multiple PSNs using a single fully qualified domain name (FQDN). End users can be given a simple and intuitive server name such as sponsor.company.com or guest.company.com that resolves to the IP address of an F5 LTM Virtual Server IP address. The first step in making this happen is to create entries in the organization's DNS service for these load-balanced portals.

Configure DNS Entries for Sponsor and My Devices Portals

If ISE Guest Services or My Devices are deployed and will be load balanced, add entries similar to the following in DNS.

```
DNS SERVER:  DOMAIN = COMPANY.COM

SPONSOR      IN      A       10.1.98.8
MYDEVICES    IN      A       10.1.98.8

ISE-PAN-1    IN      A       10.1.100.3
ISE-PAN-2    IN      A       10.1.101.3
ISE-MNT-1    IN      A       10.1.100.4
ISE-MNT-2    IN      A       10.1.101.4
ISE-PSN-1    IN      A       10.1.99.5
ISE-PSN-2    IN      A       10.1.99.6
ISE-PSN-3    IN      A       10.1.99.7
```

Configure Certificates to Support PSN Load Balancing

ISE Policy Service nodes use digital certificates to authenticate users via various Extensible Authentication Protocol (EAP) methods as well as to establish trust for secure web portals. When PSN load balancing is deployed, client supplicant requests may be directed to one of many PSNs for authentication and session establishment, or for web-based services including web authentication, device registration, guest and sponsor portals, and client provisioning. Therefore, it is critical that ISE nodes have certificates that will be trusted by the clients regardless of the PSN servicing the request.

To this end, clients will need to explicitly trust every PSN certificate presented or else trust the Certificate Authority (CA) chain that signed the PSN certificate. Additionally, for secure web requests, the client browser typically requires

that the identity listed in the certificate matches the name of the requested server. Otherwise, the user may be warned of a name mismatch and manually accept the risk if security policy allows this exception.

To illustrate this point, consider the example below that depicts load balancing for the ISE Sponsor Portal, a secure web service.

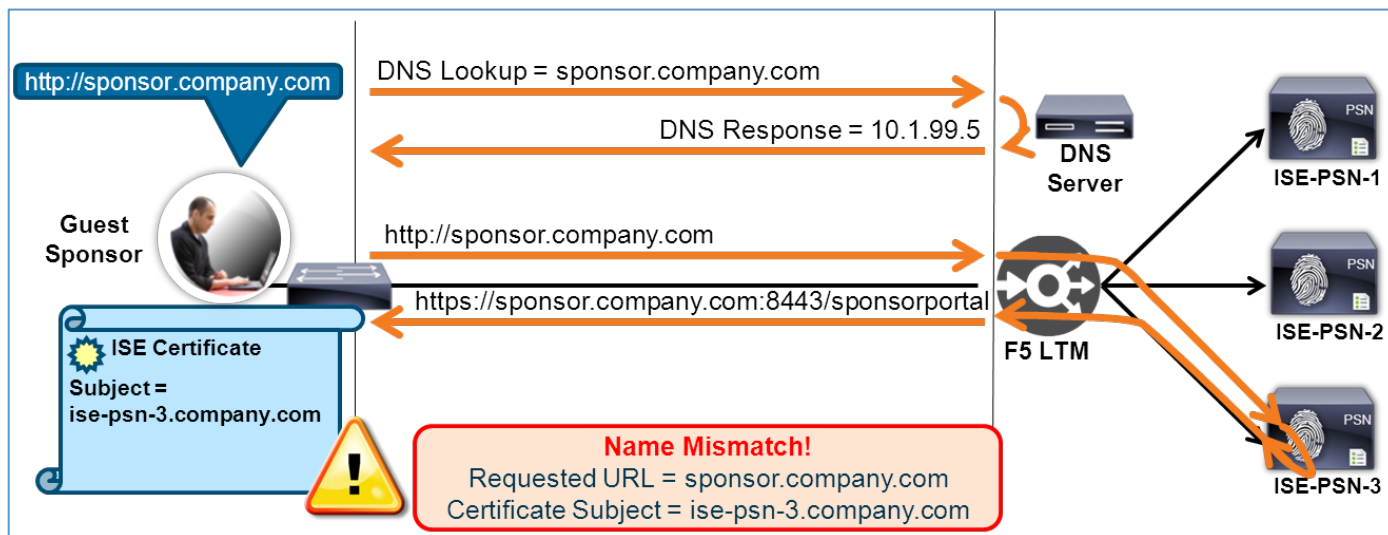


Figure 19. PSN Load Balancing Certificate Mismatch Example

The employee is given the URL of `https://sponsor.company.com` for creating new guest accounts. When the URL is entered into the employee’s browser, DNS will resolve the FQDN to the Virtual Server IP on the BIG-IP LTM. The web request is directed to ISE-PSN-3 and the PSN presents its HTTPS certificate to the employee’s browser. The server certificate includes the PSN’s identity, but this name is different than the one the employee attempted to access, so a certificate warning is presented to warn the user of the discrepancy.

To avoid certificate failures and warnings, it is important to configure the ISE PSN nodes with certificates that will be trusted. Customers can pre-provision clients with the individual certificates needed for trust based on the service, but this is often management intensive. An alternative is to deploy a PSN server certificate that is universal; in other words, a certificate that can be deployed to multiple PSNs and be trusted by each client for EAP or HTTPS access.

The diagram below shows the same scenario where the PSNs share the same server certificates that include the FQDN for all servers and services required in the Subject Alternative Name (SAN) field of the certificate.

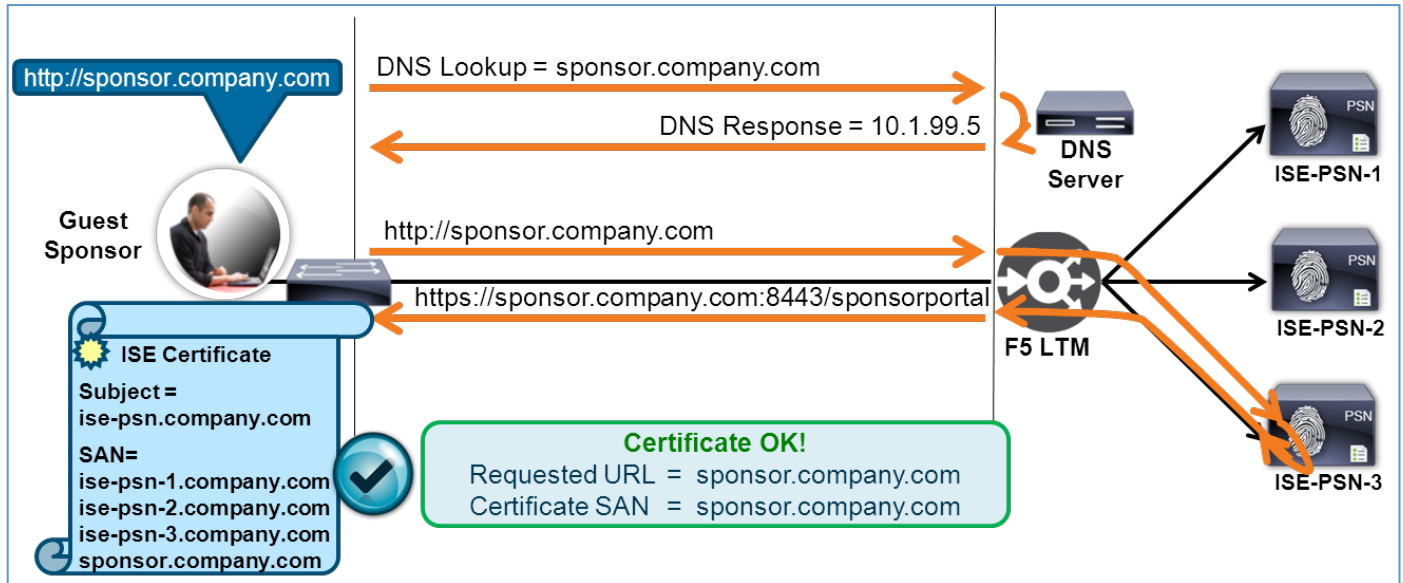


Figure 20. PSN Load Balancing Certificate Match Example

The certificate shown in the diagram is an example of a Unified Communications Certificate (UCC) or Multi-SAN certificate. This type of “universal” certificate can be deployed to each PSN in the cluster and contains the FQDN of each node, but also requires update if new nodes or services are added. An alternative to a UCC is a wildcard certificate. Traditionally, wildcard certificates have a Subject CN value that uses an asterisk (*) followed by the company domain/subdomain name as in *.company.com. An option offered by some SSL Providers is to allow this wildcard domain name to be present in the SAN field and a static entry such as ise.company.com in the Subject CN. It has been found that this combination offers the most flexibility and compatibility with different client operating systems and use cases.

Note: Each customer should carefully evaluate the use of UCC or wildcard certificates for their appropriateness and applicability. There are many factors that need to be considered when choosing digital certificates for production use. This will often be a balance between corporate security policy, risk, cost, supportability, productivity, and end user experience.

Be sure that you include DNS entries for all FQDNs referenced in the server certificate. In the case of load-balanced FQDNs, these entries should resolve to the Virtual Server IP address on the F5 BIG-IP LTM.

The following procedures are intended to serve as a brief overview of the steps required to generate a Certificate Signing Request (CSR) for either a UCC or “Wildcard SAN” certificate. Although the use of self-signed certificates may be appropriate for lab and proof of concept testing, they are often not suitable for production use. Furthermore, it is common for customers to have ISE certificates signed by a public CA to avoid certificate trust warnings for non-employees while using a private CA to sign ISE and client certificates for client certificate provisioning and authentication using EAP-TLS.

ISE 1.2 supports one certificate for all HTTPS authentications to the ISE node and another certificate for all EAP authentications. ISE 1.3 supports unique HTTPS certificates per portal.

Generate a CSR for an ISE Server Certificate

Step 1 From the ISE admin interface, navigate to Administration > System > Certificates > Local Certificates and click **Add** from the right panel:

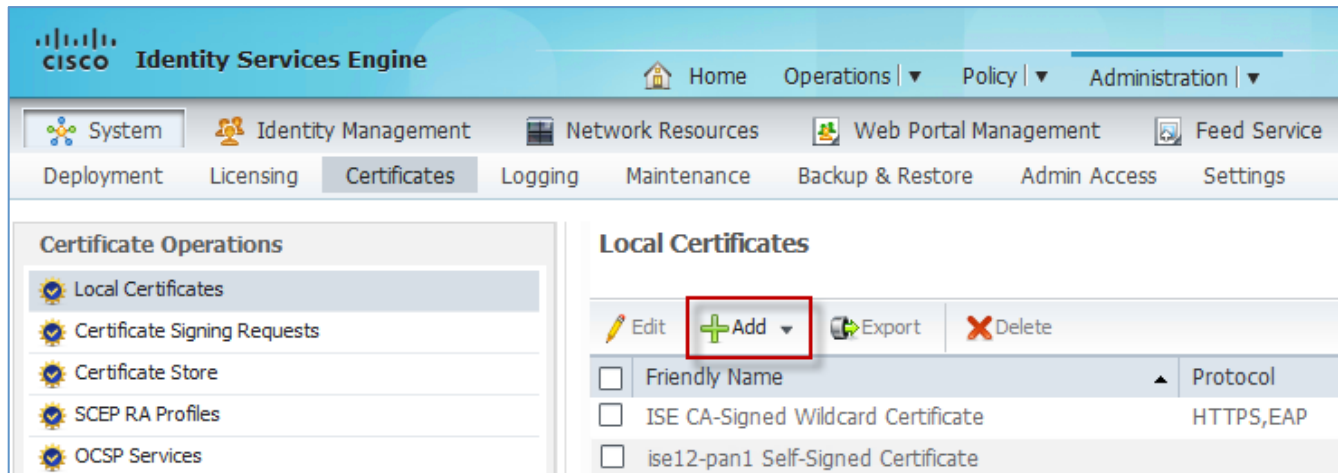


Figure 21. Generate CSR for ISE Server Certificate

Step 2 Select Generate Certificate Signing Request from the drop-down menu.

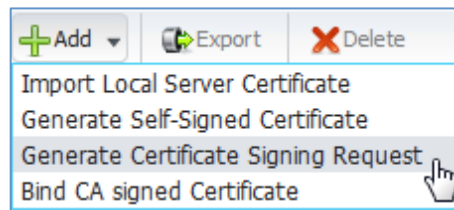


Figure 22. Select ISE CSR Operation

Step 3 Complete the CSR form. To create a universal certificate for the ISE PSNs, you can enter a generic FQDN under the subject using your specific domain (Example: ise.company.com).

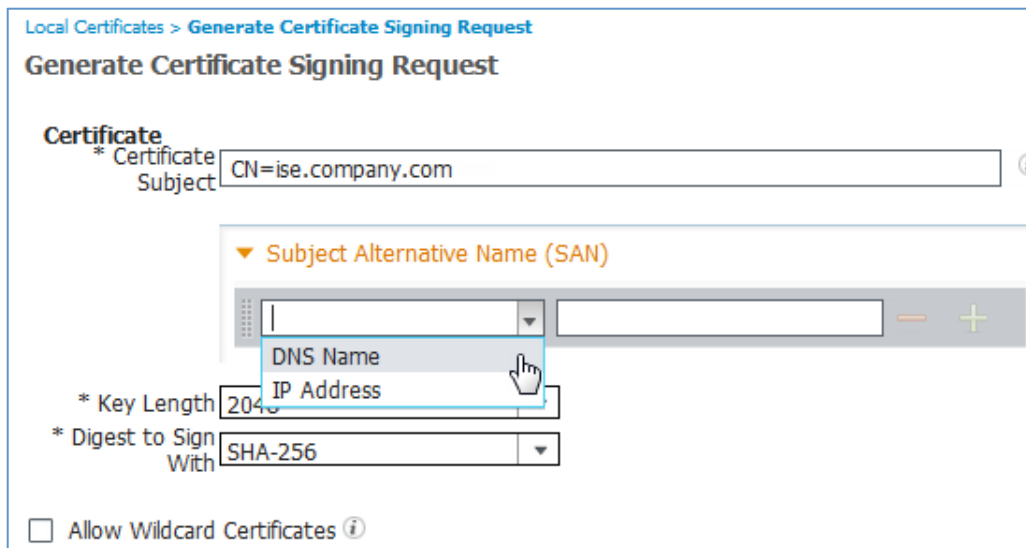


Figure 23. ISE CSR Properties Page

Step 4 Add SAN entries by expanding the Subject Alternative Name (SAN) field. Select **DNS Name** for the field type.

- a. **UCC Certificate:** For a UCC certificate, add the same FQDN as the Subject CN to the SAN field. Use the + icon to the right of new entry to create additional entries. Continue to add SAN entries for all PSN nodes and services such as the Sponsor Portal and My Devices Portal. The FQDN of each PSN node will be included in this list as shown in the example.

Local Certificates > Generate Certificate Signing Request

Generate Certificate Signing Request

Certificate

* Certificate Subject: CN=ise.company.com

▼ Subject Alternative Name (SAN)

DNS Name	ise.company.com	-	+
DNS Name	ise-psn-1.company.com	-	+
DNS Name	ise-psn-2.company.com	-	+
DNS Name	ise-psn-3.company.com	-	+
DNS Name	sponsor.company.com	-	+
DNS Name	mydevices.company.com	-	+

Figure 24. ISE CSR UCC Certificate Example

Depending on policy and certificate usage, the Administration and Monitoring node FQDNs may also be included in the SAN list.

- b. **Wildcard SAN Certificate:** For a certificate with a wildcard in the SAN, start by adding the same FQDN as the Subject CN to the SAN field. Use the + icon to the right of new entry to create an additional entry. Next, add a wildcard entry in the SAN field as shown in the example.

Local Certificates > Generate Certificate Signing Request

Generate Certificate Signing Request

Certificate

* Certificate Subject: CN=ise.company.com

▼ Subject Alternative Name (SAN)

DNS Name	ise.company.com	-	+
DNS Name	*.company.com	-	+

* Key Length: 2048

* Digest to Sign With: SHA-256

Allow Wildcard Certificates

Figure 25. ISE CSR Wildcard SAN Certificate Example

Be sure to check the box Allow Wildcard Certificates.

- Step 5** Set the Key Length and Digest to Sign With values per your security requirements and click **Submit** to complete the form.
- Step 6** Navigate to the Certificate Signing Request section in the left panel, select the newly created CSR, and click **Export**.

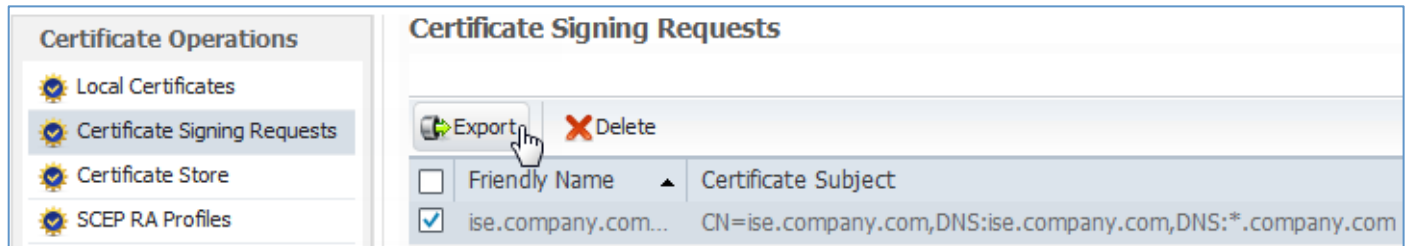


Figure 26. Display ISE Certificate Signing Requests

- Step 7** Sign the exported CSR with a private or public CA.

Note: Be sure to import the signing CA certificate or certificate chain to the Certificate Store on each ISE node to use this certificate. For certificate chains, import each certificate in the chain as an individual cert rather than a single file.

- Step 8** To bind the signed certificate, select the **Bind CA Signed Certificate** option from the drop-down menu in Step 2 (under Local Certificates).

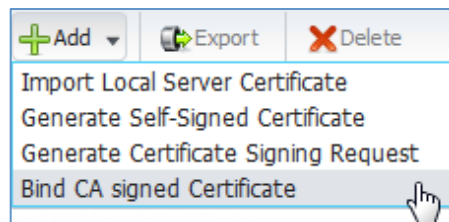


Figure 27. Select Bind CA-Signed Certificate Operation

- Step 9** Complete the form:
- Browse to the CA-signed certificate and upload it to the ISE node.
 - Check the Enable Validation of Certificate Extensions checkbox if policy required RFC-conformance.
 - Check the Allow Wilcard Certificates option as appropriate.
 - Check the required protocols for certificate usage:
 - EAP will select the certificate for use in all EAP authentications.
 - HTTPS will select the certificate for use in all HTTPS communications including web portals and inter-node communications.

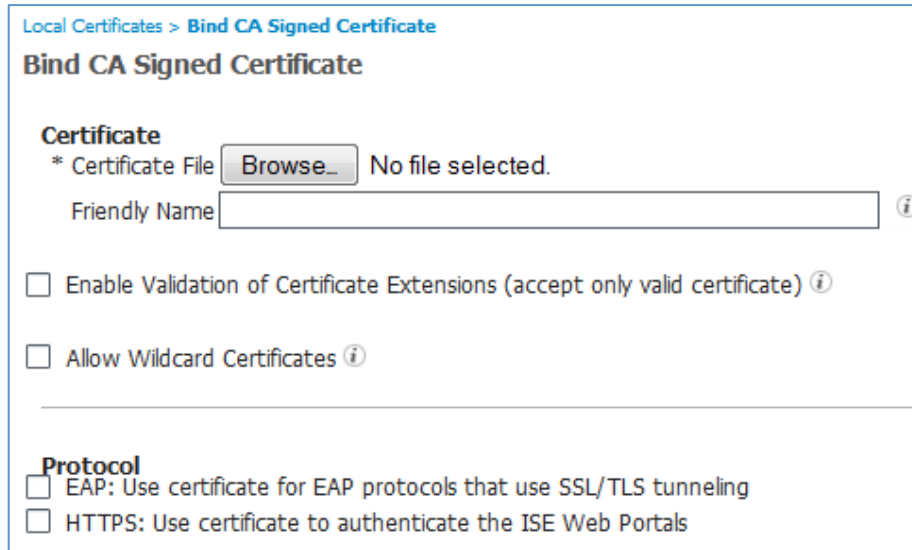


Figure 28. ISE Bind CA-Signed Certificate Properties Page

e. Click **Submit** to install the certificate.

Step 10 To apply the same certificate to other nodes, select the new universal certificate under Local Certificates and click **Export** to export the certificate and private key. Be sure to secure the certificate and private key pair and password!

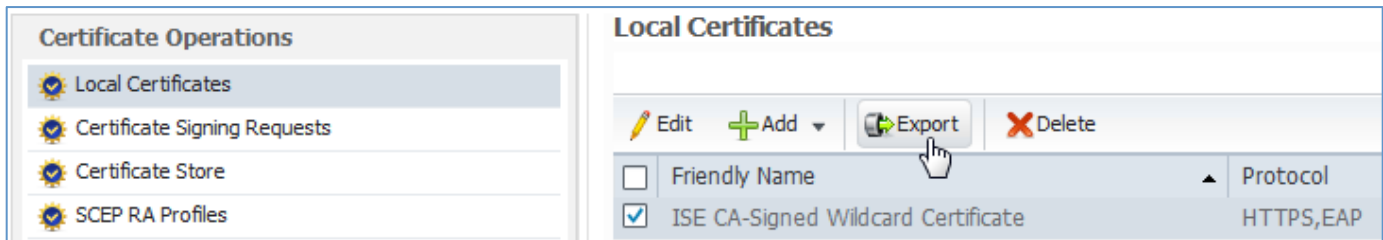


Figure 29. Export ISE Server Certificate

Step 11 Go to the admin interface of the other ISE nodes that will use this certificate and navigate to Administration > System > Certificates > Local Certificates. Select the **Import Local Server Certificate** option from the Add drop-down menu as shown.

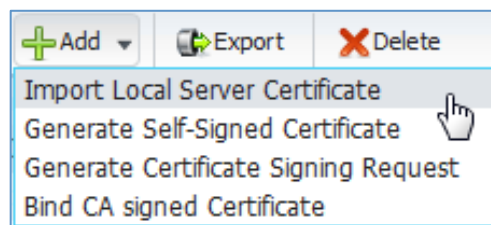


Figure 30. Import ISE Server Certificate

Step 12 Complete the form per Step 8 above.

IP Forwarding for Non-LB traffic

In addition to specific PSN traffic that must be sent directly to the Virtual Server IP address(es) for load balancing, there are a number of flows that do not require load balancing and simply need to be forwarded by the inline F5 appliance. This traffic includes:

- Node communications between PSNs and each Admin and Monitoring node.
- All management traffic to/from the PSN real IP addresses such as HTTPS, SSH, SNMP, NTP, DNS, SMTP, and Syslog.
- Repository and file management access initiated from PSN including FTP, SCP, SFTP, TFTP, NFS, HTTP, and HTTPS.
- All external AAA-related traffic to/from the PSN real IP addresses such as AD, LDAP, RSA, external RADIUS servers (token or foreign proxy), and external CA communications (CRL downloads, OCSP checks, SCEP proxy).
- All service-related traffic to/from the PSN real IP addresses such as Posture and Profiler Feed Services, partner MDM integration, pxGrid, and REST/ERS API communications.
- Client traffic direct to PSN real IP addresses resulting from ISE Profiler (NMAP, SNMP queries) and URL-Redirection such as CWA, DRW/Hotspot, MDM, Posture, and Client Provisioning.
- RADIUS CoA from PSNs to network access devices.

As you can see, there are many flows that are not subject to load balancing. To accommodate this traffic in a fully inline deployment, it is necessary to create a Virtual Server on the F5 appliance that will serve as a catch all for these traffic flows and perform IP forwarding.

Follow the configuration settings in the following table to define two separate IP forwarding servers for inbound and outbound traffic.

Note: Although possible to create a single IP Forwarding Virtual Server for both inbound and outbound traffic, the recommended virtual server configuration outlined below will establish separate inbound and outbound servers to allow traffic to be limited to the PSN nodes connected to the Internal interface.

Table 3. LTM Forwarding IP Configuration

BIG-IP LTM Object	Recommended Setting	Notes
Virtual Server (Inbound) (Main tab > Local Traffic > Virtual Servers > Virtual Server List)		
Note: Create two virtual servers for IP Forwarding—one for Inbound traffic (to PSNs) and one for Outbound traffic (from PSNs)		
Name	<IP Forwarding Server Name> Example: PSN-IP-Forwarding-Inbound	<ul style="list-style-type: none"> • Type the name of the virtual server for IP Forwarding non-load balanced traffic from external hosts to the PSNs.
Type	Forwarding (IP)	<ul style="list-style-type: none"> • Forwarding (IP) allows traffic that does not require load balancing to be forwarded by F5 to the PSNs.

Source	<Source Network Address/Mask> Example: 10.0.0.0/8		<ul style="list-style-type: none"> Type the network address with bit mask for the external network addresses that need to communicate with the ISE PSNs. Make the source as restrictive as possible while not omitting hosts that need to communicate directly to the PSNs. Since this flow is specific to inbound traffic, at a minimum the source should include the management network and ISE Admin and Monitoring nodes.
Destination	Type	Network	
	Address	<Destination Network> Example: 10.1.99.0	<ul style="list-style-type: none"> Enter the PSN network address appropriate to your environment. For added security, make the address range as restrictive as possible.
	Mask	<Destination Mask> Example: 255.255.255.224	<ul style="list-style-type: none"> Enter the PSN network address mask appropriate to your environment. For added security, make the address range as restrictive as possible.
Service Port	* / * All Ports		<ul style="list-style-type: none"> Select the wildcard service port to match all ports by default
Protocol	* All Protocols		<ul style="list-style-type: none"> Select the wildcard protocol to match all protocols by default
VLAN and Tunnel Traffic	Enabled On...		<ul style="list-style-type: none"> Optional: Restrict inbound IP forwarding to specific VLANs.
VLANs and Tunnels	<External VLANs> Example: External		<ul style="list-style-type: none"> Select the ingress VLAN(s) used by external host to communicate with the PSNs.
Virtual Server (Outbound) (Main tab > Local Traffic > Virtual Servers > Virtual Server List)			
Note: Create two virtual servers for IP Forwarding—one for Inbound traffic (to PSNs) and one for Outbound traffic (from PSNs)			
Name	<IP Forwarding Server Name> Example: PSN-IP-Forwarding-Outbound		<ul style="list-style-type: none"> Type the name of the virtual server for IP Forwarding non-load balanced traffic from the PSN servers to external hosts.
Type	Forwarding (IP)		<ul style="list-style-type: none"> Forwarding (IP) allows traffic that does not require load balancing to be forwarded by F5 from the PSNs.
Source	<Source Network Address/Mask Bits> Example: 10.1.99.0/28		<ul style="list-style-type: none"> Enter the PSN network address with bit mask. For added security, make the address range as restrictive as possible.
Destination	Type	Network	

	Address	<Destination Network> Example: 0.0.0.0	<ul style="list-style-type: none"> Enter the network address network appropriate to your environment. Make the destination as restrictive as possible while not omitting hosts that need to communicate directly to the PSNs. It may be unfeasible to limit the destinations, especially if PSNs are enabled for Internet-based Feed Services or cloud-based MDM integration.
	Mask	<Destination Mask> Example: 0.0.0.0	<ul style="list-style-type: none"> Enter the destination network mask appropriate to your environment.
Service Port	* / * All Ports		<ul style="list-style-type: none"> Select the wildcard service port to match all ports by default
Protocol	* All Protocols		<ul style="list-style-type: none"> Select the wildcard protocol to match all protocols by default
VLAN and Tunnel Traffic	Enabled On...		<ul style="list-style-type: none"> Optional: Restrict outbound IP forwarding to specific VLAN.
VLANs and Tunnels	<Internal VLAN> Example: Internal		<ul style="list-style-type: none"> Select the PSN server VLAN used to communicate with external hosts.

Verify the two new Virtual Server IP Forwarding entries. If all protocols were allowed, then it should be possible to ping each of the PSN nodes from an external management network.

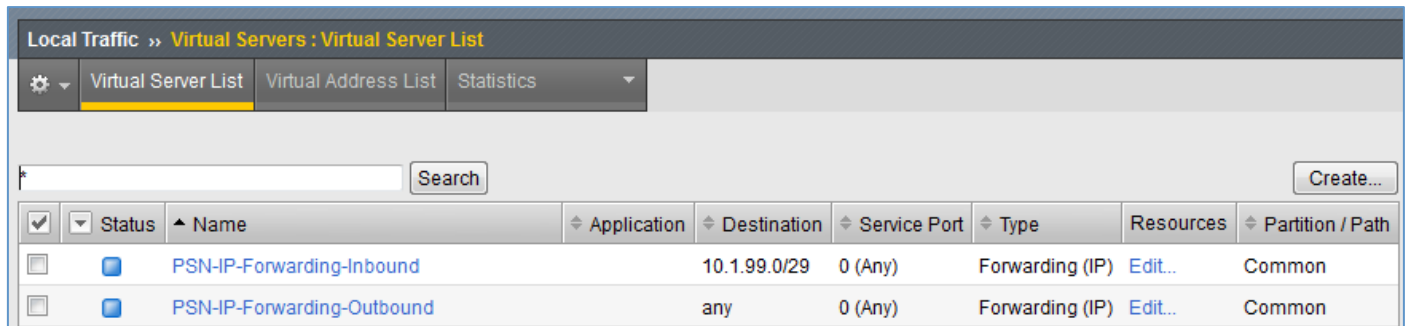


Figure 31. Forwarding IP Virtual Server List

Load Balancing RADIUS

NAT Restrictions for RADIUS Load Balancing

A common load balancing option is to have the F5 appliance perform source network address translation, also known as source NAT, or SNAT, on traffic sent to the Virtual IP address. This method can simplify routing since the real servers see the load balancer as the source of all traffic and consequently reply directly to the load balancer’s IP address whether the appliance is fully or partially in-line to the traffic flow. Unfortunately, this option is not suitable for use with ISE RADIUS AAA services when Change of Authorization (CoA) is required.

RADIUS CoA is used to allow the RADIUS server to trigger a policy server action including reauthentication, termination or updated authorization against an active session. In an ISE deployment, CoA is initiated by the PSN and sent to the NAD to which the authenticated user/device is connected. The NAD IP address is determined by the source IP address of RADIUS authentication requests, a field in the IP packet header, not a RADIUS attribute such as NAS-IP-Address.

For this reason, **SNAT of RADIUS traffic from the NAD is not compatible with RADIUS CoA in an ISE deployment.** With SNAT of RADIUS AAA traffic, PSNs see the load balancer IP address as the source of RADIUS requests and treat it as the NAD that manages the client session. As a result, RADIUS CoA requests are sent directly to the BIG-IP LTM and dropped.

The ISE Live Authentication log below shows an example of this situation.

Status	Identity	Endpoint ID	IP Address	Network Device	Session ID	Event
❌		7C:6D:62:E3:D5:05		f5-bigip	0a012c5a000000f154199b09	RADIUS Request dropped
❌		7C:6D:62:E3:D5:05		f5-bigip	0a012c5a000000f154199b09	Dynamic Authorization failed
ⓘ	employee1	7C:6D:62:E3:D5:05	10.1.40.101		0a012c5a000000f154199b09	Session State is Started
✅	employee1	7C:6D:62:E3:D5:05		f5-bigip	0a012c5a000000f154199b09	Authentication succeeded

Figure 32. Failed RADIUS CoA Due to SNAT – Part 1

Note that the F5 BIG-IP LTM appears as the source of RADIUS requests instead of the true network access device, a Cisco WLC. After a user was successfully authenticated, a CoA (a Dynamic Authorization request) was initiated and sent to the NAD which in this case is the BIG-IP LTM appliance. The more detailed failure reason in log below reveals the error is due to lack of response from the LTM appliance to the CoA request.

Event	Failure Reason
RADIUS Request dropped	11213 No response received from Network Access Device after sending a Dynamic Authorization request
Dynamic Authorization failed	11215 No response has been received from Dynamic Authorization Client in ISE
Session State is Started	
Authentication succeeded	

Figure 33. Failed RADIUS CoA Due to SNAT – Part 2

Note: A later section in this guide covers a different scenario whereby RADIUS CoA traffic initiated from PSNs to the NAD may be Source NATted. This particular scenario should not be confused with the above restriction which specifically applies to SNAT of NAD-initiated RADIUS traffic.

RADIUS Persistence

Persistence, also known as “sticky” or “stickiness” allows traffic matching specific criteria to be load balanced (or “stick”) to the same real server for processing.

To allow the PSN to properly manage the lifecycle of a user/device session, ISE requires that RADIUS Authentication and Authorization traffic for a given session be established to a single PSN. This includes additional RADIUS transactions that may occur during the initial connection phase such as reauthentication following CoA.

It is advantageous for this persistence to continue after initial session establishment to allow reauthentications to leverage EAP Session Resume and Fast Reconnect cache on the PSN. Database replication due to profiling is also optimized by reducing the number of PSN ownership changes for a given endpoint.

RADIUS Accounting for a given session should also be sent to the same PSN for proper session maintenance, cleanup and resource optimization. Therefore, it is critical that persistence be configured to ensure RADIUS Authentication, Authorization, and Accounting traffic for a given endpoint session be load balanced to the same PSN.

Sticky Methods for RADIUS

F5 BIG-IP LTM supports different methods to configure persistence including:

- **Persist Attribute** (configured under the RADIUS Service Profile).
- **Default Persistence Profile** and **Fallback Persistence Profile** (specified under the Virtual Server Resources). Persistence Profiles further allow the specification of an iRule that defines persistence logic.

The recommended method for ISE RADIUS load balancing is the iRule option. Although the Persist Attribute option is simple and may be sufficient in some deployments, the iRule method is recommended as it offers superior processing capabilities based on multiple attributes, fallback logic, and options to log events for advanced troubleshooting.

Note: If persistence is configured under both the RADIUS Service Profile and Default Persistence Profile, then the RADIUS Service Profile takes precedence. If the RADIUS Service Profile references an iRule for persistence, the iRule takes precedence.

Sticky Attributes for RADIUS

There are numerous attributes that F5 can use for persistence including, but not limited to, RADIUS attributes (Calling-Station-ID, Framed-IP-Address, NAS-IP-Address, IETF or Cisco Session ID) or Source IP Address. The source IP address is typically the same as the IP address of the RADIUS client (the NAD) or RADIUS NAS-IP-Address.

Cisco’s Audit Session ID (also known as CPM Session ID) is a unique value that is calculated by the NAD based on its NAS-IP-Address, an incrementing counter value, and the session start timestamp. Unlike the RFC 2866 [Acct-Session-Id](#) that may change over re-authentications, the Audit Session ID can be carried over multiple RADIUS reauthentications, each which needs to be sent to the same PSN for processing. Although a reasonable choice for most Cisco access devices, it is not suitable for all devices. Additionally, it is possible in some scenarios that the Audit

Session ID is renegotiated by the NAD during client reauthentication attempts, for example during a failed wireless roam to a new access point or controller.

NAS-IP-Address or Source IP address may be reasonable choices where there are numerous network access devices (RADIUS clients) but only few clients per NAD. Under these conditions one may expect reasonable load distribution. However, for cases where many clients connect to a single NAD, then persistence on NAD IP address will likely result in over-loading of specific PSNs.

Calling-Station-ID is a common attribute across many RADIUS authentication methods and is based on a unique endpoint. This value does not change across multiple connection attempts using the same network adapter. Therefore, this attribute is the recommended persistence attribute.

There are some cases where the Calling-Station-ID value is not populated such as certain 3rd-party NADs, so it is recommended to have a fallback persistence method defined in such cases. Framed-IP-Address (typically the client IP address) and/or NAS-IP-Address/Source IP Address are suitable choices.

The recommended persistence attribute for ISE RADIUS load balancing is Calling-Station-ID with the option to use Framed-IP-Address as an adjunct to Calling-Station-Id. Source IP address or NAS-IP-Address is recommended fallback methods. Joining Framed-IP-Address to the primary attribute can allow non-RADIUS traffic sourced from the same end user/device to be load balanced to the same PSN.

Example F5 BIG-IP LTM iRules for RADIUS Persistence

This section highlights working iRule examples for RADIUS Persistence.

RADIUS Persistence iRule Example #1: radius_mac_sticky

This is the generally recommended iRule and is based on RADIUS Calling-Station-Id as the primary persistence attribute. If the Calling-Station-Id attribute is not populated, then the persistence falls back to the RADIUS NAS-IP-Address attribute.

```
# ISE persistence iRule based on Calling-Station-Id (MAC Address) with fallback to NAS-
IP-Address as persistence identifier

when CLIENT_DATA {
  # 0: No Debug Logging  1: Debug Logging
  set debug 1

  # Persist timeout (seconds)
  set nas_port_type [RADIUS::avp 61 "integer"]
  if {$nas_port_type equals "19"}{
    set persist_ttl 3600
    if {$debug} {set access_media "Wireless"}
  } else {
    set persist_ttl 28800
    if {$debug} {set access_media "Wired"}
  }

  # If MAC address is present - use it as persistent identifier
  # See Radius AV Pair documentation on
https://devcentral.f5.com/wiki/irules.RADIUS\_\_avp.ashx
  if {[RADIUS::avp 31] ne "" }{
    set mac [RADIUS::avp 31 "string"]

    # Normalize MAC address to upper case
```

```

    set mac_up [string toupper $mac]
    persist uie $mac_up $persist_ttl
    if {$debug} {
        set target [persist lookup uie $mac_up]
        log local0.alert "Username=[RADIUS::avp 1] MAC=$mac Normal MAC=$mac_up
MEDIA=$access_media TARGET=$target"
    }

} else {
    set nas_ip [RADIUS::avp 4 ip4]
    persist uie $nas_ip $persist_ttl
    if {$debug} {
        set target [persist lookup uie $nas_ip]
        log local0.alert "No MAC Address found - Using NAS IP as persist id.
Username=[RADIUS::avp 1] NAS IP=$nas_ip MEDIA=$access_media TARGET=$target"
    }
}
}
}

```

Since the persistence TTL value is set, it will take precedence over the Persistence Profile timeout setting. The iRule also includes a logging option to assist with debugging. Set the debug variable to “1” to enable debug logging. Set the debug variable to “0” to disable debugs logging.

Here is sample output when these log statements are enabled (not commented out using hash):

```

Sat Sep 27 13:55:44 EDT 2014  alert f5      tmm[9443]
Rule /Common/radius_mac_sticky <CLIENT_DATA>: Username=6C-20-56-13-E9-FC
MAC=6C-20-56-13-E9-FC Normal MAC=6C-20-56-13-E9-FC MEDIA=Wired TARGET=

Sat Sep 27 13:55:43 EDT 2014  alert f5      tmm[9443]
Rule /Common/radius_mac_sticky <CLIENT_DATA>: Username=6c205613e9fc
MAC=6C-20-56-13-E9-FC Normal MAC=6C-20-56-13-E9-FC MEDIA=Wired
TARGET=/Common/radius_auth_pool 10.1.99.6 1812

Sat Sep 27 13:55:40 EDT 2014  alert f5      tmm[9443]
Rule /Common/radius_mac_sticky <CLIENT_DATA>: Username=employee1
MAC=7c-6d-62-e3-d5-05 Normal MAC=7C-6D-62-E3-D5-05 MEDIA=Wireless
TARGET=/Common/radius_acct_pool 10.1.99.7 1813

Sat Sep 27 13:55:40 EDT 2014  alert f5      tmm[9443]
Rule /Common/radius_mac_sticky <CLIENT_DATA>: Username=employee1
MAC=7c-6d-62-e3-d5-05 Normal MAC=7C-6D-62-E3-D5-05 MEDIA=Wireless
TARGET=/Common/radius_acct_pool 10.1.99.7 1813

Sat Sep 27 13:55:39 EDT 2014  alert f5      tmm[9443]
Rule /Common/radius_mac_sticky <CLIENT_DATA>: Username=employee1
MAC=7c-6d-62-e3-d5-05 Normal MAC=7C-6D-62-E3-D5-05 MEDIA=Wireless TARGET=

Sat Sep 27 13:55:39 EDT 2014  alert f5      tmm[9443]
Rule /Common/radius_mac_sticky <CLIENT_DATA>: Username=employee1
MAC=7c-6d-62-e3-d5-05 Normal MAC=7C-6D-62-E3-D5-05 MEDIA=Wireless TARGET=

Sat Sep 27 13:55:39 EDT 2014  alert f5      tmm[9443]
Rule /Common/radius_mac_sticky <CLIENT_DATA>: Username=employee1
MAC=7c-6d-62-e3-d5-05 Normal MAC=7C-6D-62-E3-D5-05 MEDIA=Wireless TARGET=

Sat Sep 27 13:55:38 EDT 2014  alert f5      tmm[9443]

```

```

Rule /Common/radius_mac_sticky <CLIENT_DATA>: Username=00-50-56-A0-0B-3A
MAC=00-50-56-A0-0B-3A Normal MAC=00-50-56-A0-0B-3A MEDIA=Wired TARGET=

Sat Sep 27 13:55:37 EDT 2014 alert f5 tmm[9443]
Rule /Common/radius_mac_sticky <CLIENT_DATA>: No MAC Address found
- Using NAS IP as persist id. Username=#ACSACL#-IP-CENTRAL_WEB_AUTH-5334c9a5
NAS IP=10.1.50.2 MEDIA=Wired TARGET=

Sat Sep 27 13:55:37 EDT 2014 alert f5 tmm[9443]
Rule /Common/radius_mac_sticky <CLIENT_DATA>: Username=005056a00b3a
MAC=00-50-56-A0-0B-3A Normal MAC=00-50-56-A0-0B-3A MEDIA=Wired TARGET=

```

RADIUS Persistence iRule Example #2: radius_macip_sticky

This iRule is also based on Calling-Station-Id as the primary persistence attribute but also includes the Framed-IP-Address as a second identifier that allows RADIUS packets that include the Framed-IP-Address but not the Calling-Station-Id to maintain persistence to the same server. It can also server to stick packets sourced from this IP address to be sent to the same PSN. This could be used in an SSL Offload case where clients are redirected to an F5 Virtual Server IP rather than to a specific PSN. By sending the traffic to the F5 for SSL termination, additional security and traffic policies can be applied to the packet before a new connection is established to the real PSN.

```

# ISE persistence iRule based on Calling-Station-Id (Client MAC Address) and Framed-IP-
Address (Client IP address)

when CLIENT_ACCEPTED {
  set framed_ip [RADIUS::avp 8 ip4]
  set calling_station_id [RADIUS::avp 31 "string"]
  # log local0. "Request from $calling_station_id:$framed_ip"
  persist uie "$calling_station_id:$framed_ip"
}

```

Fragmentation and Reassembly for RADIUS

When persistence is based on a RADIUS attribute within the UDP packet, it is critical that the load balancer reassembles the IP fragments in order for the load balancer to make the correct PSN forwarding decision. Otherwise, large RADIUS packets such as those containing certificates for EAP-TLS may be fragmented and load balanced using a fallback mechanism. This can cause fragments to be sent to different PSNs and result in client authentication failures.

Fortunately, “When a BIG-IP virtual server receives an IP fragment, the Traffic Management Microkernel (TMM) queues the packet and waits to collect and reassemble the remaining fragments into the original message. TMM does not generate a flow for the fragment until TMM reassembles and processes the entire message. If part of the message is lost, the BIG-IP system discards the fragment.” For more information, see F5 support article [SOL9012: The BIG-IP LTM IP fragment processing](#).

Load balancing using type FastL4 is an exception to the above behavior whereby IP fragment reassembly must be explicitly enabled under the FastL4 Protocol Profile. Current recommendation is to use Standard as the load balancing type so fragmentation/reassembly of UDP RADIUS packets should not be an issue.

Persistence Timeout for RADIUS

F5 defines a Persistence Timeout, or Time to Live (TTL), that controls the duration that a given persistence entry should be cached. Once expired, a new packet without a matching entry can be load balanced to a different server.

In an ISE deployment, it is recommended that RADIUS for a given session be load balanced to the same PSN even after initial session establishment to optimize session maintenance and profiling database replication. Therefore, a longer persistence timeout is generally proposed for RADIUS. A value of five minutes (300 seconds) should be adequate for most deployments to cover the initial session establishment. If ISE services like posture and onboarding are deployed, then 10 or 15 minutes may be necessary to cover the initial assessment, provisioning and remediation phase. If EAP Session Resume or Profiling Services are enabled, then even longer timeouts are recommended, say one hour (3600 seconds) for wireless and eight hours (28800 seconds) for wired deployments. These longer persistence intervals will optimize authentication performance, general session lifecycle maintenance, and profiling data replication.

Note: A side effect of longer persistence timeouts is that it may take longer for existing sessions to be load balanced to a newly added server. The persistence timers for existing sessions will need to expire or be cleared before they can be load balanced to the new PSN. Based on load balancing method such as Least Connections, it is likely that a majority of new sessions will be sent to the new PSN until load increases and is commensurate with other PSNs.

The persistence timeout setting ultimately depends on the network environment. For highly mobile environments where the average connect time to the network is much lower, then a lower persistence setting may be more appropriate to more closely match the expected connect time. In more static environments like a wired LAN that includes mostly immobile endpoints, much longer persistence timeouts can be set.

Note: It is possible to configure separate Virtual Servers with different persistence timeouts. It is also possible to leverage F5 LTM iRules to change the persistence TTL based on a RADIUS attribute like Network Device Group Type or Location.

The persistence timeout can be set directly under the Persistence Profile or through an iRule named under the Persistence Profile. If both are configured, the iRule takes precedence.

NAD Requirements for RADIUS Persistence

In order to apply persistence based on specific attributes in a RADIUS packet, it is necessary that each NAD properly populates these attributes with the expected data and format.

Cisco Catalyst Switches

By default, Cisco Catalyst switches populate the RADIUS Calling-Station-ID attribute with the MAC address of the wired hosts connected to its switchports. There are some cases where it may be desirable to supplement the information sent in RADIUS requests. The following are some examples:

Table 4. RADIUS Attributes for Cisco Catalyst Switches

Cisco Catalyst IOS Command	Description
radius-server attribute 8 include-in-access-req	Include Framed-IP-Address (if available) in RADIUS Access Requests
radius-server attribute 31 send nas-port-detail	Include client IP address for remote console (vty) connections to the switch
radius-server attribute 31 mac format ietf upper-case	Set the MAC address format to 00-00-40-96-3E-4A (all upper case letters)

Cisco Wireless LAN Controllers

By default, Cisco Wireless LAN Controllers populate the RADIUS Calling-Station-ID attribute with the MAC address of the wireless clients when RADIUS NAC is enabled on the WLAN. There are some deployments that use Local Web Authentication (LWA) where RADIUS NAC is not enabled. In these cases, if the Auth Call-Station-ID attribute is set to IP address, then the Calling-Station-Id uses the client IP address rather than the MAC address. This can break persistence for RADIUS. The diagram depicts the typical settings to ensure client MAC is populated in the Calling-Station-Id for most cases.

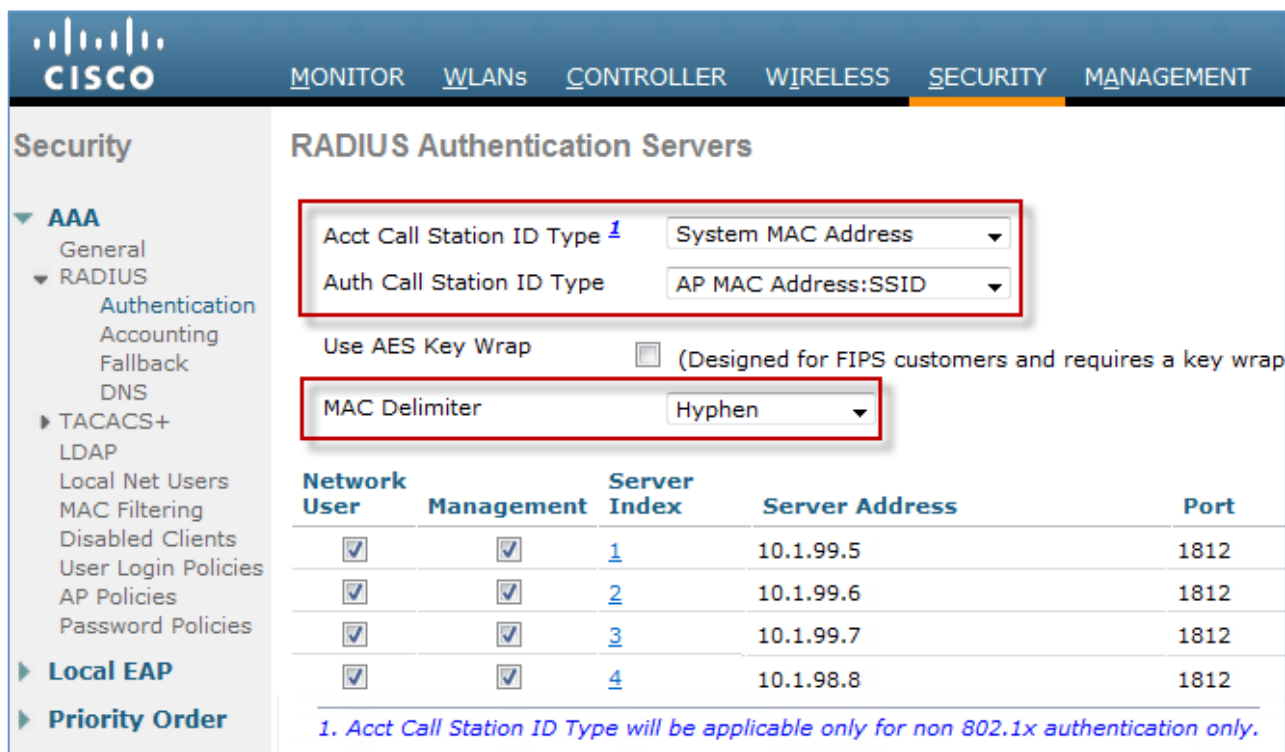


Figure 34. RADIUS Attributes for Cisco Wireless Controllers

Note: WLC versions prior to 7.6 may not display separate entries for Auth and Accounting Call Station ID. In those versions, the single entry will specify the format for Authentication and Authorization requests.

For reference, the RADIUS NAC setting is required to ensure that the Cisco Audit Session ID is presented in the RADIUS request. It is configured under the WLAN settings in the Advanced tab as shown in the figure.

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'employee'

General Security QoS Policy-Mapping **Advanced**

Allow AAA Override <input checked="" type="checkbox"/> Enabled Coverage Hole Detection <input checked="" type="checkbox"/> Enabled Enable Session Timeout <input checked="" type="checkbox"/> 7200 Session Timeout (secs) Aironet IE <input checked="" type="checkbox"/> Enabled Diagnostic Channel <input type="checkbox"/> Enabled Override Interface ACL IPv4 None IPv6 None Layer2 Acl None P2P Blocking Action Disabled Client Exclusion <input checked="" type="checkbox"/> Enabled 180 Timeout Value (secs) Maximum Allowed Clients 0 Static IP Tunneling <input type="checkbox"/> Enabled Wi-Fi Direct Clients Policy Disabled Maximum Allowed Clients 200	DHCP DHCP Server <input type="checkbox"/> Override DHCP Addr. Assignment <input checked="" type="checkbox"/> Required OEAP Split Tunnel (Printers) <input type="checkbox"/> Enabled Management Frame Protection (MFP) MFP Client Protection <input type="checkbox"/> Optional DTIM Period (in beacon intervals) 802.11a/n (1 - 255) 1 802.11b/g/n (1 - 255) 1 NAC NAC State Radius NAC
--	--

Figure 35. RADIUS Attributes for Cisco Wireless Controllers

Cisco ASA Remote Access VPN Servers

By default, Cisco Adaptive Security Appliances (ASAs) populate the RADIUS Calling-Station-ID attribute with the public IP address of the full-tunnel remote access VPN client. The real client MAC address is not available to the ASA since the connection is over an L3 IP connection.

For other Cisco and non-Cisco RADIUS NADs, you can view the contents of the various RADIUS attributes from the NAD logs, ISE authentication detail logs, or packet captures.

RADIUS Load Balancing Data Flow

The diagram depicts the expected traffic flow for load-balancing RADIUS Authentication, Authorization, and Accounting.

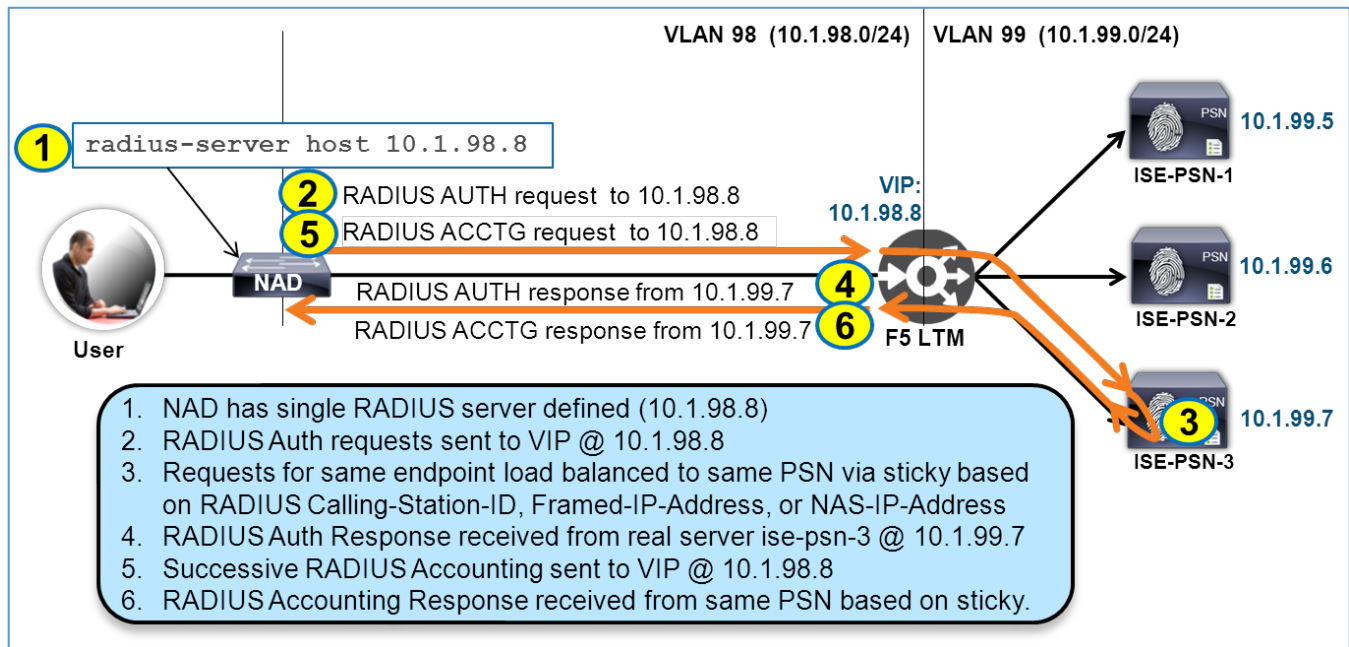


Figure 36. RADIUS Load Balancing Traffic Flow

RADIUS Health Monitoring

F5 Monitors are used to perform periodic health checks against node members in a load-balanced pool. These monitors, or probes, validate that a real server is healthy before sending it requests. The term *healthy* is a relative term which can range in meaning from “Server is IP reachable using ICMP ping” to “Server is actively and successfully responding to simulated application requests; additionally, out-of-band checks validate resources are sufficient to support additional load”.

F5 LTM Monitor for RADIUS

F5 BIG-IP LTM includes a RADIUS Authentication monitor that will be used for monitoring the health of the ISE PSN servers. It will periodically send a simulated RADIUS Authentication request to each PSN in the load-balanced pool and verify that a valid response is received. A valid response can be either an Access-Accept or an Access-Reject. As covered under the ISE prerequisite configuration section, it is critical that the following be configured on the ISE deployment for the F5 LTM health monitor to succeed:

- F5 LTM internal IP address is configured as a RADIUS Network Device
- Matching RADIUS secret key configured under the Network Device definition
- A valid user account in an applicable identity store if want the RADIUS monitor request to return an Access-Accept

This same probe will be used to monitor the members of the RADIUS Accounting pool to reduce the number of RADIUS requests sent to each PSN.

RADIUS Monitor Timers

The Monitor timer determines how frequently the health status probes are sent to each member of a load-balanced pool. Timers should be set short enough to allow failover before a RADIUS request from an access device times out and long enough to prevent excessive and unnecessary load on the ISE PSNs.

The optimal values ultimately depend on the network environment and the RADIUS server configuration on each of the access devices. A reasonable start value for RADIUS timeout on a Cisco WLC Controller ranges from 5-10 seconds with three retries for a total of 20-40 seconds. A typical RADIUS timeout for a Cisco Catalyst switch is approximately 10-15 seconds with two to three retries for a total of 30-60 seconds.

Longer timeouts and retries may be required for switches/routers connected across slower or less reliable WAN links. Other potential causes for RADIUS delays include slow connections to backend identity stores or extensive attribute retrieval from remote directories. Under the authentication log details you may see a Step Latency counter that reveals excessive delays in identity store responses. Slow or misconfigured DNS services can also lead to delayed responses from backend stores. Ideally these issues are addressed to reduce overall RADIUS latency, but it may be necessary to set higher values on network access devices as an interim solution.

So how does all of this relate to F5 LTM RADIUS Health Monitors? The goal is to set the F5 LTM monitor timers such that they detect PSN failure and try another PSN before the NAD RADIUS request times out. Otherwise, the F5 BIG-IP LTM will continue to send requests to the same failed PSN until the configured monitor interval is exceeded. For example, if the total NAD RADIUS timeout is 40 seconds, the interval may need to be set to 31 seconds. At the same time, setting an interval of 11 seconds will likely be too excessive and simply cause unnecessary RADIUS authentication load on each of the PSNs. If RADIUS timers differ significantly between groups of NADs or NAD types, it is recommended to use the lower settings to accommodate all NADs using the same RADIUS Virtual Servers.

Note: Be sure to take into consideration whether the test RADIUS account used by the F5 LTM Monitor is an internal ISE user account, or one that must be authenticated to an external identity store as this will impact total RADIUS response time. For more details on user account selection, refer to the section User Account Selection for RADIUS Probes.

The F5 LTM RADIUS Monitor has two key timer settings:

- Interval = probe frequency (default = 10 sec)
- Timeout = total time before monitor fails (default = 31 seconds)

Therefore, we can deduce that four health checks are attempted before declaring a node failure:

- $\text{Timeout} = (3 * \text{Interval}) + 1$

Sample LTM Monitor configuration for RADIUS:

```
ltm monitor radius /Common/radius_1812 {
    debug no
    defaults-from /Common/radius
    destination *:1812
    interval 10
    password P@$w0rd
    secret P@$w0rd
    time-until-up 0
    timeout 31
    username f5-probe
}
```

}

User Account Selection for RADIUS Probes

The RADIUS Monitor requires that a user account be configured to send in the periodic RADIUS authentication request. This raises the question of which account to use—A user defined in the ISE Internal User database? An external user in Microsoft AD, LDAP directory, or other identity store? Or simply a non-existent account?!

Another decision is based on the security of the user account. It is important that this user account only be used to validate the PSNs are successfully processing RADIUS requests. No access should be available to this account in the event the credentials are leaked and used for access to secured resources. This may be a reason to choose an invalid user account so that an Access-Reject is returned. As noted, the BIG-IP LTM will deem this response as valid in determining health status since it must have been processed by the PSN's RADIUS server.

An alternative to the above method is to use a valid account, but to be sure that no access privileges are granted to the authenticated user. ISE controls these permissions using the Authorization Policy. The PSN can authenticate the probe user (Access-Accept), but also return a RADIUS Authorization that explicitly denies access. For example, an Access Control List (ACL) that returns 'deny ip any any' could be assigned, or an unused/quarantine VLAN. Further, the Authentication and Authorization Policy rule should specifically limit the probe user account to the F5 IP address or other conditions (authentication protocol, service type, network device group, etc) that limit where account is expected.

General guidance is to use the ISE Internal User database account with different password to force Access-Reject, unless validation of an external user account is required to verify backend database operation. This requirement may stem from the premise that "If the PSN cannot authenticate to my identity store, then it is as good as down even if RADIUS is functioning".

If AD/LDAP account validation is required as terms for determining RADIUS status, then it is recommended to return Access-Accept when the identity store is available and to lock down authorization for probe account as noted. There are implications to RADIUS failover that need to be considered on backend store failure, i.e. return Process Error versus Access-Reject and potential impact to the load balancing cluster as a whole. If AD/LDAP is down for all PSNs, then the NADs need to failover to different cluster since the VIP will be declared down.

ISE Filtering and Log Suppression

After properly configuring the RADIUS Monitor checks you are overjoyed by the friendly green icons under the F5 Pool List or Pool Member List that signify your success and a healthy RADIUS server farm...

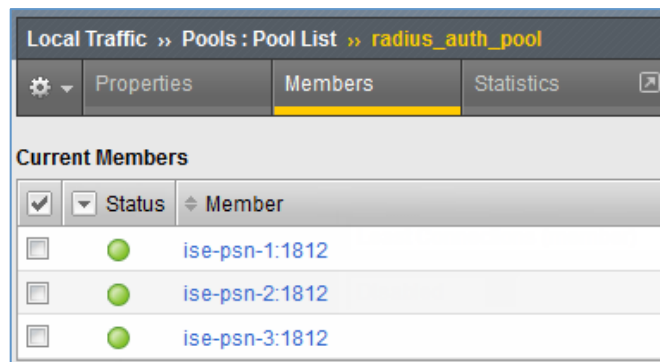


Figure 37. Validating Health Monitors for RADIUS Load Balancing

Your joy is diminished once you return to the ISE Live Authentications dashboard to find the consequence of your success...
















Time	Status	Details	Repeat Count	Identity	Network Device	Server	Authorization Pr...	Event	Auth Method
2014-09-17 14:25:34.825	✓			f5-probe	f5-bigip	ise12-psn3	RADIUS_Probes	Authentication succeeded	PAP_ASCII
2014-09-17 14:25:33.830	✓			f5-probe	f5-bigip	ise12-psn1	RADIUS_Probes	Authentication succeeded	PAP_ASCII
2014-09-17 14:25:32.823	✓			f5-probe	f5-bigip	ise12-psn2	RADIUS_Probes	Authentication succeeded	PAP_ASCII
2014-09-17 14:25:12.912	✓			f5-probe	f5-bigip	ise12-psn2	RADIUS_Probes	Authentication succeeded	PAP_ASCII
2014-09-17 14:25:24.807	✓			f5-probe	f5-bigip	ise12-psn3	RADIUS_Probes	Authentication succeeded	PAP_ASCII
2014-09-17 14:25:23.820	✓			f5-probe	f5-bigip	ise12-psn1	RADIUS_Probes	Authentication succeeded	PAP_ASCII
2014-09-17 14:25:44.829	✓			f5-probe	f5-bigip	ise12-psn3	RADIUS_Probes	Authentication succeeded	PAP_ASCII
2014-09-17 14:25:14.910	✓			f5-probe	f5-bigip	ise12-psn3	RADIUS_Probes	Authentication succeeded	PAP_ASCII
2014-09-17 14:25:13.912	✓			f5-probe	f5-bigip	ise12-psn1	RADIUS_Probes	Authentication succeeded	PAP_ASCII
2014-09-17 14:25:02.883	✓			f5-probe	f5-bigip	ise12-psn2	RADIUS_Probes	Authentication succeeded	PAP_ASCII
2014-09-17 14:25:04.893	✓			f5-probe	f5-bigip	ise12-psn3	RADIUS_Probes	Authentication succeeded	PAP_ASCII
2014-09-17 14:25:03.909	✓			f5-probe	f5-bigip	ise12-psn1	RADIUS_Probes	Authentication succeeded	PAP_ASCII
2014-09-17 14:24:53.896	✓			f5-probe	f5-bigip	ise12-psn1	RADIUS_Probes	Authentication succeeded	PAP_ASCII
2014-09-17 14:24:54.882	✓			f5-probe	f5-bigip	ise12-psn3	RADIUS_Probes	Authentication succeeded	PAP_ASCII
2014-09-17 14:24:52.893	✓			f5-probe	f5-bigip	ise12-psn2	RADIUS_Probes	Authentication succeeded	PAP_ASCII

Figure 38. Authentication Logging for RADIUS Health Monitors

If an invalid user account was used, the above would instead be filled with red events for every probe authentication attempt. In either case, these numerous and repetitive log entries can make it difficult to focus on the items of interest like access attempts by network users and devices.

To filter out the “noise”, it is recommended to enable PSN Collection Filters. Collection Filters allow you to filter out logging of events based on failure/pass status and other conditions including

- User Name
- Policy Set Name
- NAS-IP-Address
- Device-IP-Address
- MAC (Calling-Station-ID)

For BIG-IP LTM monitor checks, a simple Collection Filter can be configured based on Device-IP-Address or NAS-IP-Address that is typically the LTM’s internal interface IP, or else use the User Name of the probe account as shown in the example.

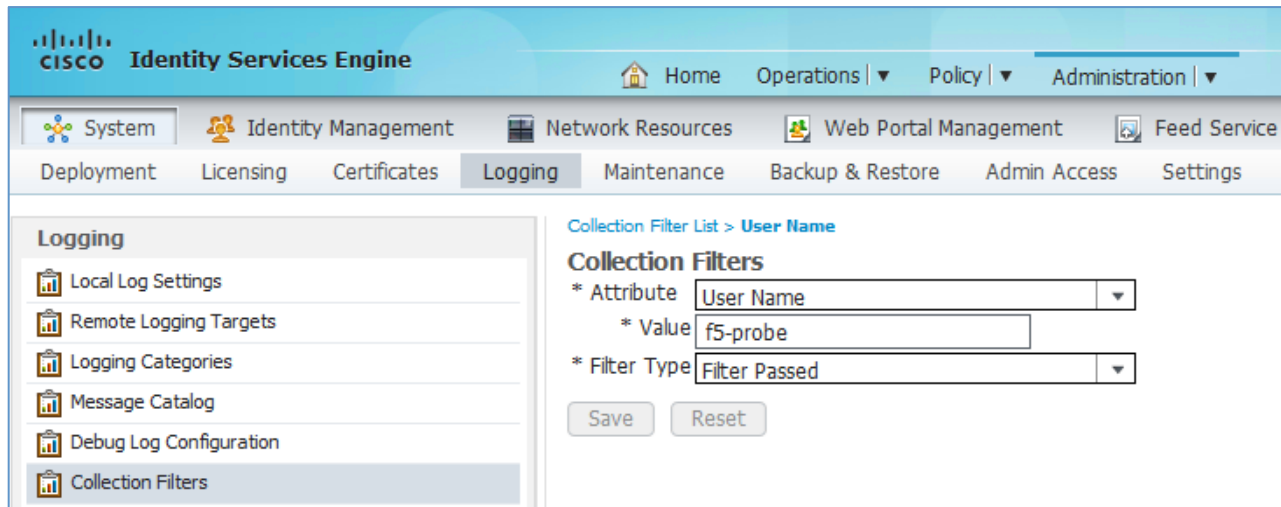


Figure 39. ISE Collection Filters for RADIUS Health Monitors

If the probe user account is expected to fail authentication, then Filter Type should be set to “Filter Failed”. (Collection Filters are configured under **Administration > System > Logging > Collection Filters**).

RADIUS Load Balancing: F5 LTM Configuration Details

This section provides the detailed F5 LTM configuration for RADIUS load balancing of ISE PSN servers including the recommended settings and considerations for each component.

The RADIUS Load Balancing configuration is broken down into the following major components:

- RADIUS Health Monitor
- RADIUS Profiles
 - UDP
 - RADIUS Service
 - RADIUS Persistence
- Pool Lists for Authentication/Authorization and Accounting
- Virtual Servers for RADIUS Authentication/Authorization and Accounting

Use the settings outlined in the table to configure F5 LTM for RADIUS load balancing with ISE PSNs.

Table 5. LTM RADIUS Load Balancing Configuration

BIG-IP LTM Object	Recommended Setting	Notes
Health Monitor (Main tab > Local Traffic > Monitors)		
Name	<RADIUS Monitor Name> Example: radius_1812	• Enter a name for the RADIUS Authentication and Authorization health monitor.
Type	RADIUS	• F5 provides a native monitor for RADIUS Authentication

Timers: Interval and Timeout	<p>Wireless:</p> <p>Interval: 10</p> <p>Timeout: 31</p> <p>Wired:</p> <p>Interval: 15</p> <p>Timeout: 46</p>	<ul style="list-style-type: none"> Timers should be set short enough to allow failover before RADIUS request from access device times out and long enough to reduce excessive logging to the ISE PSNs Recommended Cisco WLC RADIUS Timeout value ranges from 5-10 seconds with 3 retries. A Common RADIUS timeout for a Cisco Catalyst switch is approximately 30-45 seconds total. The longer timeouts and retries may be required for switches/routers connected across slower or less reliable WAN links. Refer to the “RADIUS Monitor Timers” section for additional details.
User Name	<p><ISE User Name></p> <p>Example:</p> <p>f5-probe</p>	<ul style="list-style-type: none"> Type the user name of the ISE user account. The name should match the value configured under <i>Add F5 BIG-IP LTM as a NAD for RADIUS Health Monitoring</i> in the “ISE Configuration Prerequisites” section. See “User Account Selection for RADIUS Probes” section for more details on account selection.
Password	<ISE User Password>	<ul style="list-style-type: none"> Type the password the ISE user account. The password should match the value configured under <i>Add F5 BIG-IP LTM as a NAD for RADIUS Health Monitoring</i> in the “ISE Configuration Prerequisites” section.
Secret	<RADIUS Secret>	<ul style="list-style-type: none"> Type the RADIUS secret key used to communicate with the PSNs. The RADIUS secret should match the value configured under <i>Add F5 BIG-IP LTM as a NAD for RADIUS Health Monitoring</i> in the “ISE Configuration Prerequisites” section.
NAS IP Address	<NAS IP Address>	<ul style="list-style-type: none"> Optional. By default, BIG-IP LTM will use the interface, or Self IP. If wish to match the monitor’s RADIUS requests using a different NAS-IP-Address, enter new value here.
Alias Service Port	1645 or 1812	<ul style="list-style-type: none"> Set the service port to be the same as used for the RADIUS Authentication/Authorization Virtual Server and Pool.
iRules (Main tab > Local Traffic > iRules)		
Name	<p><RADIUS Persistence iRule Name></p> <p>Example: radius_mac_sticky</p>	<ul style="list-style-type: none"> Enter a name for the iRule used to persist RADIUS Authentication, Authorization, and Accounting traffic.
Definition	<iRule Definition>	<ul style="list-style-type: none"> Enter the iRule details. Refer to <i>Example F5 BIG-IP LTM iRules for RADIUS Persistence</i> under the “RADIUS Persistence” section for more details.
Profiles (Main tab > Local Traffic > Profiles)		

UDP (Protocol > UDP)	Name	<Profile Name> Example: ise_radius_udp	<ul style="list-style-type: none"> Type a unique name for the UDP profile
	Parent Profile	udp	
	Idle Timeout	60	<ul style="list-style-type: none"> UDP idle timeout should be set based on the RADIUS environment and load balancer resources. High RADIUS activity will consume more F5 appliance resources to maintain connection states. This setting can be increased in networks with lower authentication activity or sufficient appliance capacity. Conversely, the value may need to be tuned lower with higher authentications activity or lower appliance resource capacity. For initial deployment, it is recommended to start with the default setting of 60 seconds.
	Datagram LB	<Disabled>	<ul style="list-style-type: none"> ISE requires multiple RADIUS packets for a given host be sent to the same PSN.
RADIUS (Services > RADIUS)	Name	<Profile Name> Example: ise_radiusLB	<ul style="list-style-type: none"> Type a unique name for the RADIUS Service profile.
	Parent Profile	radiusLB	<ul style="list-style-type: none"> Defining a RADIUS profile allows F5 to process RADIUS Attribute-Value Pairs (AVPs) in iRules
	Persist Attribute	<Not Configured>	<ul style="list-style-type: none"> Recommendation is to use iRule to define persistence attribute Persist Attribute option is simple and may be sufficient in some deployments, but the iRule method is recommended for its additional support for advanced rule processing, multiple attributes, fallback logic, and options to log events to assist in troubleshooting. If iRule not used, recommendation for persist attribute value is "31" (Calling-Station-ID). In the event Calling-Station-ID (or Framed-IP-Address) is not present, Source IP address or RADIUS NAS-IP-Address are suitable fallback persistence options.
Persistence	Name	<Profile Name> Example: radius_sticky	<ul style="list-style-type: none"> Type a unique name for the RADIUS persistence profile.
	Parent Profile	Universal	<ul style="list-style-type: none"> Universal profile allows specification of an iRule for advanced persistence logic

	Match Across Services	Enabled	<ul style="list-style-type: none"> When using separate Virtual Servers that share the same IP address but different service ports, this setting allows load balancing to persist across RADIUS Auth and Accounting services. No requirement to Match Across Servers when Virtual Servers share the same IP address. For more information, see F5 support article SOL5837: Match Across options for session persistence.
	iRule	<iRule Name> Example: radius_mac_sticky	<ul style="list-style-type: none"> Specify iRule used to set RADIUS persistence. See “RADIUS Persistence” section for more details on recommended iRules for persistence.
	Timeout	<Persist Timeout> Wireless: 3600 seconds (1 hour) Wired: 28800 seconds (8 hours)	<ul style="list-style-type: none"> Recommendation is to use iRule to define persistence timeout. Persistence timeout configured in iRule overrides profile setting here. If iRule not used, set Persistence Timeout based on environment. These factors include access method, device types, and average connection times. It is possible to set different persistence TTLs in F5 through separate Virtual Servers or through iRules. See “RADIUS Persistence” section for more details on recommended timeout values.
<p>Pool List (Main tab > Local Traffic > Pools > Pool List)</p> <p>The Pool List contains the list of real servers that service load balanced requests for a given Virtual Server.</p> <p>Note: Create two server pools—one for RADIUS Authentication and Authorization and another for RADIUS Accounting</p>			
Name	<Pool Name> Examples: radius_auth_pool radius_acct_pool		<ul style="list-style-type: none"> Type a unique name for each RADIUS pool—one pool will be defined for RADIUS Authentication and Authorization and another pool will be defined for RADIUS Accounting.
Health Monitors	<RADIUS Health Monitor> Example: radius_1812		<ul style="list-style-type: none"> Enter the RADIUS Health Monitor configured in previous step. Note: The same monitor will be used to verify both RADIUS Auth and Accounting services on the ISE PSN appliances to minimize resource consumption on both F5 and ISE appliances.
Allow SNAT	No		<ul style="list-style-type: none"> RADIUS CoA support requires that SNAT be disabled. Setting here reinforces SNAT setting in Virtual Server definition.

Action on Service Down	Reselect	<ul style="list-style-type: none"> Reselect option ensures established connections are moved to an alternate pool member when a target pool member becomes unavailable. For additional details on failed node handling, refer to following F5 Support articles: <ul style="list-style-type: none"> SOL15095: Overview of the Action On Service Down feature SOL8968: Enabling persistence for a virtual server allows returning clients to bypass load balancing
Member IP Addresses	<ISE PSN addresses in the LB cluster> Examples: ise-psn-1 10.1.99.5 ise-psn-2 10.1.99.6 ise-psn-3 10.1.99.7	<ul style="list-style-type: none"> These are the real IP addresses of the PSN appliances. The PSNs are configured as nodes under the Node List. These entries can be automatically created when defined within the Pool List configuration page.
Member Service Port	<Separate, Unique Ports for RADIUS Authentication/Authorization and Accounting> Examples: Authentication/Authorization Pool: 1645 or 1812 Accounting Pool: 1646 or 1813	<ul style="list-style-type: none"> For each pool, define the appropriate RADIUS Authentication or Accounting port to be used to connect to the PSNs.
Load Balancing Method	Least Connections (node)	<ul style="list-style-type: none"> Least Connections (member) also viable, but 'node' option allows F5 to take into consideration all connections across pools.
Virtual Server (Main tab > Local Traffic > Virtual Servers > Virtual Server List)		
Note: Create two virtual servers—one for RADIUS Authentication and Authorization and one for RADIUS Accounting		
Name	<RADIUS Virtual Server Name> Examples: RADIUS Authentication: ise_radius_auth RADIUS Accounting: ise_radius_acct	<ul style="list-style-type: none"> Enter the name to identify the virtual server for RADIUS Auth and RADIUS Accounting
Type	Standard	<ul style="list-style-type: none"> Standard allows specification of profiles for the UDP Protocol and RADIUS
Source	<Source Network Address/Mask> Example: 10.0.0.0/8	<ul style="list-style-type: none"> Type the network address with bit mask for the external network addresses that need to communicate with the ISE PSNs. Make the source as restrictive as possible while not omitting RADIUS clients (network access devices) that need to communicate to the PSNs for RADIUS AAA.

Destination (VIP Address)	Type	Host	
	Address	<Single IP Address for RADIUS Authentication, Authorization, and Accounting> Example: 10.1.98.8	<ul style="list-style-type: none"> Enter the Virtual IP Address for RADIUS AAA services. Single IP address (versus separate IP addresses for Authentication/Authorization and Accounting) is recommended as it simplifies both load balancer configuration and the access device (RADIUS client) configuration.
Service Port	<Separate, Unique Ports for RADIUS Authentication/Authorization and Accounting> Examples: RADIUS Authentication: UDP/1645 or UDP/1812 RADIUS Accounting: UDP/1646 or UDP/1813		<ul style="list-style-type: none"> Wildcard port (all UDP ports) is an option, but general recommendation is to define separate Virtual Servers that share a single VIP but each with distinct ports for RADIUS Authentication/Authorization and Accounting. This offers additional load balancing controls and management by Virtual Server and service.
Protocol	UDP		<ul style="list-style-type: none"> UDP Protocol Profile and RADIUS Profile to be defined. See Profile section in the table for more details.
Protocol Profile (Client)	<UDP Protocol Profile> Example: ise_radius_udp		<ul style="list-style-type: none"> Enter the name of the UDP Protocol Profile defined earlier.
RADIUS Profile	<RADIUS Service Profile> Example: ise_radiusLB		<ul style="list-style-type: none"> Enter the name of the RADIUS Service Profile defined earlier.
VLAN and Tunnel Traffic	Enabled On...		<ul style="list-style-type: none"> Optional: Restrict inbound RADIUS requests to specific VLANs.
VLANs and Tunnels	<External VLANs> Example: External		<ul style="list-style-type: none"> Select the ingress VLAN(s) used by external access devices to communicate with the PSNs.
Source Address Translation, or "SNAT Pool"	None		<ul style="list-style-type: none"> RADIUS CoA support requires that SNAT be disabled.
Default Pool	<Pool Name> Examples: RADIUS Auth: radius_auth_pool RADIUS Accounting: radius_acct_pool		<ul style="list-style-type: none"> Select the Server Pool name defined for RADIUS Authentication/Authorization or Accounting See "Pool List" section in table for more details.
Default Persistence Profile	<Persistence Profile Name> Example: radius_sticky		<ul style="list-style-type: none"> Select the name of the RADIUS Persistence Profile created earlier.

Fallback Persistence Profile	<Fallback Persistence Profile Name> Example: source_addr	<ul style="list-style-type: none"> • This setting should not be required since we will include a fallback persistence method within the iRule. The iRule settings take precedence over values entered here. • If the iRule deployed does not have such a fallback method defined, then you can enter a value here such as Source IP address.
------------------------------	---	--

Best Practice: After making changes to the RADIUS Load Balancing configuration, it may be necessary to clear existing connections to ensure any traffic currently being processed by less-specific Virtual Servers such as Forwarding (IP) hit the new, more-specific Virtual Servers created for RADIUS traffic. Use the `tmsh sys delete connection` command from the F5 BIG-IP LTM console to clear all existing connections, or use with parameters to delete specific connections based on protocol (udp/tcp), client/server IP address, or client/server port number.

RADIUS CoA Handling

RADIUS Change of Authorization (CoA) is a communication is used by ISE to trigger a new policy on an existing network session. Unlike typical RADIUS Authentication, Authorization, and Accounting (AAA) traffic initiated by an access device (RADIUS client) towards the PSN (RADIUS server), RADIUS CoA is instead initiated by the PSN. In this communication flow, the PSN becomes the client and the access device becomes the server.

Network Access Device Configuration for CoA

Since RADIUS CoA is not a transaction that is started by the network access device, each NAD must be configured to trust the source of the CoA packets. This section shows the basic configuration for Cisco access switches and wireless controllers to trust CoA packets from the PSNs.

Cisco Catalyst Switches

Cisco Catalyst switches must be configured with the IP address and RADIUS secret key for each PSN to be a trusted source of RADIUS CoA requests. The PSN is the client in this communication as noted in the sample switch configuration.

```

aaa server radius dynamic-author
 client 10.1.99.5 server-key cisco123
 client 10.1.99.6 server-key cisco123
 client 10.1.99.7 server-key cisco123
 client 10.1.99.8 server-key cisco123
 client 10.1.99.9 server-key cisco123
 client 10.1.99.10 server-key cisco123
 <...one entry per PSN...>

```

Cisco Wireless LAN Controllers

Cisco WLCs only trust RADIUS CoA from configured RADIUS Authentication servers as shown in the sample configuration.

RADIUS Authentication Servers

Acct Call Station ID Type [1](#) System MAC Address

Auth Call Station ID Type AP MAC Address:SSID

Use AES Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS)

MAC Delimiter Hyphen

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	10.1.99.5	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2	10.1.99.6	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3	10.1.99.7	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4	10.1.99.8	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5	10.1.99.9	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	6	10.1.99.10	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	7	10.1.99.X	1812	Disabled	Enabled

Figure 40. RADIUS CoA Configuration for Cisco Wireless Controllers

Source NAT for RADIUS CoA

An obvious downside of the NAD configuration for RADIUS CoA is that each access device must be individually configured with the unique IP address of every PSN. What if new PSNs are added? What if existing ones must be readdressed or removed? The management of these entries can be problematic and become out of sync. Additionally, some access devices like the WLC are limited by the number of RADIUS Server entries thus making it difficult to configure trust for a large number of possible PSN servers.

The solution to this management dilemma is to configure Source NAT for RADIUS CoA traffic initiated by the PSNs to be that of the RADIUS Virtual Server IP address. The diagram depicts this scenario whereby all traffic on ISE CoA port UDP/1700 originating from the PSNs is source NATted to the RADIUS VIP address.

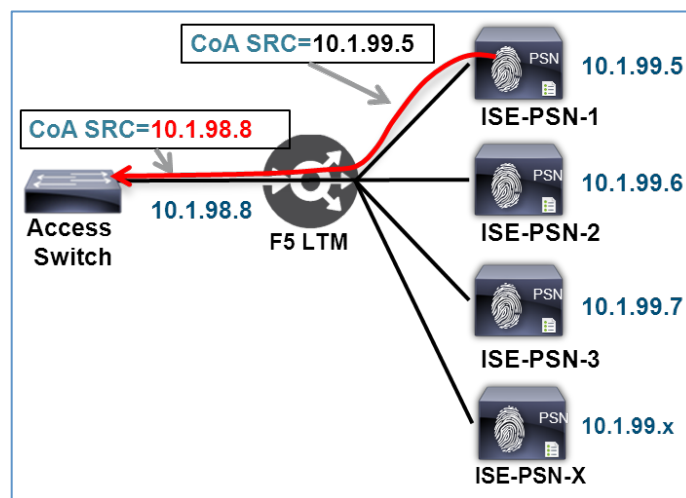


Figure 41. Source NAT for RADIUS CoA

Since the RADIUS VIP is already configured as a trusted RADIUS Server in Cisco WLCs, no additional entries are required. Similarly, Cisco Catalyst Switches can be configured with one client entry per load-balanced group of PSNs. The following examples show how SNAT can simplify the NAD’s CoA configuration.

Best Practice: The use of SNAT for PSN-initiated CoA traffic is a best practice to simplify NAD configuration and facilitate change changes in PSN addresses from the F5 appliance rather than changing the configuration on each NAD.

The SNAT configuration depicted in this section is specific to RADIUS CoA traffic initiated by the PSNs and destined to the NADs. **This should not be confused with restrictions on SNAT for RADIUS AAA traffic in the opposite direction, i.e. from the NADs to the PSNs.** SNAT of NAD-initiated RADIUS AAA traffic will break CoA operation. Refer to the “NAT Restrictions for RADIUS Load Balancing” section for additional details.

RADIUS CoA Configuration Examples using SNAT

Cisco Catalyst Switch Example:

```
aaa server radius dynamic-author
client 10.1.98.8 server-key cisco123
```

Cisco Wireless LAN Controller Example:

The screenshot shows the 'RADIUS Authentication Servers' configuration page. It includes several settings: 'Acct Call Station ID Type' set to 'System MAC Address', 'Auth Call Station ID Type' set to 'AP MAC Address:SSID', 'Use AES Key Wrap' unchecked, and 'MAC Delimiter' set to 'Hyphen'. Below these settings is a table with the following data:

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<u>1</u>	10.1.98.8	1812	Disabled	Enabled

Figure 42. CoA Configuration using SNAT for Cisco Wireless LAN Controller

RADIUS CoA SNAT: F5 LTM Configuration Details

Using a basic NAD CoA configuration without SNAT, CoA packets can be sent directly through the F5 BIG-IP LTM using the IP Forwarding servers configured earlier in this guide. This section details the F5 LTM configuration required to simplify the NAD CoA configuration by Source NATting RADIUS CoA traffic initiated by the ISE PSNs.

Use the settings outlined in the table to configure F5 LTM to SNAT RADIUS CoA traffic from ISE PSNs.

Table 6. LTM RADIUS CoA SNAT Configuration

BIG-IP LTM Object	Recommended Setting		Notes
SNAT Pool List (Main tab > Local Traffic > Address Translation > SNAT Pool List)			
Name	<RADIUS CoA SNAT Pool Name> Example: radius_coa_snatpool		<ul style="list-style-type: none"> Type the name of the SNAT pool to be used for RADIUS CoA.
IP Address	<RADIUS VIP Address> Example: 10.1.98.8		<ul style="list-style-type: none"> Enter the IP address of the RADIUS Virtual Server used for RADIUS AAA. The RADIUS VIP will be the only member in the SNAT pool.
Virtual Server (Main tab > Local Traffic > Virtual Servers > Virtual Server List)			
Name	<RADIUS CoA SNAT Server> Example: RADIUS-COA-SNAT		<ul style="list-style-type: none"> Type the name of the virtual server for the SNAT of RADIUS CoA traffic from the PSNs to network access devices.
Type	Standard		<ul style="list-style-type: none"> Standard profile allows the specification for source and destination networks and ports needed to define RADIUS CoA traffic flows.
Source	<Source Network Address/Mask> Example: 10.1.99.0/28		<ul style="list-style-type: none"> Type the network address with bit mask for the ISE PSNs. Restrict the source network to the PSNs, the source of RADIUS CoA traffic.
Destination	Type	Network	
	Address	<Destination Network> Example: 10.0.0.0	<ul style="list-style-type: none"> Enter the network address appropriate to your environment. For added security, make the address range as restrictive as possible while being sure to cover all CoA-capable NADs.
	Mask	<Destination Mask> Example: 255.0.0.0	<ul style="list-style-type: none"> Enter the network address mask appropriate to your environment. For added security, make the address range as restrictive as possible.
Service Port	1700 / Other		<ul style="list-style-type: none"> Enter port 1700, the default CoA port for ISE.
Protocol	UDP		<ul style="list-style-type: none"> Select the wildcard protocol to match all protocols by default
VLAN and Tunnel Traffic	Enabled On...		<ul style="list-style-type: none"> Optional: Restrict RADIUS CoA traffic to a specific VLAN.
VLANs and Tunnels	<Internal VLAN> Example: Internal		<ul style="list-style-type: none"> Select the PSN server VLAN used to communicate with NADs.
Source Address Translation	SNAT		<ul style="list-style-type: none"> Enable SNAT for RADIUS CoA traffic

SNAT Pool	<RADIUS CoA SNAT Pool> Example: radius_coa_snatpool	<ul style="list-style-type: none">• Select the name of the previously configured SNAT Pool List.
-----------	--	--

Note: Be sure to configure the NADs with the appropriate client entries for CoA based on whether SNAT is used or not used for RADIUS CoA.

Load Balancing ISE Profiling

Introduction

What is ISE Profiling?

Profiling is an ISE service that collects attributes about network-connected endpoints and correlates the data to classify the device. Common classifications include network printers, IP phones, client workstations by OS type, and mobile endpoints such as Apple iOS and Android phones and tablets.

The Profiling service can be performed with or without RADIUS-based authentication and is extremely helpful in adding context as to “what” is connected to the network. The end result is better network visibility and the ability to include an endpoint’s classification, or profile assignment, in network access policies.

ISE Profiling can process different types of data and supports a variety of collection methods. The type of endpoint data collected is specific to each collector process, or probe. ISE currently supports the following probe categories:

- RADIUS
- SNMP Query and Trap
- DHCP
- HTTP
- DNS
- NMAP
- NetFlow

Why Should I Load Balance Profiling Traffic?

Some ISE probes require that data be sent from network infrastructure directly to the PSN including RADIUS, DHCP (via DHCP relay/helper), SNMP Traps, and NetFlow. To support redundancy in a non-LB deployment, it is often necessary to send the data for these probes to multiple PSNs. This can result in excessive data collection and can impact scaling for the ISE deployment as critical profile data must be continuously replicated to other nodes.

One method to optimize local synchronization of profile data is to deploy ISE Node Groups. This topic has already been covered under *Configure Node Groups for Policy Service Nodes in a Load-Balanced Cluster* in the “ISE Configuration Prerequisites” section.

Another method to optimize profile data collection is to limit the number of PSNs that receive data for a given endpoint while still providing redundancy. Profiling collection and data replication can be further optimized by limiting the collection for a given endpoint to the same PSN. One solution to support this requirement is to load balance profiling data. Instead of configuring each sender of RADIUS, DHCP, SNMP Trap, or NetFlow profile data to multiple PSNs, load balance allows a single Virtual Server to be configured. This simplifies configuration, especially if PSNs are added to the deployment or network parameters modified. Load balancing minimizes network bandwidth utilization as multiple targets can be consolidated into one while providing redundancy.

Note: In deployments that involve multiple data centers for disaster recovery, it is common that profiling data be sent to both data centers from remote sites. In this scenario, it is recommended to deploy separate load-balanced clusters in each data center. Therefore, it is possible that network devices may require a second target configured for profiling data. Since the profile data sources are usually configured with an IP address, DNS-

based solutions like F5's BIG-IP Global Traffic Manager (GTM) or Cisco's Global Site Selector (GSS) would not apply. To support a single target, solutions like Anycast with intelligent routing, Cisco IOS Embedded Event Manager (EEM), or service templates may be required to dynamically update targets or route traffic to a single destination.

Which Profiling Data Should Be Load Balanced?

Of the multiple profiling probes supported by ISE, the ones that can benefit most from PSN load balancing by F5 BIG-IP LTM include:

- RADIUS (UDP/1645-1646 and UDP/1812-1813)
- DHCP (UDP/67)
- SNMP Trap (UDP/162)
- NetFlow (Export port is often configurable, but UDP/9996 and UDP/2055 most common)

The DNS probe sends reverse lookup requests to external DNS servers, so while this traffic can technically be load balanced by the F5 BIG-IP LTM, it does not directly impact the PSNs.

Load Balancing RADIUS Profiling Data

Since RADIUS data is already load-balanced as part of RADIUS AAA, no additional load balancing configuration is required.

Cisco Catalyst Switches and Wireless LAN Controllers support a feature called Device Sensor. Device Sensor optimizes profiling by allowing the access device to locally collect and consolidate endpoint data and centrally report the results using RADIUS Accounting. Again, this profile traffic is automatically covered by the RADIUS AAA load balancing configuration.

Best Practice: Device Sensor optimizes profile collection by consolidating multiple attributes that normally require separate data sources and probes and reporting them to a single PSN target using RADIUS Accounting. This process has the additional benefit of sending profile data for multiple probe categories to the *same* PSN. This can significantly reduce the replication requirements for profiling data.

Note: The remainder of this section will focus on the load balancing of DHCP, SNMP Traps, and NetFlow packets to PSNs.

Health Monitors for Profiling Services: DHCP, SNMP, and NetFlow

The profiling data for DHCP, SNMP Traps, and NetFlow are all UDP-based and also unidirectional. This means that no response traffic is expected from the PSNs when consuming the profile data by these probes. Consequently, F5 monitors that rely on application-specific responses are not applicable. The use of simple ICMP is suitable to verify node is IP reachable. Since most ISE deployments combine Profiling and RADIUS user services, the reuse of the RADIUS monitor is a reasonable option to verify that ISE application services are running. In general, if RADIUS AAA services are not operational, you will likely not want to send profiling data to the node when both services are configured on the PSN.

Load Balancing DHCP Profiling Data

ISE supports the consumption of both DHCP SPAN data as well as traffic sent using DHCP Proxy and DHCP Relay. As SPAN and Proxy options are single destination methods, the focus of DHCP load balancing discussion will be on Relay which supports multiple simultaneous destinations.

The most common method for forwarding DHCP requests to specific DHCP servers from a router or Layer 3 switch is known as IP Helper. This method uses the Cisco IOS **ip helper-address** command to define one or more recipients for DHCP packets received by endpoints on the local Layer 2 domain. The following example configuration shows how a Cisco Catalyst Switch can forward DHCP packets to a valid DHCP server and to multiple PSNs for profile data collection.

```
!  
interface Vlan10  
description EMPLOYEE  
ip address 10.1.10.1 255.255.255.0  
ip helper-address 10.1.100.100 <--- Real DHCP Server  
ip helper-address 10.1.99.5 <--- ISE-PSN-1  
ip helper-address 10.1.99.6 <--- ISE-PSN-2  
ip helper-address 10.1.98.7 <--- ISE-PSN-3  
!  
interface Vlan11  
description GUEST  
ip address 10.1.11.1 255.255.255.0  
ip helper-address 10.1.100.100 <--- Real DHCP Server  
ip helper-address 10.1.99.5 <--- ISE-PSN-1  
ip helper-address 10.1.99.6 <--- ISE-PSN-2  
ip helper-address 10.1.98.7 <--- ISE-PSN-3  
!
```

By using an F5 BIG-IP LTM, the configuration can be simplified as shown.

```
!  
interface Vlan10  
description EMPLOYEE  
ip address 10.1.10.1 255.255.255.0  
ip helper-address 10.1.100.100 <--- Real DHCP Server  
ip helper-address 10.1.98.8 <--- F5 VIP  
!  
interface Vlan11  
description GUEST  
ip address 10.1.11.1 255.255.255.0  
ip helper-address 10.1.100.100 <--- Real DHCP Server  
ip helper-address 10.1.98.8 <--- F5 VIP  
!
```

Any changes to the real PSN quantity or addressing behind the F5 BIG-IP LTM will be transparent to the forwarding switch/router.

DHCP Profiling Data Flow

The sample diagram shows the typical flow for sending DHCP traffic to both a real DHCP Server and an F5 BIG-IP LTM appliance. Unlike the real DHCP Server requests, the PSNs will never reply.

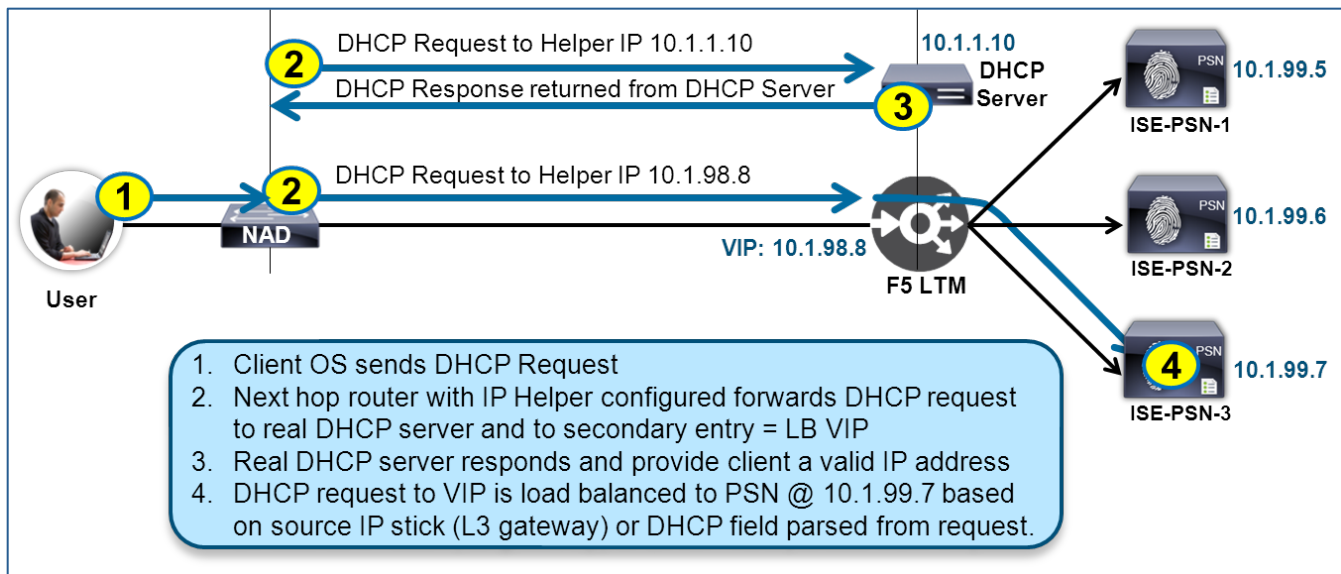


Figure 43. DHCP Profiling Traffic Flow

Standard client to DHCP server packets use UDP/67 as the destination service port. The Virtual Server configured for DHCP load balancing can share the same IP address used by RADIUS load balancing. Optionally, a separate, dedicated interface with a unique node IP address can be configured on each PSN for the purpose of consuming profiling data.

DHCP Profiling Persistence

The source IP address for relayed DHCP requests is that of the forwarding router/switch (the IP Helper). This device is usually the endpoint's default gateway on the access network. In ISE deployments that include numerous default gateways, the source IP address of the DHCP packet is a reasonable attribute choice for persistence. This is due to the fact that each client is more likely to connect to the same access device over time, so multiple DHCP packets from the same endpoint tend to be sent to the same PSN. Also, the larger the distribution of clients over multiple gateways, the better the distribution of DHCP requests across load balanced PSNs.

Technically, each DHCP packet could be sent to a different PSN in the load-balanced cluster. The reason to apply persistence is to help optimize data collection and minimize database replication. By sending all DHCP packets for a given endpoint to the same PSN, we minimize the need to synchronize profiling data across ISE nodes in the deployment.

If there are fewer gateways or if large, uneven populations of endpoints are handled by small number of gateways (Examples: Layer 2 access switches where VLANs terminate on large distribution or core switches; large wireless deployments that use Cisco WLCs to aggregate many users to a central location), then it may be necessary to use a different persistence attribute to achieve better load distribution while ensuring DHCP data for same clients reach the same PSNs.

This is another case where advanced F5 iRule logic can be very powerful. Through intelligent parsing, an iRule can determine the location of a key DHCP option field and use that as the basis for persistence. Two examples are DHCP option 61 (dhcp-client-identifier) and DHCP Option 50 (dhcp-requested-address). The Client Identifier is typically the MAC address of the endpoint whereas Requested Address is typically the client IP address. (Reference: [RFC2132 "DHCP Options and BOOTP Vendor Extensions"](#))

Furthermore, a persistence iRule that matches on DHCP Client Identifier can be configured to leverage the existing RADIUS persistence iRule resulting in all requests from the same client MAC address being sent to the same PSN (See diagram). This can significantly optimize profiling collection and data base replication.

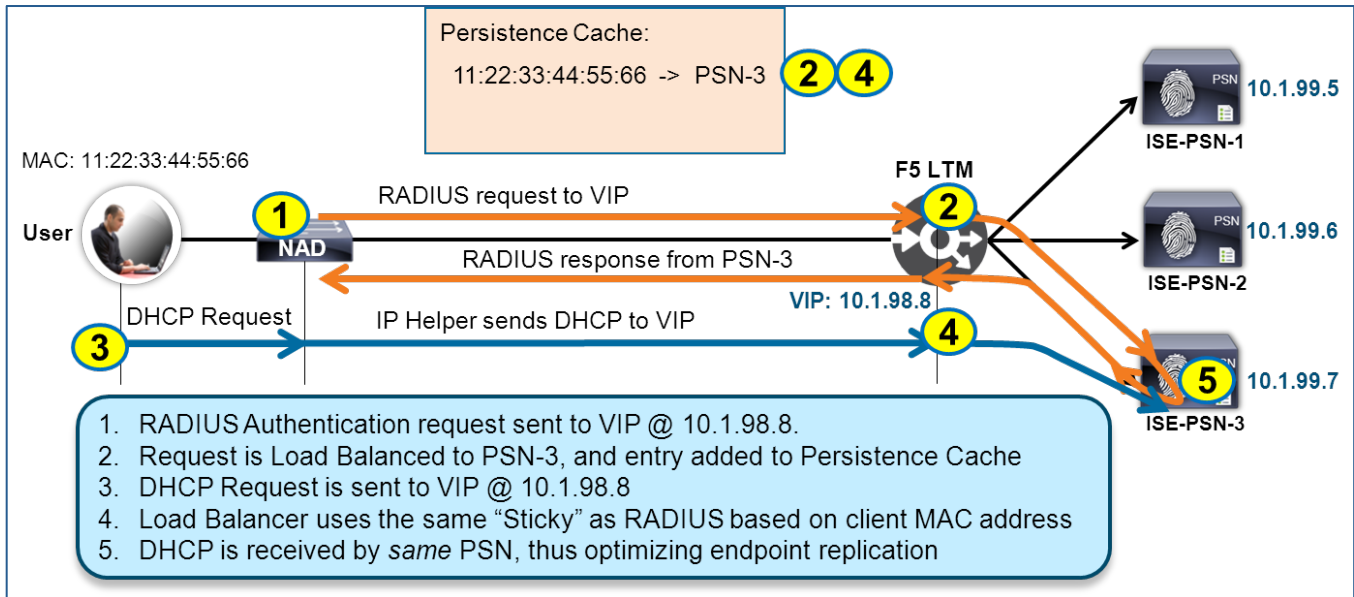


Figure 44. DHCP Profiling Persistence Based on MAC Address

The standard configuration section will show the use of simple source address persistence. An example of the advanced DHCP parser iRule is included in the Appendix for reference.

Load Balancing SNMP Trap Profiling Data

The main purpose of the SNMP Trap probe is to trigger a PSN to send an SNMP Query against the endpoint’s switchport. Since RADIUS Accounting can also trigger this same switchport query, the use of SNMP traps for profiling is generally recommend only in cases where RADIUS-based port authentication is not already deployed. This is commonly the case during an initial ISE deployment as part of a network discovery phase.

The processing of SNMP traps is limited to wired access switches and does not apply to Wireless or VPN access methods. Therefore, the source IP address of SNMP traps will be determined by the exit interface (default behavior) or the interface defined using the `snmp-server trap-source <interface>` command.

Similar to DHCP relay agents, without the use of load balancers, a common configuration requires that multiple SNMP trap hosts be configured for redundancy as shown in the sample switch configuration.

```
!  
snmp-server trap-source GigabitEthernet1/0/24  
snmp-server enable traps snmp linkdown linkup  
snmp-server enable traps mac-notification change move  
snmp-server host 10.1.99.5 version 2c public mac-notification snmp  
snmp-server host 10.1.99.6 version 2c public mac-notification snmp  
snmp-server host 10.1.99.7 version 2c public mac-notification snmp  
!
```

The use of the F5 BIG-IP LTM allows the configuration to be simplified by reducing the number of trap targets as shown.

```
!  
snmp-server trap-source GigabitEthernet1/0/24  
snmp-server enable traps snmp linkdown linkup  
snmp-server enable traps mac-notification change move  
snmp-server host 10.1.98.8 version 2c public mac-notification snmp  
!
```

Any changes to the real PSN quantity or addressing behind the BIG-IP LTM will be transparent to the sending switch/router.

The general recommendation for persistence of SNMP traps is Source IP address, the trap source of the access switch. Like DHCP packets, the load distribution of SNMP traps will depend on the number and size of the access switches. SNMP Linkup traps do not contain endpoint information, only switch and interface index information. Therefore, there is no discernible attributes specific to an endpoint. If MAC Notification traps are configured instead, then they will include the client MAC address and it would be possible to configure an iRule to parse that data for non-encrypted traps (SNMv1/2c or SNMPv3 without encryption). Since the use of traps for profiling is often during pre-RADIUS deployment, the impact to ISE deployment is limited and persistence on source IP is typically adequate.

Standard SNMP traps use UDP/162 as the destination service port. The Virtual Server configured for SNMP Trap load balancing can share the same IP address used by RADIUS load balancing and other Virtual Servers used for profiling. Optionally, a separate, dedicated interface with a unique node IP address can be configured on each PSN for the purpose of consuming profiling data.

Load Balancing Netflow Profiling Data

Profiling using Netflow should be limited to exception use cases, such as the classification of critical endpoints that cannot authenticate themselves to the network. These types of devices are prevalent in verticals such as healthcare, manufacturing, and other environments where the mission-specific endpoints can only be distinguished by their traffic flows. Excessive or indiscriminate use of NetFlow for profiling purposes can result in potential high loads on network and ISE resources.

NetFlow is sent (exported) by Layer 3 switches and routers in the network. Like DHCP relays, the source of NetFlow is not always from an access layer device. NetFlow is more commonly deployed on aggregation points in the network such as WAN routers or distribution or core switches. Without the use of load balancers, multiple NetFlow Export destinations would need to be configured for redundancy, if supported by the Netflow-capable router/switch or an intermediate NetFlow Collector. NetFlow may contain data from multiple endpoints that are located virtually any point in the network which makes virtually impossible to persist NetFlow for a given endpoint to a specific PSN. The

primary benefit of load balancing NetFlow exports to ISE is to provide redundancy and to simplify the export configuration. The recommended persistence attribute is the source IP address, a value that can be controlled on the export device using the **ip flow-export source <interface>** command.

Best Practice: Be sure to closely monitor any NetFlow records sent to the load balancer for bandwidth and performance impact on both the F5 and ISE appliances. It is recommended that a phased approach be used to better gauge the impact of each new router/switch configured to export NetFlow to the load balancer.

Although configurable, common destination ports for NetFlow export include UDP/9995 and UDP/2055. The Virtual Server configured for NetFlow load balancing may share the same Virtual IP address used by RADIUS load balancing and other profiling services, but the pool members should be configured to use a dedicated PSN interface, each with a unique node IP address. This ensures traffic separation for the NetFlow profiling data on the PSN. If NetFlow bandwidth is a concern on the F5 appliance, then a unique Virtual Server IP address on a separate F5 interface can be configured on the load balancer appliance.

Note: When configuring the dedicated NetFlow interfaces on the individual PSNs, be sure to set each node’s Profiling Configuration for the correct interface and port.

Profiling Load Balancing: F5 LTM Configuration Details

This section provides the detailed F5 BIG-IP LTM configuration for load balancing ISE Profiling data to PSNs including the recommended settings and considerations for each component.

Use the settings outlined in the table to configure F5 LTM to load balance Profiling data with ISE PSNs.

Table 7. LTM Profiling Load Balancing Configuration

BIG-IP LTM Object	Recommended Setting		Notes
iRules (Main tab > Local Traffic > iRules)			
OPTIONAL: Configure iRule for DHCP profiling only if planning to deploy persistence based on client MAC address.			
Name	<DHCP Persistence iRule Name> Example: dhcp_mac_sticky		Enter a name for the iRule used to persist DHCP traffic.
Definition	<iRule Definition>		Enter the iRule details. For additional details, refer to the “DHCP Profiling Persistence” section and the Appendix for sample iRule for DHCP persistence based on client MAC address.
Profiles (Main tab > Local Traffic > Profiles)			
UDP (Protocol > UDP)	Name	<Profile Name> Example: ise_profiling_udp	<ul style="list-style-type: none"> Type a unique name for the UDP profile The configuration of a unique profile for profiling will allow changes to be made without impacting other Virtual Servers with a UDP profile defined.
	Parent Profile	udp	

	Idle Timeout	Immediate	<ul style="list-style-type: none"> Set Idle Timeout to Immediate. Profiling traffic from DHCP and SNMP Traps are one-way flows to PSNs—no response sent to these packets.
	Datagram LB	<Disabled>	<ul style="list-style-type: none"> It is recommended that profiling data from the same NAD, or endpoint where applicable, be sent to the same PSN.
Persistence (OPTIONAL: Advanced DHCP use case—per host)	Name	<Profile Name> Example: dhcp_sticky	<ul style="list-style-type: none"> Type a unique name for the DHCP persistence profile.
	Parent Profile	Universal	<ul style="list-style-type: none"> Universal profile allows specification of an iRule for advanced persistence logic
	Match Across Services	Enabled	<ul style="list-style-type: none"> When using separate Virtual Servers that share the same IP address but different service ports, this setting allows load balancing to persist across RADIUS and DHCP services. No requirement to Match Across Servers when Virtual Servers share the same IP address. For more information, see F5 support article SOL5837: Match Across options for session persistence.
	iRule	<iRule Name> Example: dhcp_mac_sticky	<ul style="list-style-type: none"> Specify iRule used for DHCP profiling persistence. See “DHCP Load Balancing Persistence” section for more details on recommended iRule for persistence.
	Timeout	<Persist Timeout> Wireless: 3600 seconds (1 hour) Wired: 28800 seconds (8 hours)	<ul style="list-style-type: none"> Recommendation is to use iRule to define persistence timeout. Persistence timeout configured in iRule overrides profile setting here. If iRule not used, set Persistence Timeout based on environment. These factors include access method, device types, and average connection times. It is possible to set different persistence TTLs in F5 through separate Virtual Servers or through iRules. See “Persistence” section for more details on recommended timeout values.

Pool List (Main tab > Local Traffic > Pools > Pool List)

The Pool List contains the list of real servers that service load balanced requests for a given Virtual Server.

Note: Create one server pool for each ISE Profiling Probe to be load balanced—DHCP/SNMP Trap/NetFlow

Name	<Pool Name> Examples: profiling_dhcp_pool profiling_snmptrap_pool profiling_netflow_pool	<ul style="list-style-type: none"> Type a unique name for each Profiling pool—one pool will be defined for each profiling method—DHCP, SNMP Traps, NetFlow—as required.
------	--	--

Health Monitors	<Profiling Health Monitor> Example: radius_1812	<ul style="list-style-type: none"> • Enter the RADIUS Health Monitor configured in previous step. • Note: The same monitor will be used to verify both RADIUS AAA and Profiling services on the ISE PSN appliances to minimize resource consumption on both F5 and ISE appliances. • If RADIUS is not load balanced, then the simple gateway_icmp monitor can be used to check PSN availability.
Action on Service Down	Reselect	<ul style="list-style-type: none"> • Reselect option ensures established connections are moved to an alternate pool member when a target pool member becomes unavailable. For additional details on failed node handling, refer to following F5 Support articles: <ul style="list-style-type: none"> o SOL15095: Overview of the Action On Service Down feature o SOL8968: Enabling persistence for a virtual server allows returning clients to bypass load balancing
Member IP Addresses	<ISE PSN addresses in the LB cluster> Examples: ise-psn-1 10.1.99.5 ise-psn-2 10.1.99.6 ise-psn-3 10.1.99.7	<ul style="list-style-type: none"> • These are the real IP addresses of the PSN appliances. • The PSNs are configured as nodes under the Node List. These entries can be automatically created when defined within the Pool List configuration page. • For NetFlow, be sure to configure a dedicated PSN interface with unique IP address for each pool member.
Member Service Port	<Profiling UDP Port> Examples: DHCP: 67 SNMP Trap: 162 NetFlow: 9996 or 2055 , configurable	<ul style="list-style-type: none"> • For each pool, define the appropriate UDP port to be used to connect to the PSNs.
Load Balancing Method	Round Robin	<ul style="list-style-type: none"> • Note: LB methods such as Fastest (application) do not apply since the PSN does not respond to load-balanced profiling traffic.
<p>Virtual Server (Main tab > Local Traffic > Virtual Servers > Virtual Server List)</p> <p>Note: Create one virtual server per profiling service configured—DHCP/SNMP Trap/NetFlow</p>		
Name	<RADIUS Virtual Server Name> Examples: DHCP: ise_profiling_dhcp SNMP Traps: ise_profiling_snmptrap NetFlow: ise_profiling_netflow	<ul style="list-style-type: none"> • Enter the name to identify the virtual server for Profiling service
Type	Standard	<ul style="list-style-type: none"> • Standard allows specification of profiles for the UDP Protocol.

Source	<Source Network Address/Mask> Example: 10.0.0.0/8		<ul style="list-style-type: none"> Type the network address with bit mask for the external network addresses that need to communicate with the ISE PSNs. Make the source as restrictive as possible while not omitting profiling senders (network access devices, IP Helper gateways, and NetFlow exporters) that need to communicate to the PSNs for profiling.
Destination (VIP Address)	Type	Host	
	Address	<Single IP Address used for RADIUS and Profiling Services> Example: 10.1.98.8	<ul style="list-style-type: none"> Enter the Virtual IP Address for Profiling Services. Single IP address (versus separate IP addresses for RADIUS and Profiling) is recommended as it simplifies both load balancer configuration and network device configurations.
Service Port	<Profiling UDP Port> Examples: DHCP: 67 SNMP Trap: 162 NetFlow: 9996 or 2055 , configurable		<ul style="list-style-type: none"> Wildcard port (all UDP ports) is an option, but general recommendation is to define separate Virtual Servers that share a single VIP but each with distinct ports for RADIUS AAA and Profiling Services. This offers additional load balancing controls and management by Virtual Server and service.
Protocol	UDP		<ul style="list-style-type: none"> UDP Protocol Profile and RADIUS Profile to be defined. See Profile section in the table for more details.
Protocol Profile (Client)	<UDP Protocol Profile> Example: ise_profiling_udp		<ul style="list-style-type: none"> Enter the name of the UDP Protocol Profile defined earlier.
VLAN and Tunnel Traffic	Enabled On...		<ul style="list-style-type: none"> Optional: Restrict inbound profiling data to specific VLANs.
VLANs and Tunnels	<External VLANs> Example: External		<ul style="list-style-type: none"> Select the ingress VLAN(s) used by external profile data source to communicate with the PSNs.
Default Pool	<Pool Name> Examples: DHCP: profiling_dhcp_pool SNMP Traps: profiling_snmptrap_pool NetFlow: profiling_netflow_pool		<ul style="list-style-type: none"> Select the Server Pool name defined for RADIUS Authentication/Authorization or Accounting See "Pool List" section in table for more details.

Default Persistence Profile	<Persistence Profile Name> General profiling example: source_addr DHCP iRule example: dhcp_sticky	<ul style="list-style-type: none">• Select the name of the Default Persistence Profile. In general, source_addr is a reasonable option. If used, recommend create new Persistence Profile based on Source Address Affinity to allow custom configuration for persist timer and Matching options.• If a DHCP iRule was created to provide per endpoint load balancing and persistence, then select the name of the Persistence Profile created earlier.
Fallback Persistence Profile	<Fallback Persistence Profile Name> Example: source_addr	<ul style="list-style-type: none">• This setting should not be required since we will include a fallback persistence method within the iRule. The iRule settings take precedence over values entered here.• If the iRule deployed does not have such a fallback method defined, then you can enter a value here such as Source IP address.

Load Balancing ISE Web Services

ISE supports a number of web-based services including Admin access, guest services, web authentication, and endpoint compliance assessment, quarantine, provisioning, and remediation. For the purpose of understanding when and how to integrate F5 load balancing, it will help to characterize ISE web services into two general categories:

- URL-Redirected
- Direct Access

URL-Redirected Web Services

URL-Redirected web services include ISE web portals and other resources that endpoints are automatically redirected to during the RADIUS auth session. These web-based services include the following:

- Central Web Authentication (CWA)
- Device Registration WebAuth (DRW) (ISE 1.2 and below)
- Hotspot (ISE 1.3 and above)
- Client Provisioning and Posture (CPP)
- Mobile Device Management (MDM)
- Native Supplicant Provisioning (NSP)
- Endpoint Protection Services (EPS) and Blacklisting
- Custom Landing Page

With the exception of a custom landing page, all of the listed services entail the use of ISE sessionization. Sessionization uses an Audit Session ID to track the lifecycle of an endpoint's connection between a network access device and a specific PSN. (Refer to the "RADIUS Sticky Attributes" section for more details on session IDs). URL Redirection with sessionization requires that endpoints are redirected to a specific PSN that "owns" the session. During RADIUS authorization, the PSN processing the connection may return a URL Redirect that includes its own FQDN and unique Audit Session ID. This tells the client exactly which PSN to attempt direct HTTPS access and informs the receiving PSN which specific RADIUS session the request pertains.

URL-Redirection Traffic Flow

The diagram depicts the basic traffic flow for URL-Redirected traffic with sessionization.

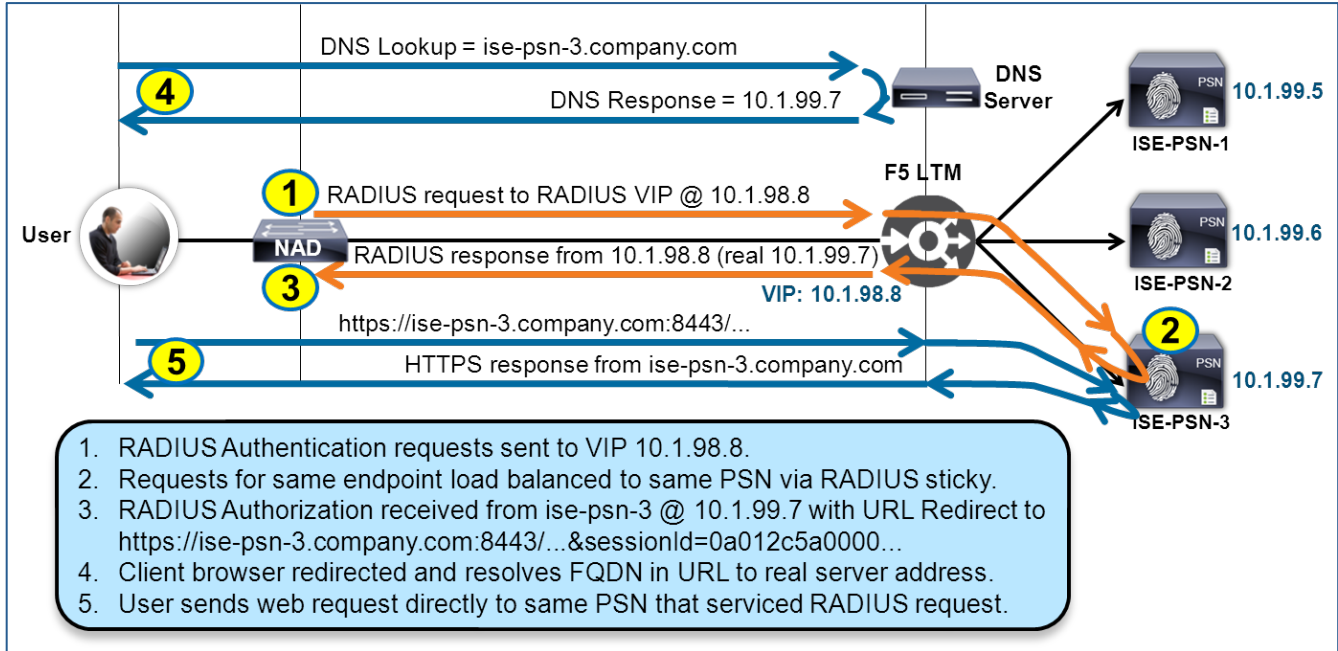


Figure 45. URL-Redirect Traffic Flow

Note that the redirected web request always follows the PSN that is servicing the RADIUS session. Also note that the web request is sent directly to a specific PSN IP address and not to a Virtual Server IP address on the F5 BIG-IP LTM. If RADIUS is load balanced, then the resulting redirected web service is also load balanced.

In summary, sessionized URL-Redirected web services are implicitly load balanced based on RADIUS connections and do not require any explicit F5 LTM load balancing configuration.

Shared PSN Portal Interface for URL-Redirected Portals

If the ISE PSNs are configured to use a single interface for RADIUS and web services, then the HTTPS communications must be allowed using the general IP forwarding rule. For reference, the default ports for most redirected web services include TCP/8443, TCP/8444, and TCP/8905.

Dedicated PSN Portal Interface for URL-Redirected Portals

If the ISE PSNs are configured to use a dedicated interface for web services, then all client HTTPS traffic to the PSNs can bypass the F5 BIG-IP LTM. ISE 1.3 and above simplifies the separation of traffic flows by supporting multiple default gateways per interface. This allows traffic received on the web service interface to be sent out same interface while allowing isolation of RADIUS and management traffic on a different interface. Under ISE 1.2 and earlier releases, only a single default gateway is supported. Therefore, the most effective method to bypass the F5 LTM appliance would be to Source NAT the client traffic on a Layer 3 switch before it reaches the web portal network. The PSNs can then respond to a locally NATted address or be configured with a static route to the SNAT address/network via the web portal interface.

The diagram depicts the deployment of separate PSN interfaces for RADIUS and Web Services. TCP-based traffic from user networks to the web portal network (10.1.91.0/24) and service ports is Source NATted by the Layer 3 switch. This design simplifies the PSN routing configuration (allows simple default gateway), maintain path isolation, and allows client web traffic to completely bypass the BIG-IP LTM IP Forwarding server.

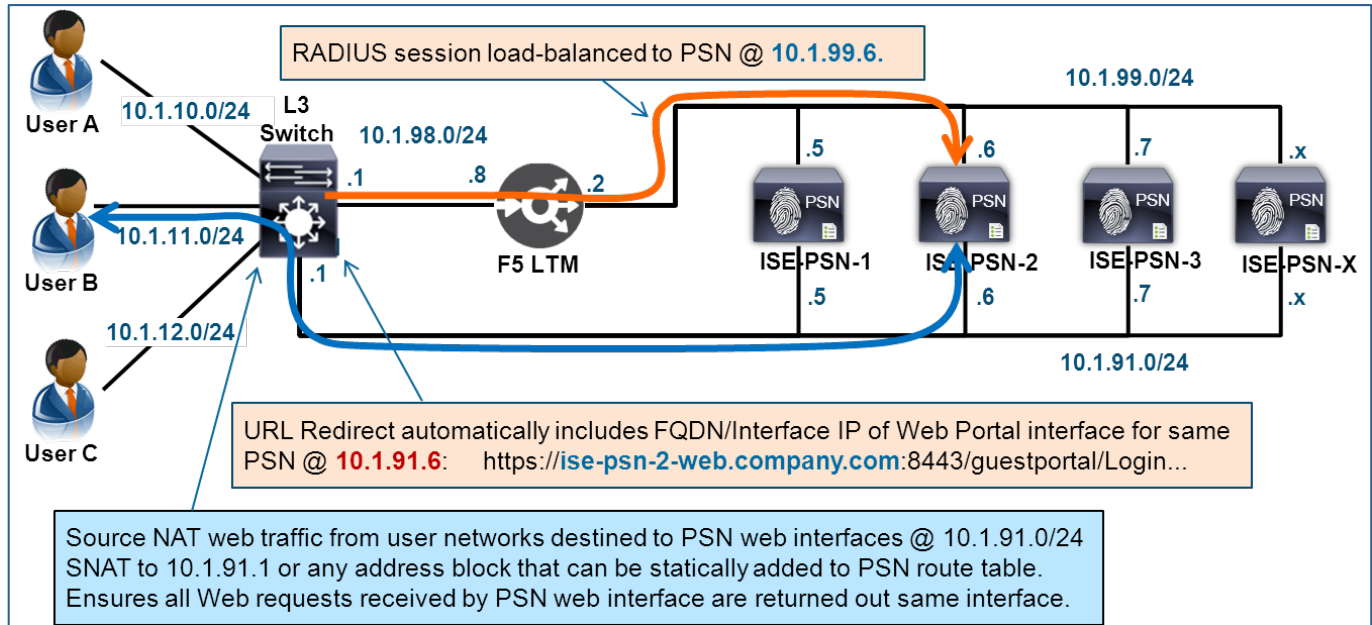


Figure 46. URL-Redirected Traffic Flow Using Multiple PSN Interfaces

Sample SNAT Configuration—Cisco Catalyst Switch

```

!
interface Vlan10
 ip address 10.1.10.1 255.255.255.0
 ip nat inside
!
interface Vlan11
 ip address 10.1.11.1 255.255.255.0
 ip nat inside
!
interface Vlan12
 ip address 10.1.12.1 255.255.255.0
 ip nat inside
!
interface Vlan91
 ip address 10.1.91.1 255.255.255.0
 ip nat outside
!
ip nat inside source list ise-guest interface Vlan91 overload
!
ip access-list extended ise-guest
 permit tcp any host 10.1.91.5 range 8000 8999
 permit tcp any host 10.1.91.6 range 8000 8999
 permit tcp any host 10.1.91.7 range 8000 8999
!

```

Refer to the “Load Balancing Sponsor, My Devices, and LWA Portals” section for more details on shared versus dedicated PSN interfaces. The section includes an example of using SNAT on the F5 LTM appliance to support HTTPS load balancing for specific ISE web portals while still supporting URL-Redirected HTTPS flows on dedicated PSN interfaces.

Direct-Access Web Services

In addition to URL-Redirected web services, ISE supports a number of portals that are accessed through manual navigation of a client browser or through a static configuration on a network access device or web page. These portals are not accessed as the result of URL redirection sent in a RADIUS authorization. This category of web-based services includes the following:

- Admin access
- Sponsor Portal
- My Devices Portal
- Local Web Authentication (LWA)

With the exception of Admin access, all of these portal services can be load balanced using F5 BIG-IP LTM. Admin client requests should always be sent to the Primary Administration Node (PAN) so load balancing with the Secondary PAN does not apply.

Both the Sponsor and My Devices portals are accessed by entering the appropriate URL into the client browser. Access does not rely on sessionization and therefore not tied to a specific RADIUS session. These services may be accessed on any PSN where User Services are enabled on the PSN.

LWA is typically configured as a static URL on the network access device. Unlike CWA, LWA does not rely on sessionization and the ISE portal is simply used as a means to capture user credentials for submission by the access device during RADIUS authentication.

F5 BIG-IP load balancing of Sponsor, My Devices, and LWA can significantly improve user experience, scalability, and redundancy since URLs are no longer limited to a single static value that points to a single PSN. Instead, the URL that is provided to guest sponsors and registrants can resolve to an F5 LTM Virtual Server IP address that can be processed by any one of many PSNs in the load-balanced cluster. Similarly, network access devices that require LWA support (for example, older platforms/versions of the Cisco Wireless LAN Controller) can be configured with a single external web portal URL that is serviced by multiple PSNs behind an F5 LTM VIP.

Web Portal Load Balancing Traffic Flow

The diagram depicts a sample traffic flow for load balancing the Sponsor Portal. The same flow applies to My Devices Portal and LWA. The client web request is sent to the F5 LTM VIP and load balanced to an available PSN member in the Virtual Server Pool.

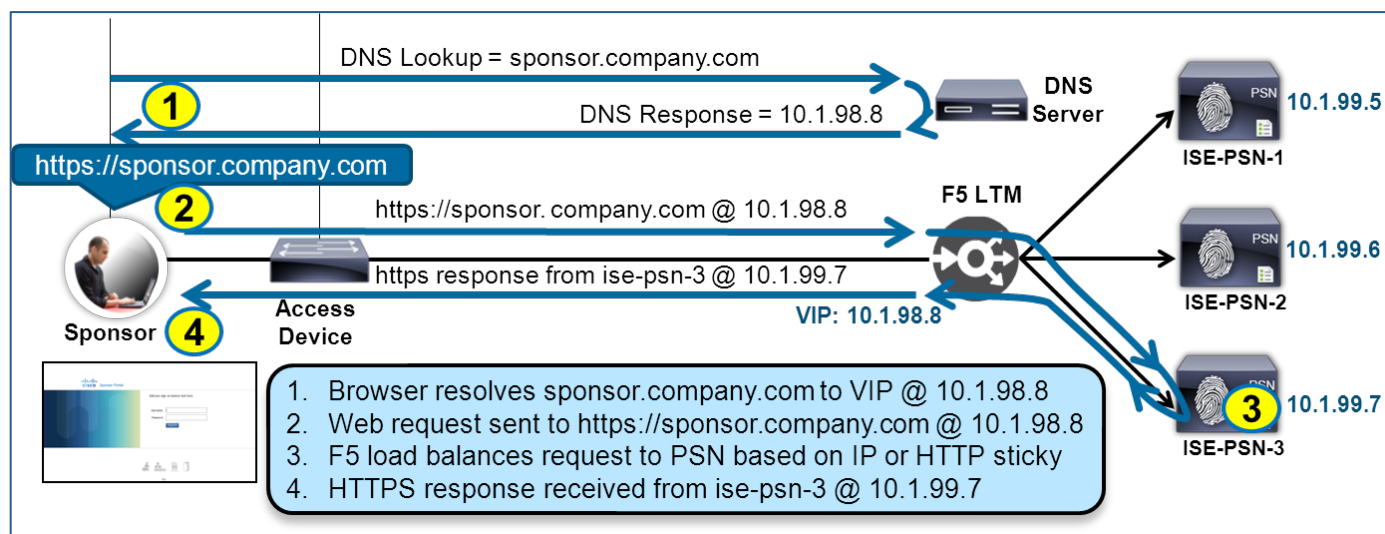


Figure 47. Web Portal Load Balancing Traffic Flow

Load Balancing Sponsor, My Devices, and LWA Portals

The default HTTPS service port for the ISE Sponsor, My Devices, and LWA Portals is TCP/8443. The port is configurable in ISE so make sure to validate the service port when configuring the Virtual Server in F5 BIG-IP LTM.

Shared PSN Portal Interface for Direct-Access Portals

The portals can share the same PSN interface and IP address as RADIUS AAA services or can be hosted on one or more dedicated PSN interfaces. If the portals share the RADIUS interface, typically GigabitEthernet0, then the Virtual Server IP address for RADIUS LB can also be shared but TCP service ports will be unique to the web portal configuration. Member nodes will share the same IP addresses as RADIUS pool members but will also use unique TCP service ports that match the portal configuration.

Dedicated PSN Portal Interface for Direct-Access Portals

If dedicated PSN interfaces are used for web services, the Virtual Server IP address may still be shared with RADIUS, but the member nodes must be configured to use their interface-specific IP addresses and service ports. Alternatively, a separate Virtual Server IP address may be configured if policy requires full separation between RADIUS control traffic and client web traffic.

ISE 1.3 and above simplifies the separation of traffic flows by supporting multiple default gateways per interface. This allows traffic received on the web service interface to be sent out same interface while allowing isolation of RADIUS and management traffic on a different interface.

Under ISE 1.2 and earlier releases, the PSNs forward traffic based on its static routing table. The nodes do not automatically send return traffic on the receiving interface. Consequently, if only a single default gateway is configured on each PSN, web return traffic from the PSNs will take the same path as RADIUS and other management traffic. Although possible to configure static routes for each destination network to achieve symmetric traffic flows, this process can prove to be very management intensive, error prone, and sometimes impossible based on the addressing scheme of the network. Therefore, if path isolation is required between PSN interfaces and services, then F5 LTM should perform source NAT on web traffic so that PSNs reply on the same interface.

The diagram depicts an example configuration using a dedicated PSN interface for web services. All web portal traffic will automatically be routed to the correct PSN but return traffic will be sent out the management interface, by default. SNAT on the F5 BIG-IP LTM can ensure responses are returned to the F5 LTM interface connected to the portal network.

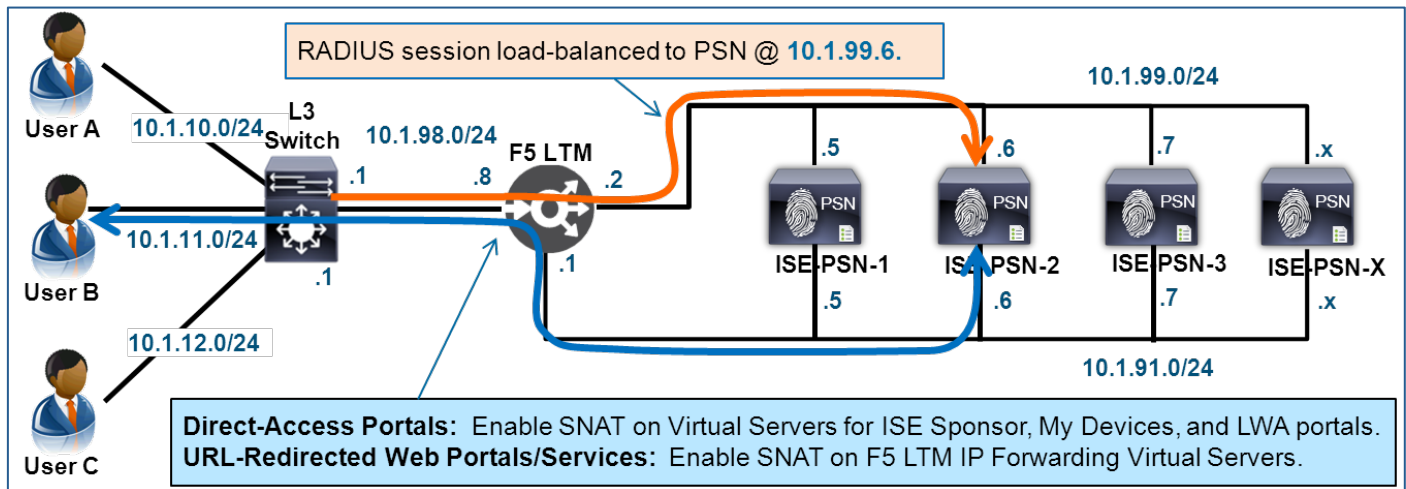


Figure 48. Web Portal Load Balancing Traffic Flow Using Multiple Interfaces

Note: When deploying a separate, dedicated interface for additional ISE services like web portals or profiling, be sure to configure the upstream Layer 3 switch/router with a static route to the isolated network that points to the F5's interface IP address as the next hop.

ISE Web Portal Interfaces and Service Ports

The specific interfaces and ports for ISE web portals and services are configured under the ISE Guest configuration. Verify the ISE settings before configuring the F5 BIG-IP LTM to use specific ISE IP addresses and ports.

ISE 1.3: The portal interface and service port are configured under the individual portal configuration.

- **Sponsor Portals:** Guest Access > Configure > Sponsor Portals > (Portal Name) > Portal Behavior and Flow Settings > Portal Settings
- **My Devices Portals:** Administration > Device Portal Management > My Devices > (Portal Name) > Portal Behavior and Flow Settings > Portal Settings
- **LWA Portals:** Guest Access > Configure > Guest Portals > (Portal Name) > Portal Behavior and Flow Settings > Portal Settings

Under ISE 1.2, all portal interface and service ports are defined under **Administration > Web Portal Management > Settings > General > Ports**. Default settings are shown in the diagram.

Web Portal Settings

Admin Portal Settings

HTTP Port

HTTPS Port

Blacklist Portal Settings

HTTPS Port (Valid Range 8000 to 8999)

Allowed Interfaces GigabitEthernet 0
 GigabitEthernet 1
 GigabitEthernet 2
 GigabitEthernet 3

Guest Portal and Client Provisioning Portal Settings

HTTPS Port (Valid Range 8000 to 8999)

Allowed Interfaces GigabitEthernet 0
 GigabitEthernet 1
 GigabitEthernet 2
 GigabitEthernet 3

My Devices Portal Settings

HTTPS Port (Valid Range 8000 to 8999)

Allowed Interfaces GigabitEthernet 0
 GigabitEthernet 1
 GigabitEthernet 2
 GigabitEthernet 3

Sponsor Portal Settings

HTTPS Port (Valid Range 8000 to 8999)

Allowed Interfaces GigabitEthernet 0
 GigabitEthernet 1
 GigabitEthernet 2
 GigabitEthernet 3

Portal FQDNs

Default Sponsor Portal FQDN

Default My Devices Portal FQDN

Figure 49. ISE 1.2 Web Portal Interfaces and Ports Configuration

Note the option at the bottom of the ISE 1.2 configuration page to set the FQDN for the Sponsor and My Devices Portals. For ISE 1.3, these FQDN values are configured within the portal along with the interface/port settings. Portal FQDNs allow requests sent to these URIs using HTTP or HTTPS to be automatically redirected to the respective portal on the specified HTTPS Port. For example, an employee that enters `http://sponsor.company.com` into their browser will be redirected to `https://sponsor.company.com:8443/sponsorportal`. The same redirection will occur if `https` is used in the initial web request.

Note: To support load balancing to the Sponsor, My Devices, and LWA portals, be sure DNS is properly configured so that these FQDNs resolve to the correct F5 Virtual Server IP address.

The following rules apply to the load-balancing configuration of two or more portals (Sponsor, My Devices, LWA):

- If multiple portals share the same PSN interfaces and service ports, then the same Virtual Servers and Pools may be defined to cover all.

- If multiple portals use different PSN interfaces or service ports, then separate Virtual Servers with separate Pools must be defined for each unique combination.

Virtual Servers and Pools to Support Portal FQDNs and Redirection

Both Sponsor and My Devices Portals support Portal FQDNs. As previously discussed, Portal FQDNs simplify portal access by providing a user-friendly and abbreviated web destination to be used instead of a more complex URL that includes portal number, portal name, and other parameter details. The portal FQDN should be easy to remember. End users can enter this simplified URL into their browser using either HTTP or HTTPS on their default ports (TCP/80 and TCP/443, respectively), and the ISE PSN node will automatically redirect the user's browser to the specific portal on its unique service port.

To facilitate the Portal FQDN functionality without requiring F5 LTM to perform the interception and translation, it is recommended to configure three Virtual Servers for the Sponsor and/or My Devices portals—one each for the initial HTTP/S and another for the actual target portal and service port. Using this configuration, the initial portal request will hit the Virtual Server on either TCP/80 or TCP/443 and be redirected by ISE to TCP/8443, for example. Although separate F5 LTM Pools could be configured on each port, we will simplify the backend configuration by using a single pool that services requests on any port.

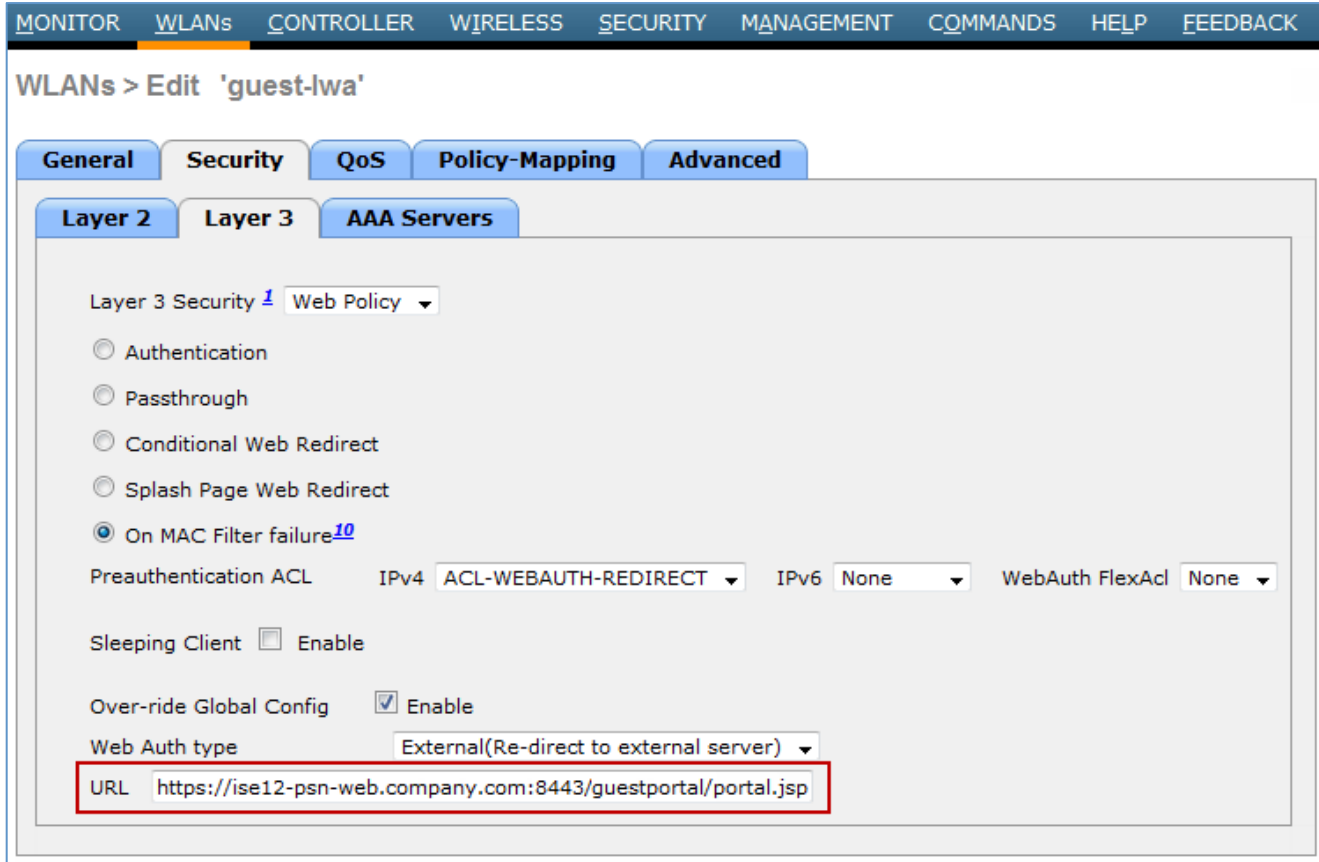
LWA Configuration Example for Cisco Wireless Controller

When LWA is deployed, the destination portal URL is manually configured into the network access device. Since the end user is not required to remember or type in the URL, it is not necessary to simplify the configured URL. In these cases, the detailed URI for the specific portal including target port, path, and parameters can be defined without relying on redirection. The specific URL syntax will depend on ISE version.

- ISE 1.2 LWA Portal Examples:
 - `https://LWA_VIP_FQDN:8443/guestportal/portal.jsp` (default portal)
 - `https://LWA_VIP_FQDN:8443/guestportal/portals/portal_name/portal.jsp`
 - `https://LWA_VIP_FQDN:8443/guestportal/Login.action?portalname=portal_name`
- ISE 1.3 LWA Portal Example:
 - `https://LWA_VIP_FQDN:8443/portal/PortalSetup.action?portal=portal_name`

[where **LWA_VIP_FQDN** is the DNS FQDN assigned to the F5 LTM Virtual Server IP used for LWA and **portal_name** is the name of the portal (case sensitive).]

The diagram shows an example Cisco WLC configuration for defining an F5 LTM VIP FQDN as the target for an LWA portal.



MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'guest-lwa'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 3 Security ¹ Web Policy ▾

Authentication
 Passthrough
 Conditional Web Redirect
 Splash Page Web Redirect
 On MAC Filter failure¹⁰

Preauthentication ACL IPv4 ACL-WEBAUTH-REDIRECT ▾ IPv6 None ▾ WebAuth FlexAcl None ▾

Sleeping Client Enable

Over-ride Global Config Enable

Web Auth type External(Re-direct to external server) ▾

URL https://ise12-psn-web.company.com:8443/guestportal/portal.jsp

Figure 50. Static URL Configurations for LWA on Cisco Wireless Controllers

In the above example, **ise12-psn-web.company.com** is the FQDN that resolves to the F5 LTM VIP address assigned to the LWA portal(s).

HTTPS Persistence for Direct-Access Portals

Clients that connect to the Sponsor, My Devices, and LWA portals are not bound to a specific RADIUS server and can therefore connect to any PSN that offers the web service. Each client attempts to connect directly to the portal using his or her own IP address, so persistence can be set using simple source IP address. The persistence timeout can be set to a sufficient amount of time client is expected to connect to portal and complete the transaction. The setting should be commensurate with the sponsor portal inactivity timeout, say 20 minutes (default value in ISE 1.2).

HTTPS Health Monitoring

F5 BIG-IP LTM Monitors are used to perform periodic health checks against node members in a load-balanced pool. These monitors, or probes, validate that a real server is healthy before sending it requests. The term *healthy* is a relative term which can range in meaning from “Server is IP reachable using ICMP ping” to “Server is actively and successfully responding to simulated application requests; additionally, out-of-band checks validate resources are sufficient to support additional load”.

F5 LTM Monitor for HTTPS

F5 LTM includes an HTTPS monitor that will be used for monitoring the web portal health of the ISE PSN servers. It will periodically send a simulated web request to each PSN in the load-balanced pool and verify that a valid response is received. In this guide, we will treat a simple “200 OK” as valid response for the destination portal.

A single pool will be configured and shared for all web portals that use the same PSN interface and service port. A single probe is configured for a given portal interface and service port. This probe is defined under the shared pool and can be used by multiple Virtual Servers that share the same web portal ports. This will reduce the number of monitor requests sent to each PSN.

HTTPS Monitor Timers

The Monitor timer determines how frequently the health status probes are sent to each member of a load-balanced pool. Timers should be set short enough to allow failover before a HTTP/S request from a user’s browser times out and long enough to prevent excessive and unnecessary load on the ISE PSNs.

The initial recommendation is to use the default timeout settings for the F5 LTM HTTPS Monitor. The F5 LTM HTTPS Monitor has two key timer settings:

- Interval = probe frequency (default = 5 sec)
- Timeout = total time before monitor fails (default = 16 seconds)

Therefore, we can deduce that four health checks are attempted before declaring a node failure:

- $\text{Timeout} = (3 * \text{Interval}) + 1$

Sample F5 LTM Monitor configuration for HTTPS (ISE 1.2):

```
ltm monitor https /Common/ise_https_8443 {
  cipherlist DEFAULT:+SHA:+3DES:+kEDH
  compatibility enabled
  defaults-from /Common/https
  destination *:8443
  interval 5
  password xxx
  recv "HTTP/1.1 200 OK"
  send "GET /sponsorportal/"
  time-until-up 0
  timeout 16
  username xxx
}
```

User Account Selection for HTTPS Probes

The HTTPS Monitor used in this guide requires that a user account be configured to send in the periodic monitor request. To receive a valid response, it is not necessary to specify a valid account. In the monitor example shown, the values **xxx** are the *actual* settings configured and not dummy values.

HTTPS Load Balancing: F5 LTM Configuration Details

This section provides the detailed F5 LTM configuration for HTTP/S load balancing of ISE PSN servers including the recommended settings and considerations for each component.

The HTTPS Load Balancing configuration is broken down into the following major components:

- HTTPS Health Monitor
- Profiles
 - TCP
 - Persistence
- Pool Lists for Web Portals
- Virtual Servers for HTTP and HTTPS

Use the settings outlined in the table to configure F5 LTM for HTTPS load balancing with ISE PSNs.

Table 8. LTM HTTPS Load Balancing Configuration

BIG-IP LTM Object	Recommended Setting	Notes
Health Monitor (Main tab > Local Traffic > Monitors)		
Name	<HTTPS Monitor Name> Example: ise_https_8443	<ul style="list-style-type: none"> • Enter a name for the HTTPS health monitor. • If the Sponsor, My Devices, or LWA portals use different service ports or interfaces, then a separate monitor should be configured for each unique combination.
Type	HTTPS	<ul style="list-style-type: none"> • F5 provides a native monitor for HTTPS, the protocol used for the ISE web portals.
Interval	5 seconds	<ul style="list-style-type: none"> • Default setting
Timeout	16 seconds	<ul style="list-style-type: none"> • Default setting
Send String	<Web Request String> ISE 1.2 Examples: GET /sponsorportal/ GET /mydevicesportal/ ISE 1.3 Examples: GET /sponsorportal/PortalSetup.action?portal=Sponsor%20Portal%20%28default%29 GET /sponsorportal/PortalSetup.action?portal=My%20Devices%20Portal%20%28default%29	<ul style="list-style-type: none"> • If portals share same service port, then either example shown could be used. If Sponsor Portal is active on specified port, then My Devices Portal on same port should be healthy, and vice versa. • The ISE 1.3 examples show options for requesting the default Sponsor and My Devices portals. Since the portal names include special characters, the Unicode equivalents have been specified, where %20 matches a space and %28 and %29 match open and closed parenthesis, respectively.

Receive String	<Web Response String> Example: HTTP/1.1 200 OK		<ul style="list-style-type: none"> The probe will send requests to the actual service port, for example TCP/8443. The expected response is 200 OK rather than 302 Not Found which is expected during redirection.
User Name	<User Name for web portal authentication> Example: xxx		<ul style="list-style-type: none"> Any User Name may be specified and does not need to be a valid user account.
Password	<User Name for web portal authentication> Example: xxx		<ul style="list-style-type: none"> Any Password may be specified and does not need to be a valid password.
Alias Service Port	8443 (Configurable on ISE)		<ul style="list-style-type: none"> Enter the service port configured on ISE for specific web portal type.
Profiles (Main tab > Local Traffic > Profiles)			
TCP (Protocol > TCP)	Name	<Profile Name> Example: ise_https_tcp	<ul style="list-style-type: none"> Type a unique name for the TCP profile. Default tcp profile can be used, but defining unique profile allows for customization without disruption to other servers that may be sharing same parent profile.
	Parent Profile	tcp	
	Idle Timeout	300	<ul style="list-style-type: none"> Default setting
Persistence	Name	<Profile Name> Example: https_sticky	<ul style="list-style-type: none"> Type a unique name for the HTTPS persistence profile.
	Parent Profile	source_addr	<ul style="list-style-type: none"> Universal profile allows specification of an iRule for advanced persistence logic
	Match Across Services	Enabled	<ul style="list-style-type: none"> When using separate Virtual Servers that share the same IP address but different service ports, this setting allows load balancing to persist across Web portals and services. No requirement to Match Across Servers if the Virtual Servers for web portals share the same IP address. For more information, see F5 support article SOL5837: Match Across options for session persistence.
	Timeout	<Persist Timeout> Example: 1200 seconds (20 minutes)	<ul style="list-style-type: none"> Recommendation is to set value commensurate with portal inactivity timer or time expected for user to complete task. See “HTTPS Persistence” section for more details on recommended timeout values.

<p>Pool List (Main tab > Local Traffic > Pools > Pool List)</p> <p>The Pool List contains the list of real servers that service load balanced requests for a given Virtual Server.</p> <p>Note: Create one server pool that is shared for all Sponsor, My Devices, and LWA portals that share the same PSN interface and service port. If applicable, create additional server pools for each unique interface and service port defined for Sponsor, My Devices, and LWA portals. If all portals use same PSN interface port, for example 8443, then a single pool is required.</p>		
Name	<p><Pool Name></p> <p>Example: web_portals_pool</p>	<ul style="list-style-type: none"> Type a unique name for the portal pool—one pool will be shared by the Virtual Servers used for HTTP (Port 80) and HTTPS (443) as well as the unique service port (Port 8443 by default).
Health Monitors	<p><RADIUS Health Monitor></p> <p>Example: ise_https_8443</p>	<ul style="list-style-type: none"> Enter the HTTPS Health Monitor configured in previous step.
Allow SNAT	<p>Shared PSN Interface: (Optional)</p> <p>Dedicated PSN Interface: Yes</p>	<ul style="list-style-type: none"> If PSNs have only one interface used for RADIUS and HTTPS, then this can optionally be set to No. SNAT is required if PSNs will use a separate interface for web portal connections.
Member IP Addresses	<p><ISE PSN addresses in the LB cluster></p> <p>Shared Interface Examples:</p> <p>ise-psn-1: 10.1.99.5</p> <p>ise-psn-2: 10.1.99.6</p> <p>ise-psn-3: 10.1.99.7</p> <p>Dedicated Interface Examples:</p> <p>ise-psn-1-web: 10.1.91.5</p> <p>ise-psn-2-web: 10.1.91.6</p> <p>ise-psn-3-web: 10.1.91.7</p>	<ul style="list-style-type: none"> These are the real IP addresses of the PSN appliances. The PSNs are configured as nodes under the Node List. These entries can be automatically created when defined within the Pool List configuration page. These IP addresses are the same as the RADIUS pool members when sharing a single PSN interface. These IP addresses are different than the RADIUS pool member interfaces when dedicated portal interfaces are configured.
Member Service Port	<p>0</p>	<ul style="list-style-type: none"> Although valid to create separate pools and member nodes that listen on unique ports (TCP/80, TCP/443, TCP/8443, for example), this guide will use a single pool per unique interface/portal port combination. The use of the wildcard port simplifies the configuration and allows requests on any TCP port.
Load Balancing Method	<p>Least Connections (node)</p>	<ul style="list-style-type: none"> Alternative LB methods include Fastest (application). Least Connections (member) also viable, but 'node' option allows F5 to take into consideration all connections across pools.
<p>HTTP/S Virtual Server (Main tab > Local Traffic > Virtual Servers > Virtual Server List)</p> <p>Note: Create one virtual server for each group of web portals using a unique service port</p>		

Name	<HTTPS Virtual Server Name> Examples: HTTP (80): ise_http_portals HTTPS (443): ise_https_portals HTTPS (8443): ise_https8443_portals		<ul style="list-style-type: none"> • Enter the name to identify the virtual servers for HTTP/S Load Balancing. • Create one virtual server for each group of web portals using a unique interface and service port.
Type	Standard		<ul style="list-style-type: none"> • Standard type allows specification of profiles for the TCP and HTTP Protocols.
Source	<Source Network Address/Mask> Example: 10.0.0.0/8		<ul style="list-style-type: none"> • Type the network address with bit mask for the external users that need to communicate with the ISE PSNs. • Make the source as restrictive as possible while not omitting users that need to communicate to the PSNs for web services.
Destination (VIP Address)	Type	Host	
	Address	<Single IP Address for RADIUS and HTTPS> Example: 10.1.98.8	<ul style="list-style-type: none"> • Enter the Virtual IP Address for ISE web services. • Define a unique IP address (versus same IP addresses for RADIUS AAA) if require client portal traffic to connect on a different interface than RADIUS/management traffic.
Service Port	<PSN Portal Port> Examples: HTTP: 80 HTTPS: 443 HTTPS over 8443: 8443		<ul style="list-style-type: none"> • Configure the web service ports to match the ISE settings.
Protocol	TCP		
Protocol Profile (Client)	<TCP Protocol Profile> Example: ise_https_tcp		<ul style="list-style-type: none"> • Enter the name of the TCP Protocol Profile defined earlier.
HTTP Profile	None		<ul style="list-style-type: none"> • No HTTP Services Profile required. Inclusion here is to simply note explicit setting to not specify a profile.
VLAN and Tunnel Traffic	Enabled On...		<ul style="list-style-type: none"> • Optional: Restrict inbound web requests to specific VLANs.
VLANs and Tunnels	<External VLANs> Example: External		<ul style="list-style-type: none"> • Select the ingress VLAN(s) used by external client users to access the PSN web portals.

Source Address Translation, or "SNAT Pool"	Shared interface: None Dedicated interfaces: SNAT > Auto Map	<ul style="list-style-type: none"> If RADIUS and Web Portals share the same PSN interface, then SNAT should be set to None. If RADIUS and Web Portals use different PSN interfaces, then SNAT should be set to Auto Map.
Default Pool	<Pool Name> Example: web_portals_pool	<ul style="list-style-type: none"> Select the Server Pool name defined for HTTP/S. See "Pool List" section in table for more details.
Default Persistence Profile	<Persistence Profile Name> Example: https_sticky	<ul style="list-style-type: none"> Select the name of the HTTPS Persistence Profile created earlier.

Virtual Server (Inbound Web) (Main tab > Local Traffic > Virtual Servers > Virtual Server List)

Note: Create a new virtual server for IP Forwarding if using a dedicated PSN web interfaces and require support for URL-Redirected traffic.

Name	<IP Forwarding Server Name> Example: PSN-IP-Forwarding-Inbound-Web		<ul style="list-style-type: none"> Type the name of the virtual server for IP Forwarding URL-Redirected traffic from external hosts to the PSNs.
Type	Forwarding (IP)		<ul style="list-style-type: none"> Forwarding (IP) allows traffic that does not require load balancing (URL-Redirected traffic) to be forwarded by F5 to the PSNs.
Source	<Source Network Address/Mask> Example: 10.0.0.0/8		<ul style="list-style-type: none"> Type the network address with bit mask for the external network users that need to communicate with the PSN web portals. Make the source as restrictive as possible while not omitting hosts that need to communicate directly to the PSNs.
Destination	Type	Network	
	Address	<Destination Network> Example: 10.1.91.0	<ul style="list-style-type: none"> Enter the PSN network address used for the web portals. For added security, make the address range as restrictive as possible.
	Mask	<Destination Mask> Example: 255.255.255.224	<ul style="list-style-type: none"> Enter the PSN network address mask appropriate to your environment. For added security, make the address range as restrictive as possible

Service Port	8443 or * (wildcard)	<ul style="list-style-type: none"> • Single URL-Redirect Service/Port: Enter specific web service port to restrict URL-Redirected flows to a specific port • Multiple Ports for Services/Portals: Enter the wildcard service port if need to match web-based services or if multiple service ports are used. For example, some URL-redirected web services like Posture and Provisioning rely on TCP/8905 and UDP/8905. An alternative option is to create separate IP Forwarding servers for each required port.
Protocol	TCP or * All Protocols	<ul style="list-style-type: none"> • For single portal/port, select TCP. For multiple portal ports/services, select the wildcard protocol to match all protocols by default.
VLAN and Tunnel Traffic	Enabled On...	<ul style="list-style-type: none"> • Optional: Restrict inbound IP forwarding to specific VLANs.
VLANs and Tunnels	<External VLANs> Example: External	<ul style="list-style-type: none"> • Select the ingress VLAN(s) used by external hosts to communicate with the PSNs.
Source Address Translation, or "SNAT Pool"	SNAT > Auto Map	<ul style="list-style-type: none"> • If RADIUS and Web Portals use different PSN interfaces, then SNAT should be set to Auto Map.

Global ISE Load Balancing Considerations

This section provides a brief overview of high availability options for a distributed ISE deployment where PSNs may be located in different geographic locations. It includes a high level discussion on considerations and solutions, but deployment details for each are beyond the scope of this guide.

The focus of the guide has been on the load balancing of ISE PSN services located in the same location and Local Area Network (LAN). In a given campus network, there is typically a single, load-balanced cluster of PSNs all connected through high-speed network connections—most commonly all in the same subnet or connected to same redundant server switches. F5 BIG-IP LTM is the prime solution for this use case.

Customer business continuity requirements often extend beyond a single campus. The ISE deployment must be able to support geographic redundancy to recover from single points of failure such as a WAN outage or catastrophic data center loss (for example, extended power outage or natural disaster). In these cases, remote locations need to be able to failover to a secondary data center, hub location, or disaster recovery site.

Potential solutions include the following:

- RADIUS AAA: Configure NADs with secondary/tertiary RADIUS Servers. Each entry may point to an F5 Virtual Server IP or individual PSNs.

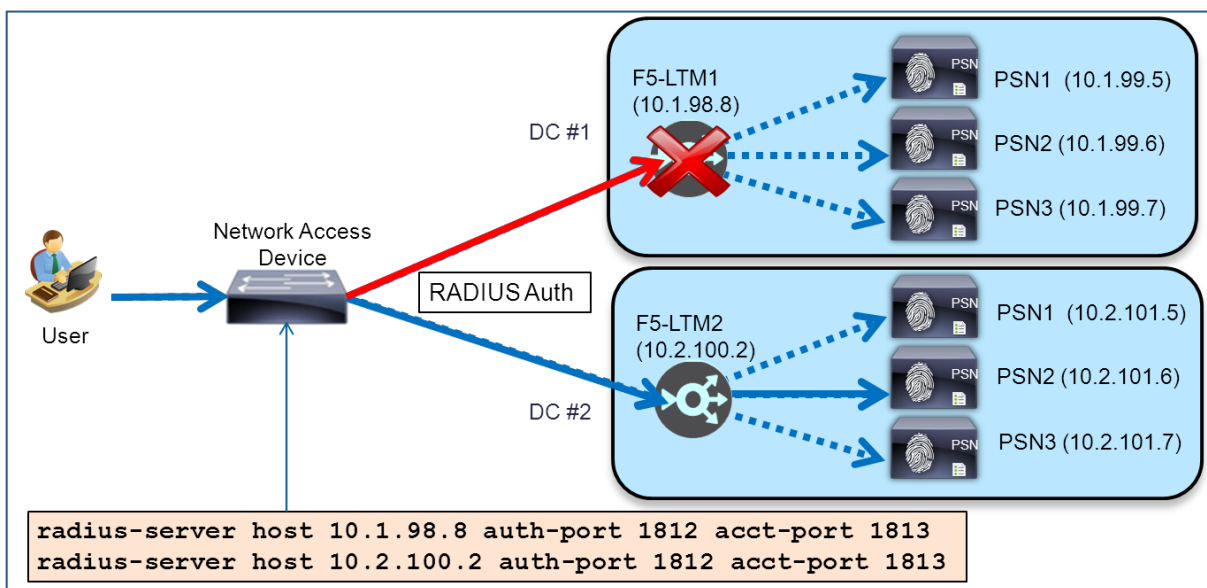


Figure 51. RADIUS Server Redundancy Using Multiple Server Definitions

- RADIUS AAA: Configure NADs with a single RADIUS Server that points to an IP Anycast address. Each F5 BIG-IP LTM appliance can be configured with this same Anycast address as the VIP for RADIUS AAA. Individual PSNs with a dedicated RADIUS interface may also share this same IP address.

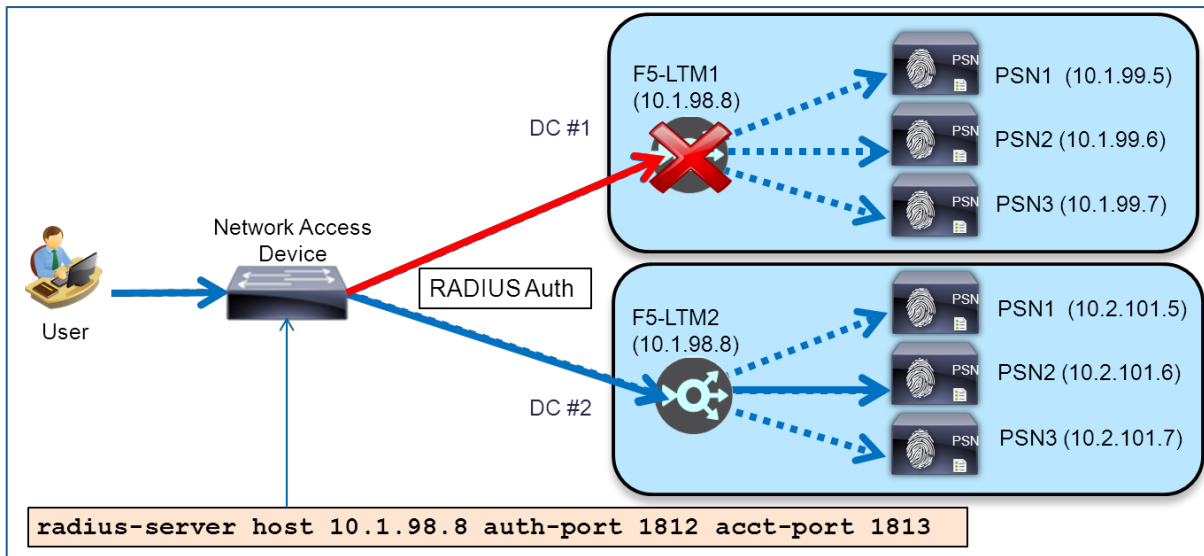


Figure 52. RADIUS Server Redundancy Using Anycast

- DHCP/SNMP Trap Profiling: For DHCP, configure L3 gateways with secondary/tertiary IP Helper statements. For SNMP Traps, configure access devices with secondary/tertiary SNMP Trap hosts. Each entry may point to an F5 Virtual Server IP or individual PSNs.

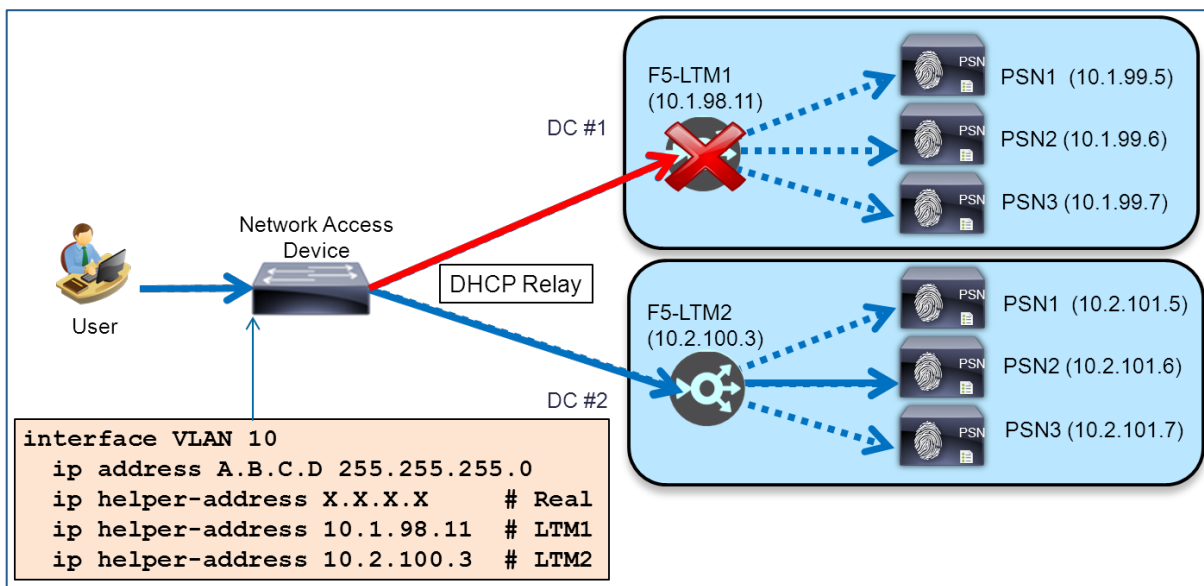


Figure 53. DHCP Profiling Redundancy Using Multiple IP Helpers

DHCP/SNMP Trap Profiling: For DHCP, configure L3 gateways with a single IP Helper entry that points to an IP Anycast address. For SNMP Traps, configure access devices with a single SNMP Trap host that points to an IP Anycast address. Each F5 BIG-IP LTM appliance can be configured with this same IP Anycast address as the VIP for DHCP/SNMP Trap Profiling. Individual PSNs with a dedicated profiling interface may also share this same IP address.

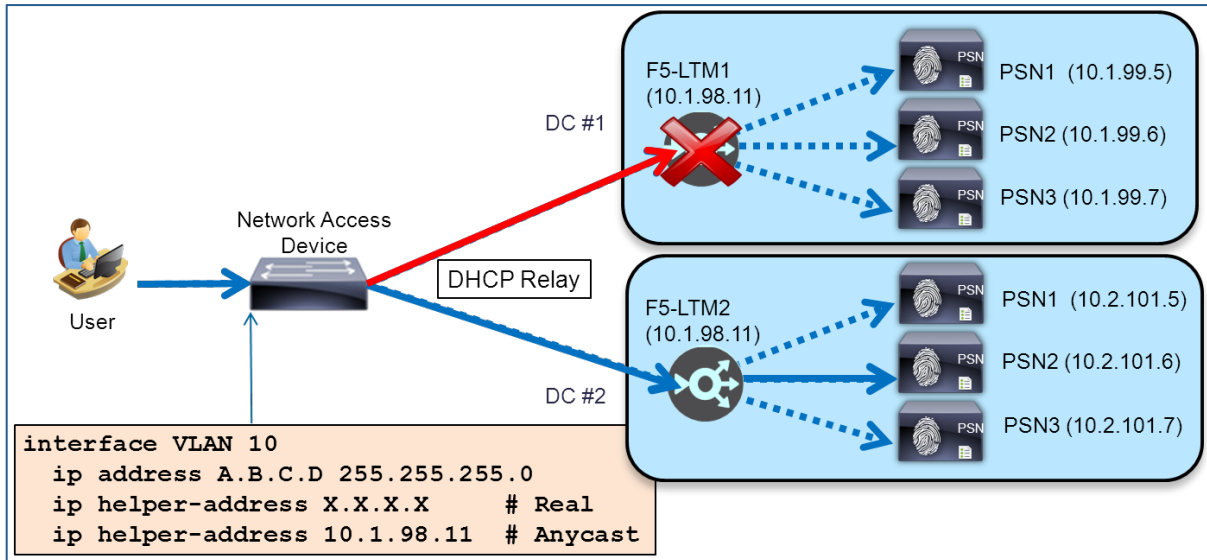


Figure 54. DHCP Profiling Redundancy Using Anycast

- HTTPS Portals: Deploy intelligent Domain Name Service to resolve DNS lookups to different IP addresses based on availability, performance, or proximity. The returned address may point to an F5 Virtual Server IP or individual PSNs. Solutions in this space range from simplistic DNS Round-Robin to more sophisticated offerings such as F5’s BIG-IP Global Traffic Manager (GTM) or Cisco’s Global Site Selector (GSS). When deployed with existing LTMs, F5 BIG-IP GTM offers a number of additional management and feature benefits.

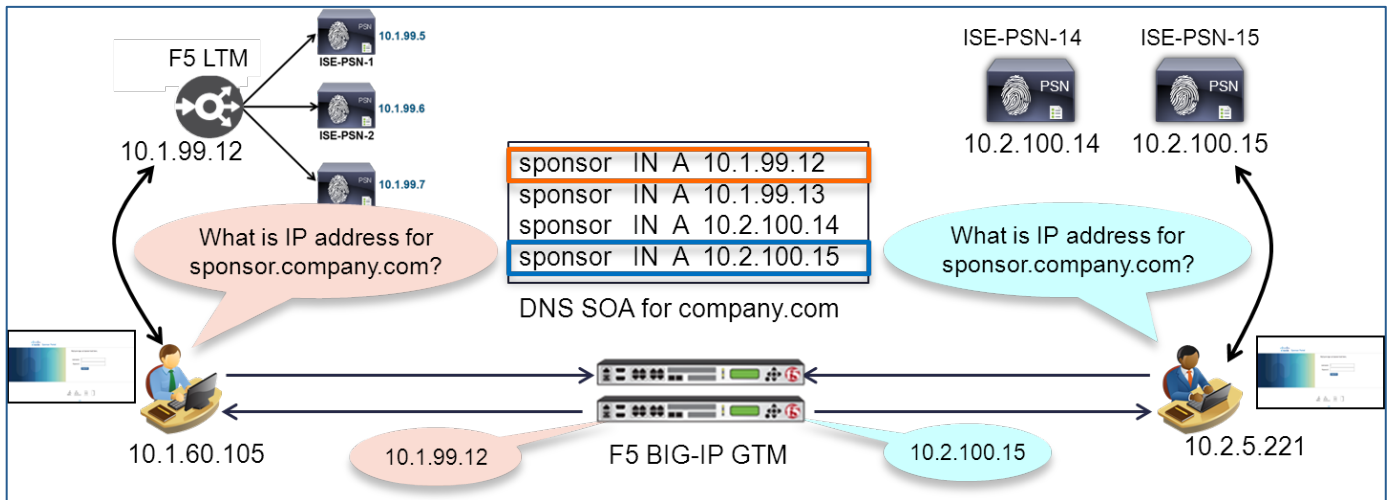


Figure 55. Web Portal Redundancy Using GTM

- HTTPS Portals: Configure DNS with a single portal FQDN for each service that resolves to a single IP Anycast address. Each F5 BIG-IP LTM appliance can be configured with this same Anycast address as the VIP for the specific HTTPS portal. Individual PSNs with a dedicated web portal interface may also share this same IP address. This option does not require advanced DNS capabilities but the F5 BIG-IP GTM can still be leveraged for other DNS feature enhancements.

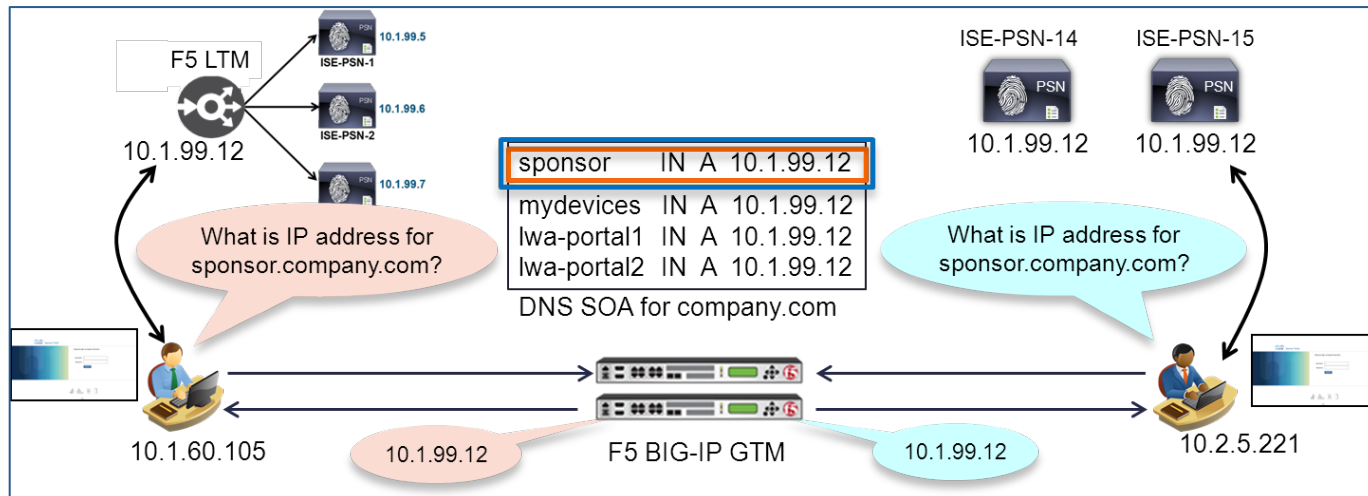


Figure 56. Web Portal Redundancy Using Anycast

Some of the options entail the use of IP Anycast. IP Anycast is simply the ability to assign the same IP address to multiple hosts in the network and to rely on routing to forward the packet from the source to a single target host. When this method is used it is critical that any node failure be automatically detected and the corresponding route to the failed node be removed from the routing table. If an Anycast target is the only host on the link/VLAN, then failure may result in route being automatically removed. In most cases however, it may be necessary to actively monitor host reachability and preferably service health to determine whether the route is valid or if it should be removed in favor of a secondary target.

Additionally, when IP Anycast is deployed, it is very important to ensure that the route metrics to each target have significant weighting or bias. If routes to Anycast targets should flap or result in an Equal-Cost Multi-Path Routing (ECMP) scenario, then traffic for a given service (RADIUS AAA, DHCP/SNMP Trap Profiling, HTTPS Portals) may be distributed to each target resulting in excessive traffic and service failures (RADIUS AAA and HTTPS Portals) or suboptimal profiling and database replication (Profiling services).

The key advantage of IP Anycast is that it greatly simplifies the configuration on access devices, profile data sources, and DNS. It can also optimize ISE Profiling by ensuring that data for a given endpoint are only sent to a single PSN. The downside of Anycast is the additional route configuration must be carefully planned and managed with appropriate monitors. Troubleshooting can also be more difficult since distinct subnetworks and IP addresses are not used.

General Monitoring and Troubleshooting

This section provides high-level recommendations to validate and troubleshoot the integration of Cisco ISE PSNs using F5 BIG-IP LTM for load balancing. It is not intended to be an exhaustive guide on this topic but rather to serve as an aid to jump start troubleshooting efforts and ensure basic configuration and deployment are correct before contacting Cisco or F5 for technical support.

Cisco ISE Monitoring and Troubleshooting

This section includes monitoring and troubleshooting topics specific to the Cisco ISE configuration.

Verify Operational Status of Cisco Components

To validate that traffic is being load balanced and processed correctly, ensure key solution components are operational. For example, if ISE nodes are not connected or not in sync to the ISE deployment, services like AAA, profiling, and web services can be impacted. The following tips can be used to help validate that the general ISE deployment is healthy, that PSNs are operational from the perspective of the network access devices, and that external ID stores are connected.

- Validate ISE Nodes Online and Connected
 - View ISE Dashboard for basic node status including connectivity, resource utilization, and latency.
 - Test connectivity between nodes and connecting devices using ping or similar tools.
 - Verify DNS is operational from the PSN console by pinging hosts using their FQDN or using the **nslookup** command to verify both name resolution of FQDNs and reverse lookup of IP addresses.

Below is an example taken from the ISE Admin node's main dashboard that shows Authentication Latency for different PSNs. It reveals trends in RADIUS latency. Additionally, the Alarms panel shows that there have been specific events related to high latency.

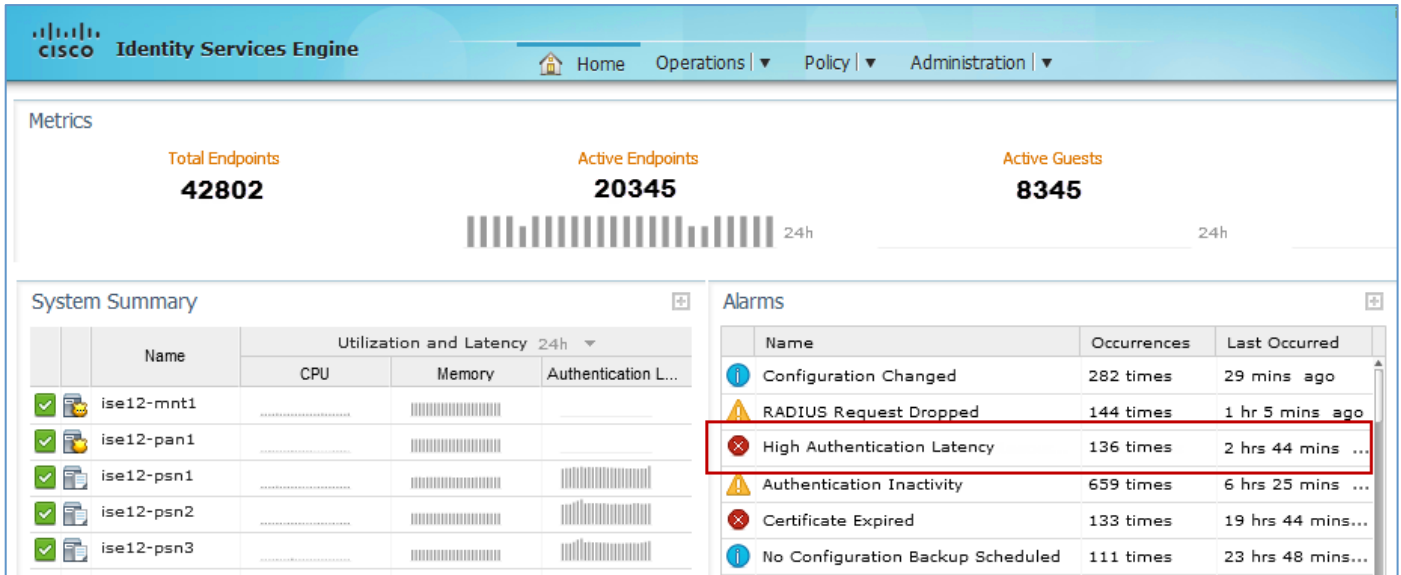


Figure 57. Using the ISE Dashboard to View ISE Server Health

Clicking the Alarm and drilling into the Authentications Details (or else viewing Authentications Details from the Live Authentications Log under Operations > Authentications) will show specific occurrences and actual points in the authentication process where high latency was observed. In the below example, AD latency for this session was over 11 seconds indicating a significant problem with the AD configuration. This situation can certainly cause RADIUS timeouts to occur.

Figure 58. Figure 1: Step Latency Details in ISE Authentication Log

Overview

Event	5200 Authentication succeeded
Username	employee1
Endpoint Id	7C:6D:62:E3:D5:05
Endpoint Profile	Apple-iPad
Authorization Profile	Central_Web_Auth_SGT_Employee
AuthorizationPolicyMatchedRule	Employee_NoPosture_1X
ISEPolicySetName	Wireless
IdentitySelectionMatchedRule	Default

Authentication Details

Source Timestamp	2014-11-03 19:15:08.416
Received Timestamp	2014-11-03 19:15:07.053
Policy Server	ise12-psn2
Event	5200 Authentication succeeded
Failure Reason	

Steps

```

11001 Received RADIUS Access-Request
11017 RADIUS created a new session
      <<< snip >>>
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-response
11522 Extracted EAP-Response/Identity for inner EAP method
11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-response
11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated
15041 Evaluating Identity Policy
15006 Matched Default Rule
15013 Selected Identity Source - AD1
24430 Authenticating user against Active Directory (🚨 Step latency=" 11023 ms")
24402 User authentication against Active Directory succeeded
22037 Authentication Passed
                
```

Figure 59. Step Latency Details in ISE Authentication Log

- Check that PSNs are synchronized under Administration > Deployment. The example below shows that the PSN3 node's database is not synchronized with the Primary Admin node.

Deployment Nodes

Edit
 Register
 Syncup
 Deregister

<input type="checkbox"/>	Hostname	Node Type	Personas	Role(s)	Services	Node Status
<input type="checkbox"/>	ise12-mnt1	ISE	Administration, Monitoring	SEC(A), SEC(M)		✔
<input type="checkbox"/>	ise12-pan1	ISE	Administration, Monitoring	PRI(A), PRI(M)		✔
<input type="checkbox"/>	ise12-psn1	ISE	Policy Service		All	✔
<input type="checkbox"/>	ise12-psn2	ISE	Policy Service		All	✔
<input type="checkbox"/>	ise12-psn3	ISE	Policy Service		All	⚠

Figure 60. ISE Deployment Node Status

- Verify the RADIUS Server status from the NADs.
 - If enabled, are RADIUS test probes succeeding or failing?
 - Are RADIUS requests timing out?
 - Does NAD debug logging for RADIUS reveal connectivity issues?

The following example shows how to verify RADIUS server status on a Cisco Catalyst Switch or IOS Router using the **show aaa servers** command. In this case, the RADIUS server at 10.1.98.8 is not responding to requests and is marked as down.


```

cat3750x#sh aaa servers
RADIUS: id 1, priority 1, host 10.1.98.8, auth-port 1812, acct-port 1813
State: current DEAD, duration 1s, previous duration 594781s
Dead: total time 95092s, count 11
Quarantined: No
Authen: request 3130, timeouts 2733, failover 0, retransmission 2054
Response: accept 395, reject 0, challenge 0
Response: unexpected 1, server error 0, incorrect 0, time 350ms
Transaction: success 395, failure 679
Throttled: transaction 0, timeout 0, failure 0
Author: request 29, timeouts 0, failover 0, retransmission 0
Response: accept 27, reject 2, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 58ms
Transaction: success 29, failure 0
Throttled: transaction 0, timeout 0, failure 0
Account: request 79816, timeouts 15483, failover 0, retransmission 11621
Request: start 36, interim 0, stop 35
Response: start 28, interim 0, stop 30
Response: unexpected 0, server error 0, incorrect 0, time 12ms
Transaction: success 64333, failure 3862
Throttled: transaction 0, timeout 0, failure 0
Elapsed time since counters last cleared: 3w4d23h30m
Estimated Outstanding Access Transactions: 2
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
Requests per minute past 24 hours:
high - 1 hours, 15 minutes ago: 5
low - 21 hours, 58 minutes ago: 0
average: 0
cat3750x#
    
```

Figure 61. RADIUS Server Health Status from Network Access Device

- Verify Identity Stores such as AD and LDAP are connected to PSNs and traffic is not being dropped.

The following example taken from ISE Admin node under Administration > Identity Management > External Identity Stores > Active Directory shows each of the ISE PSNs and their connection status to AD. Note that PSN3 is having connection issues and may cause RADIUS to succeed for Internal User accounts but fail for any externally- authenticated or authorized account.

Active Directory > AD1

Connection | Advanced Settings | Groups | Attributes

* Domain Name:

* Identity Store Name:

One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is

Join Leave Test Connection Refresh

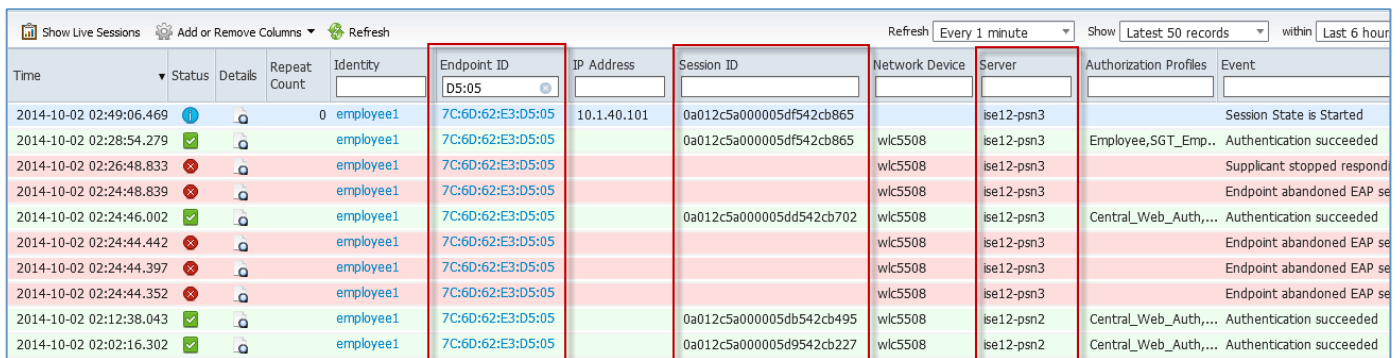
<input type="checkbox"/>	ISE Node	ISE Node Role	Status
<input type="checkbox"/>	ise12-mnt1.cts.local	SECONDARY	Connected to: ad.cts.local
<input type="checkbox"/>	ise12-pan1.cts.local	PRIMARY	Connected to: ad.cts.local
<input type="checkbox"/>	ise12-psn1.cts.local	SECONDARY	Connected to: ad.cts.local
<input type="checkbox"/>	ise12-psn2.cts.local	SECONDARY	Connected to: ad.cts.local
<input type="checkbox"/>	ise12-psn3.cts.local	SECONDARY	No Response from ISE Node.

Figure 62. ISE External Identity Store Connection Status

ISE Authentications Live Log

The ISE Authentications Live Log is accessible from the ISE Admin node under Operations > Authentications. It displays all active sessions for the past 24 hours. It can help determine if authentications are occurring successfully with load balancing and that authentication load is being distributed across multiple PSNs.

- Check authentication activity for errors with particular focus on RADIUS drops, misbehaving NADs (excessive AAA activity for same session), misbehaving supplicants (clients stopped responding or abandoned EAP sessions), and excessive client retries (new session started while another in progress). All of these may indicate issues with RADIUS authentication flow if significantly increase with the load balancer in place.
- Review the distribution of sessions across PSNs. Is the same client connecting to the same or different PSNs within the expected persistence interval? Is the Audit Session ID for the same client frequently changing within seconds or minutes?



Time	Status	Details	Repeat Count	Identity	Endpoint ID	IP Address	Session ID	Network Device	Server	Authorization Profiles	Event
2014-10-02 02:49:06.469	🟡		0	employee1	7C:6D:62:E3:D5:05	10.1.40.101	0a012c5a000005df542cb865		ise12-psn3		Session State is Started
2014-10-02 02:28:54.279	🟢			employee1	7C:6D:62:E3:D5:05		0a012c5a000005df542cb865	wlc5508	ise12-psn3	Employee,SGT_Emp...	Authentication succeeded
2014-10-02 02:26:48.833	🔴			employee1	7C:6D:62:E3:D5:05			wlc5508	ise12-psn3		Supplicant stopped respondi
2014-10-02 02:24:48.839	🔴			employee1	7C:6D:62:E3:D5:05			wlc5508	ise12-psn3		Endpoint abandoned EAP se
2014-10-02 02:24:46.002	🟢			employee1	7C:6D:62:E3:D5:05		0a012c5a000005dd542cb702	wlc5508	ise12-psn3	Central_Web_Auth,...	Authentication succeeded
2014-10-02 02:24:44.442	🔴			employee1	7C:6D:62:E3:D5:05			wlc5508	ise12-psn3		Endpoint abandoned EAP se
2014-10-02 02:24:44.397	🔴			employee1	7C:6D:62:E3:D5:05			wlc5508	ise12-psn3		Endpoint abandoned EAP se
2014-10-02 02:24:44.352	🔴			employee1	7C:6D:62:E3:D5:05			wlc5508	ise12-psn3		Endpoint abandoned EAP se
2014-10-02 02:12:38.043	🟢			employee1	7C:6D:62:E3:D5:05		0a012c5a000005db542cb495	wlc5508	ise12-psn2	Central_Web_Auth,...	Authentication succeeded
2014-10-02 02:02:16.302	🟢			employee1	7C:6D:62:E3:D5:05		0a012c5a000005d9542cb227	wlc5508	ise12-psn2	Central_Web_Auth,...	Authentication succeeded

Figure 63. ISE Live Authentications Log Example

Note: To reduce noise from uninteresting logs, use filters to focus on specific endpoints and specific PSNs including Identity, Endpoint ID, Network Device, Session ID.

- Are F5 LTM probes failing? If the health monitor probes fail, then the PSN(s) and possibly the entire virtual server may be removed from service. Verify the probe configuration is correct.

Show Live Sessions Add or Remove Columns Refresh Refresh Every 1 minute									
Time	Status	Details	Repeat Count	Identity	Endpoint ID	Network Device	Server	Event	Failure Reason
2014-10-02 02:20:45.775	✘			f5-probe1		f5-bigip	ise12-psn3	Authentication failed	22056 Subject not found
2014-10-02 02:20:44.759	✘			f5-probe1		f5-bigip	ise12-psn2	Authentication failed	22056 Subject not found
2014-10-02 02:20:43.767	✘			f5-probe1		f5-bigip	ise12-psn1	Authentication failed	22056 Subject not found
2014-10-02 02:20:35.760	✘			f5-probe1		f5-bigip	ise12-psn3	Authentication failed	22056 Subject not found
2014-10-02 02:20:34.827	✘			f5-probe1		f5-bigip	ise12-psn2	Authentication failed	22056 Subject not found
2014-10-02 02:20:33.785	✘			f5-probe1		f5-bigip	ise12-psn1	Authentication failed	22056 Subject not found
2014-10-02 02:20:25.977	✘			f5-probe1		f5-bigip	ise12-psn3	Authentication failed	22056 Subject not found
2014-10-02 02:20:24.775	✘			f5-probe1		f5-bigip	ise12-psn2	Authentication failed	22056 Subject not found
2014-10-02 02:20:23.769	✘			f5-probe1		f5-bigip	ise12-psn1	Authentication failed	22056 Subject not found
2014-10-02 02:20:15.742	✘			f5-probe1		f5-bigip	ise12-psn3	Authentication failed	22056 Subject not found
2014-10-02 02:20:14.841	✘			f5-probe1		f5-bigip	ise12-psn2	Authentication failed	22056 Subject not found
2014-10-02 02:20:13.838	✘			f5-probe1		f5-bigip	ise12-psn1	Authentication failed	22056 Subject not found
2014-10-02 02:20:05.840	✘			f5-probe1		f5-bigip	ise12-psn3	Authentication failed	22056 Subject not found
2014-10-02 02:20:04.848	✘			f5-probe1		f5-bigip	ise12-psn2	Authentication failed	22056 Subject not found

Figure 64. ISE Failed RADIUS Health Monitors Example

ISE Reports

From the ISE Admin interfaces; review **Operations > Reports** for longer-term views and additional detail of ISE Dashboard and Live Log data points.

ISE Packet Capture using TCP Dump

In some cases it is necessary to capture the packets on the network for deeper analysis. Packet capture and decode can be run directly from a specific ISE node interface using a TCP Dump facility. Captured packets can be filtered based on load-balanced traffic such as RADIUS Auth from a specific NAD, or HTTPS from a specific user IP address to a specific PSN. Furthermore, packet captures can be exported using standard formats to allow additional filtering and analysis using enhanced tools like Wireshark.

To initiate a packet capture from the ISE Admin node, navigate to **Operations > Troubleshoot > Diagnostics > General Tools > TCP Dump**. Select the PSN node and interface to capture the traffic along with filter and capture format as shown in the diagram below.

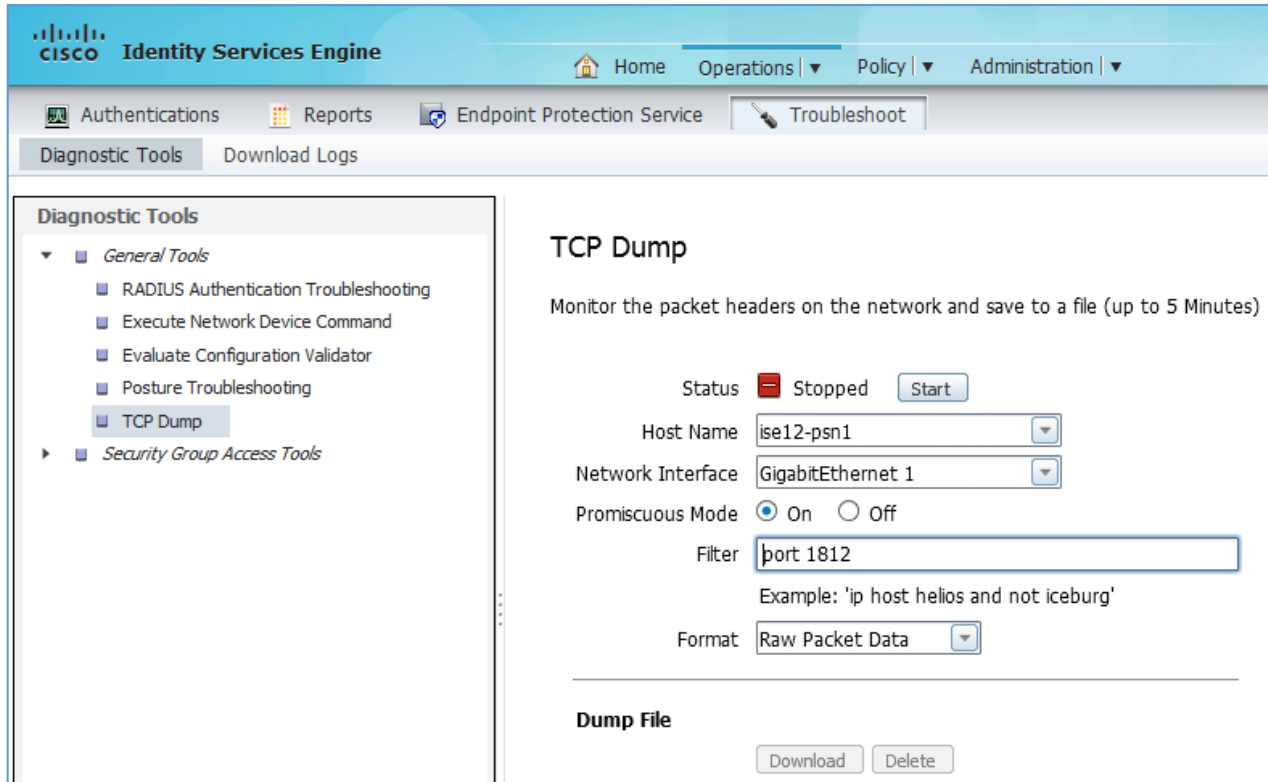


Figure 65. ISE TCP Dump Utility

Logging Suppression and Collection Filters

Within the guide we discuss the use of Collection Filters to squelch authentication success events from F5 RADIUS Health Monitors when system is operational, but you may need to disable suppression for specific endpoints or NADs to troubleshoot individual clients or access device connections.

F5 BIG-IP LTM Monitoring and Troubleshooting

This section includes monitoring and troubleshooting elements specific to the F5 configuration.

Verify Operational Status of F5 LTM Components

The following tips can be used to help validate that the general deployment is healthy and that PSNs are operational from the perspective of the F5 BIG-IP LTM appliance.

- Virtual Server Status

To view the status of Virtual Servers from the F5 LTM admin interface, navigate to **Local Traffic > Virtual Servers > Virtual Server List**. Status should be Available (green circle) for pools that use an active application monitor, or else Unknown (blue square) if no service checking is enabled. If Status is Offline (red diamond), a health monitor has failed. If connection limits are set for a node, the status could also be shown as Unavailable (yellow triangle). Status at the Virtual Server level indicates health of the pool as a whole rather than an individual pool member.

Local Traffic » Virtual Servers : Virtual Server List

Virtual Server List | Virtual Address List | Statistics

* Search Create...

<input type="checkbox"/>	Status	Name	Application	Destination	Service Port	Type	Resources	Partition / Path
<input type="checkbox"/>	●	ise_profiling_dhcp		10.1.98.8	67	Standard	Edit...	Common
<input type="checkbox"/>	■	ise_profiling_netflow		10.1.98.8	9996	Standard	Edit...	Common
<input type="checkbox"/>	■	ise_profiling_snmptrap		10.1.98.8	162 (SNMPTRAP)	Standard	Edit...	Common
<input type="checkbox"/>	◆	ise_radius_acct		10.1.98.8	1813	Standard	Edit...	Common
<input type="checkbox"/>	◆	ise_radius_auth		10.1.98.8	1812	Standard	Edit...	Common

Figure 66. LTM Virtual Server Health Status

- Pool Member Status

View the status of each Pool Member under **Local Traffic > Pools > Pool List**. Status indicators similar to those shown at the Virtual Server status level reflect the health of individual pool members.

Local Traffic » Pools : Pool List » radius_auth_pool

Properties | Members | Statistics

Load Balancing

Load Balancing Method: Least Connections (member)

Priority Group Activation: Disabled

Current Members

<input type="checkbox"/>	Status	Member	Address	Ratio	Priority Group	Conn
<input type="checkbox"/>	●	ise-psn-1:1812	10.1.99.15	1	0 (Active)	0
<input type="checkbox"/>	●	ise-psn-2:1812	10.1.99.16	1	0 (Active)	0
<input type="checkbox"/>	●	ise-psn-3:1812	10.1.99.17	1	0 (Active)	0

Figure 67. LTM Pool Member Health Status

Health Monitors

Health Monitors determine the health status of real servers and services. If a monitor fails to receive a suitable response within the configured timeout interval, the pool member will be marked as “offline” and will no longer be used to service new requests. If a Virtual Server or Pool Member is offline, then check the Health Monitor assigned to the pool or node. If the monitor never worked, then it is likely an issue with the monitor configuration. If the

monitor worked and then stops working, then check for possible configuration or software changes to the network or the PSN(s).

For service issues related to specific nodes, it is recommended to review F5 support article [SOL2531: Troubleshooting health monitors](#) to ensure monitors provide healthy status and keep the server active in the pool.

Persistence Records

Persistence Records reveal which user and device traffic is being load balanced to same real server. Any traffic matching the same source to the same service should be persisted to the same server while the persistence record is active.

- Verify the distribution of services across real servers. Is traffic persisted to all pool members or to only one or subset of members?
- Verify persist timers (Age) are consistent with the configured persist timeout, or TTL.
- Verify persistence for given endpoint is tied to expected/same PSN over time. Multiple entries for the same endpoint indicate configuration issues.

Viewing Persistence Records from the F5 LTM Web Interface

For quick viewing of persistence records from the F5 LTM web-based admin interface, navigate to **Statistics > Module Statistics > Local Traffic** and set Statistics Type to **Persistence Records**. Optionally use the Search field to filter the output.

Persistence Records—Good Example:

▲ Persistence Value	▼ Persistence Mode	Virtual Server	◆ Pool	◆ Pool Member	Age
00-30-94-C4-52-8A	Universal	ise_profiling_dhcp	profiling_dhcp_pool	10.1.99.17:67	5 seconds
00-50-56-A0-0B-3A	Universal	ise_radius_acct	radius_acct_pool	10.1.99.15:1813	715 seconds
10.1.50.2	Universal	ise_radius_auth	radius_auth_pool	10.1.99.17:1812	712 seconds
10.4.50.2	Universal	ise_radius_auth	radius_auth_pool	10.1.99.15:1812	1344 seconds
10.5.50.2	Universal	ise_radius_auth	radius_auth_pool	10.1.99.16:1812	1843 seconds
6C-20-56-13-E9-FC	Universal	ise_radius_auth	radius_auth_pool	10.1.99.15:1812	798 seconds
7C-6D-62-E3-D5-05	Universal	ise_radius_acct	radius_acct_pool	10.1.99.16:1813	124 seconds
F0-25-B7-08-33-9D	Universal	ise_radius_auth	radius_auth_pool	10.1.99.17:1812	199 seconds

Figure 68. Persistence Records Example #1

Persistence Records—Bad Example:

Statistics » Module Statistics : Local Traffic

Traffic Summary Local Traffic Network Memory

Display Options

Statistics Type Persistence Records

Data Format Normalized

Auto Refresh Disabled Refresh

* Search

▲ Persistence Value	▼ Persistence Mode	Virtual Server	Pool	Pool Member	Age
00-30-94-C4-52-8A	Universal	ise_radius_auth	radius_auth_pool	10.1.99.15:1812	33 seconds
00-30-94-c4-52-8a	Universal	ise_profiling_dhcp	profiling_dhcp_pool	10.1.99.16:67	9 seconds
00-50-56-A0-0B-3A	Universal	ise_radius_auth	radius_auth_pool	10.1.99.16:1812	33 seconds
10.1.50.2	Universal	ise_radius_auth	radius_auth_pool	10.1.99.17:1812	30 seconds
10.5.50.2	Universal	ise_radius_auth	radius_auth_pool	10.1.99.15:1812	178 seconds
7c-6d-62-e3-d5-05	Universal	ise_radius_auth	radius_auth_pool	10.1.99.17:1812	45 seconds
f0-25-b7-08-33-9d	Universal	ise_radius_auth	radius_auth_pool	10.1.99.16:1812	92 seconds

Figure 69. Persistence Records Example #2

Note in the above “Bad Example” that there are two entries for the same endpoint persisted to two different servers. This may be expected when using different persistence algorithms for different Virtual Servers, or if intentionally using different pools for different services. In the case of PSN load balancing, we typically want all traffic for a given endpoint to be sent to the same PSN. Due to variances in the MAC address format in the above example, the F5 BIG-IP LTM treated each entry as a unique endpoint and consequently load balanced the traffic to different PSNs. By normalizing the MAC address to a single format, the endpoint traffic for both flows can be sent to the same PSN as shown in “Good Example”.

Viewing Persistence Records from the F5 BIG-IP LTM Console Interface

In a production network, use of the general statistics report may not be an efficient method to search and view records for a specific endpoint. To quickly view persistence records for a specific Virtual Server, source IP address, or endpoint, use the BIG-IP LTM TMOS Shell (tmsh).

Example—Show Persistence Records for RADIUS Virtual Server

```
root@(f5) (cfg-sync Standalone) (Active) (/Common) (tmsh)# show ltm persistence persist-
records virtual ise_radius_auth
Sys::Persistent Connections
universal 10.1.98.8:1812 10.1.99.15:1812 0
universal 10.1.98.8:1812 10.1.99.15:1812 0
universal 10.1.98.8:1812 10.1.99.16:1812 0
universal 10.1.98.8:1812 10.1.99.17:1812 0
universal 10.1.98.8:1812 10.1.99.17:1812 0
Total records returned: 5
```


Example—Show Persistence Records for Specific Client Based on MAC address as Persist Key

```
root@(f5) (cfg-sync Standalone) (Active) (/Common) (tmsh) # show ltm persistence persist-
records virtual ise_radius_auth mode universal key 7C-6D-62-E3-D5-05
Sys::Persistent Connections
universal 10.1.98.8:1812 10.1.99.16:1812 0
Total records returned: 1
```

Clearing Persistence Records from the F5 BIG-IP LTM Console Interface

In some cases it may be necessary to clear existing persistence records to ensure new traffic is load balanced as expected. To clear persistence records for a specific endpoint, source IP, Virtual Server, pool, or node, use the BIG-IP LTM TMOS Shell (tmsh).

Example—Delete Persistence Records for RADIUS Virtual Server

```
root@(f5) (cfg-sync Standalone) (Active) (/Common) (tmsh) # delete ltm persistence persist-
records virtual ise_radius_auth
```

Example—Delete All Persistence Records

```
root@(f5) (cfg-sync Standalone) (Active) (/Common) (tmsh) # delete ltm persistence persist-
records
```

Clearing Connections from the F5 BIG-IP LTM Console Interface

In some cases it may be necessary to clear existing connections to ensure new traffic is load balanced as expected. To clear connections for a specific client, server, or port, use the BIG-IP LTM TMOS Shell (tmsh).

Example—Delete Connections for RADIUS Auth Services

```
root@(f5) (cfg-sync Standalone) (Active) (/Common) (tmsh) # delete sys connection cs-server-
port 1812
```

Example—Delete All Connections

```
root@(f5) (cfg-sync Standalone) (Active) (/Common) (tmsh) # delete sys connection
```

iRule Debug and View Local Traffic Logs

The iRules used in this guide for persistence included a debug logging option to be used only when troubleshooting is required. Enable iRule debug logging options and view F5 traffic logs to verify iRule persistence processing. Example output for the debug options is provided in the guide.

Packet Capture using TCP Dump

Like ISE, F5 also includes support to capture and analyze packets directly from F5 Admin Interface. Additional filtering and analysis is possible using enhanced packet capture tools like Wireshark. For more information on using the **tcpdump** command using F5, see F5 support article [SOL411: Overview of packet tracing with the tcpdump utility](#).

Network Topology, Routing, and Addressing Review

One of the most common deployment issues is related to unexpected packet flows. Be sure to have a current network diagram that shows all components with their per-interface IP addresses and VLANs. Key components include:

- Clients / Endpoints
- Network Access Devices
- Intermediate infrastructure
- BIG-IP LTM appliances
- ISE PSN appliances
- Supporting services such as DNS, NTP, AD/LDAP, and Admin and MnT nodes

Other troubleshooting checklist items include the following:

- Map out the expected path for each flow.
- Validate actual path taken by packets by reviewing configuration files, logs and packet captures, routing tables, and ARP tables.
- Take into special consideration where NAT may be deployed and addresses change.
- If F5 LTM appliance trunks multiple VLANs, note that packet captures may show both ingress and egress packets where MAC addresses change but IP addresses do not. This can sometimes cause confusion when analyzing packet captures.
- Verify symmetric path is taken and that no packets are being dropped using component logs and debugs and packet captures.

Appendix A: F5 Configuration Examples

Example F5 BIG-IP LTM Configurations

This section provides working configuration examples for F5 BIG-IP LTM to load balance multiple ISE services.

Full F5 LTM Configuration

This configuration example uses standard IP source address persistence for DHCP and does not use the DHCP Parser iRule. The DHCP Parser iRule is included in this appendix. This configuration also shows the use of a dedicated interface for ISE web services.

```
apm resource remote-desktop citrix-client-bundle /Common/default-citrix-client-bundle {
}
apm sso saml-sp-connector /Common/saml_office365 {
  assertion-consumer-uri https://login.microsoftonline.com/login.srf
  description "Predefined SP connector object for Office 365"
  entity-id urn:federation:MicrosoftOnline
}
ltm default-node-monitor {
  rule none
}
ltm node /Common/ise-psn-1 {
  address 10.1.99.15
}
ltm node /Common/ise-psn-1-web {
  address 10.1.91.15
}
ltm node /Common/ise-psn-2 {
  address 10.1.99.16
}
ltm node /Common/ise-psn-2-web {
  address 10.1.91.16
}
ltm node /Common/ise-psn-3 {
  address 10.1.99.17
}
ltm node /Common/ise-psn-3-web {
  address 10.1.91.17
}
ltm pool /Common/profiling_dhcp_pool {
  description "PSN Pool for DHCP Profiling"
  members {
    /Common/ise-psn-1:67 {
      address 10.1.99.15
    }
    /Common/ise-psn-2:67 {
      address 10.1.99.16
    }
    /Common/ise-psn-3:67 {
      address 10.1.99.17
    }
  }
  monitor /Common/radius_1812
}
```

```
    service-down-action reselect
}
ltm pool /Common/profiling_netflow_pool {
  members {
    /Common/ise-psn-1:9996 {
      address 10.1.99.15
    }
    /Common/ise-psn-2:9996 {
      address 10.1.99.16
    }
    /Common/ise-psn-3:9996 {
      address 10.1.99.17
    }
  }
  monitor /Common/gateway_icmp
}
ltm pool /Common/profiling_snmptrap_pool {
  description "PSN Pool for SNMP Trap Profiling"
  members {
    /Common/ise-psn-1:162 {
      address 10.1.99.15
    }
    /Common/ise-psn-2:162 {
      address 10.1.99.16
    }
    /Common/ise-psn-3:162 {
      address 10.1.99.17
    }
  }
  monitor /Common/gateway_icmp
}
ltm pool /Common/radius_acct_pool {
  allow-snat no
  description "PSN Pool for RADIUS Accounting"
  load-balancing-mode least-connections-node
  members {
    /Common/ise-psn-1:1813 {
      address 10.1.99.15
    }
    /Common/ise-psn-2:1813 {
      address 10.1.99.16
    }
    /Common/ise-psn-3:1813 {
      address 10.1.99.17
    }
  }
  monitor /Common/radius_1812
  service-down-action reselect
}
ltm pool /Common/radius_auth_pool {
  allow-snat no
  description "PSN Pool for RADIUS Authenticaion and Authorization"
  load-balancing-mode least-connections-node
  members {
    /Common/ise-psn-1:1812 {
      address 10.1.99.15
    }
    /Common/ise-psn-2:1812 {
      address 10.1.99.16
    }
  }
}
```

```
        /Common/ise-psn-3:1812 {
            address 10.1.99.17
        }
    }
    monitor /Common/radius_1812
    service-down-action reselect
}
ltm pool /Common/web_portals_pool {
    description "Shared pool for LB of all ISE web portal traffic"
    load-balancing-mode least-connections-node
    members {
        /Common/ise-psn-1-web:0 {
            address 10.1.91.15
        }
        /Common/ise-psn-2-web:0 {
            address 10.1.91.16
        }
        /Common/ise-psn-3-web:0 {
            address 10.1.91.17
        }
    }
    monitor /Common/ise_https_8443
}
ltm snat-translation /Common/10.1.98.8 {
    address 10.1.98.8
    inherited-traffic-group true
    traffic-group /Common/traffic-group-1
}
ltm snatpool /Common/radius_coa_snatpool {
    members {
        /Common/10.1.98.8
    }
}
ltm virtual /Common/PSN-IP-Forwarding-Inbound {
    description "Forward non-LB traffic to ISE Policy Service nodes"
    destination /Common/10.1.99.0:0
    ip-forward
    mask 255.255.255.224
    profiles {
        /Common/ise_fastL4 { }
    }
    source 10.0.0.0/8
    translate-address disabled
    translate-port disabled
    vlans {
        /Common/external
    }
    vlans-enabled
}
ltm virtual /Common/PSN-IP-Forwarding-Inbound-Web {
    destination /Common/10.1.91.0:0
    ip-forward
    ip-protocol tcp
    mask 255.255.255.224
    profiles {
        /Common/ise_fastL4 { }
    }
    source 10.0.0.0/8
    source-address-translation {
        type automap
    }
}
```

```
}
translate-address disabled
translate-port disabled
vlans {
    /Common/external
}
vlans-enabled
}
ltm virtual /Common/PSN-IP-Forwarding-Outbound {
description "Forward non-LB traffic from ISE Policy Service nodes"
destination /Common/0.0.0.0:0
ip-forward
mask any
profiles {
    /Common/ise_fastL4 { }
}
source 10.1.99.0/27
translate-address disabled
translate-port disabled
vlans {
    /Common/internal
}
vlans-enabled
}
ltm virtual /Common/RADIUS-COA-SNAT {
destination /Common/10.0.0.0:1700
ip-protocol udp
mask 255.0.0.0
profiles {
    /Common/udp { }
}
source 10.1.99.0/27
source-address-translation {
    pool /Common/radius_coa_snatpool
    type snat
}
translate-address disabled
translate-port enabled
vlans {
    /Common/internal
}
vlans-enabled
}
ltm virtual /Common/ise_http_portals {
description "ISE PSN Web Portals on TCP/80"
destination /Common/10.1.98.8:80
http-class {
    /Common/ise_httpclass
}
ip-protocol tcp
mask 255.255.255.255
persist {
    /Common/https_sticky {
        default yes
    }
}
profiles {
    /Common/ise_http { }
    /Common/ise_https_tcp { }
}
}
```

```
source 10.0.0.0/8
source-address-translation {
    type automap
}
translate-address enabled
translate-port enabled
vlans {
    /Common/external
}
vlans-enabled
}
ltm virtual /Common/ise_https8443_portals {
description "ISE PSN Web Portals on TCP/8443"
destination /Common/10.1.98.8:8443
ip-protocol tcp
mask 255.255.255.255
persist {
    /Common/https_sticky {
        default yes
    }
}
pool /Common/web_portals_pool
profiles {
    /Common/ise_https_tcp { }
}
source 10.0.0.0/8
source-address-translation {
    type automap
}
translate-address enabled
translate-port enabled
vlans {
    /Common/external
}
vlans-enabled
}
ltm virtual /Common/ise_https_portals {
description "ISE PSN Web Portals on TCP/443"
destination /Common/10.1.98.8:443
ip-protocol tcp
mask 255.255.255.255
persist {
    /Common/https_sticky {
        default yes
    }
}
pool /Common/web_portals_pool
profiles {
    /Common/ise_https_tcp { }
}
source 10.0.0.0/8
source-address-translation {
    type automap
}
translate-address enabled
translate-port enabled
vlans {
    /Common/external
}
vlans-enabled
}
```

```
}
ltm virtual /Common/ise_profiling_dhcp {
  description "ISE PSN DHCP Profiling"
  destination /Common/10.1.98.8:67
  ip-protocol udp
  mask 255.255.255.255
  persist {
    /Common/profiling_source_addr {
      default yes
    }
  }
  pool /Common/profiling_dhcp_pool
  profiles {
    /Common/ise_profiling_udp { }
  }
  source 10.0.0.0/8
  translate-address enabled
  translate-port enabled
  vlans {
    /Common/external
  }
  vlans-enabled
}
ltm virtual /Common/ise_profiling_netflow {
  destination /Common/10.1.98.8:9996
  ip-protocol udp
  mask 255.255.255.255
  pool /Common/profiling_netflow_pool
  profiles {
    /Common/ise_profiling_udp { }
  }
  source 10.0.0.0/8
  translate-address enabled
  translate-port enabled
  vlans {
    /Common/external
  }
  vlans-enabled
}
ltm virtual /Common/ise_profiling_snmptrap {
  description "ISE PSN SNMP Trap Profiling"
  destination /Common/10.1.98.8:162
  ip-protocol udp
  mask 255.255.255.255
  persist {
    /Common/profiling_source_addr {
      default yes
    }
  }
  pool /Common/profiling_snmptrap_pool
  profiles {
    /Common/ise_profiling_udp { }
  }
  source 10.0.0.0/8
  translate-address enabled
  translate-port enabled
  vlans {
    /Common/external
  }
  vlans-enabled
}
```

```
}
ltm virtual /Common/ise_radius_acct {
  description "ISE PSN RADIUS Accounting"
  destination /Common/10.1.98.8:1813
  ip-protocol udp
  mask 255.255.255.255
  persist {
    /Common/radius_sticky {
      default yes
    }
  }
  pool /Common/radius_acct_pool
  profiles {
    /Common/ise_radiusLB { }
    /Common/ise_radius_udp { }
  }
  source 10.0.0.0/8
  translate-address enabled
  translate-port enabled
  vlans {
    /Common/external
  }
  vlans-enabled
}
ltm virtual /Common/ise_radius_auth {
  description "ISE PSN RADIUS Authentication and Authorization"
  destination /Common/10.1.98.8:1812
  ip-protocol udp
  mask 255.255.255.255
  persist {
    /Common/radius_sticky {
      default yes
    }
  }
  pool /Common/radius_auth_pool
  profiles {
    /Common/ise_radiusLB { }
    /Common/ise_radius_udp { }
  }
  source 10.0.0.0/8
  translate-address enabled
  translate-port enabled
  vlans {
    /Common/external
  }
  vlans-enabled
}
ltm virtual-address /Common/0.0.0.0 {
  address any
  arp disabled
  icmp-echo disabled
  mask any
  traffic-group /Common/traffic-group-1
}
ltm virtual-address /Common/10.0.0.0 {
  address 10.0.0.0
  arp disabled
  icmp-echo disabled
  mask 255.0.0.0
  traffic-group /Common/traffic-group-1
}
```



```
}
ltm virtual-address /Common/10.1.91.0 {
  address 10.1.91.0
  arp disabled
  icmp-echo disabled
  mask 255.255.255.224
  traffic-group /Common/traffic-group-1
}
ltm virtual-address /Common/10.1.98.8 {
  address 10.1.98.8
  mask 255.255.255.255
  traffic-group /Common/traffic-group-1
}
ltm virtual-address /Common/10.1.99.0 {
  address 10.1.99.0
  arp disabled
  icmp-echo disabled
  mask 255.255.255.224
  traffic-group /Common/traffic-group-1
}
ltm classification signature-version {
  version-number 0
}
ltm monitor http /Common/ise_http {
  defaults-from /Common/http
  destination *:80
  interval 5
  password xxx
  recv "HTTP/1.1 302 Found"
  send "GET /redir"
  time-until-up 0
  timeout 16
  username xxx
}
ltm monitor https /Common/ise13_https_443 {
  cipherlist DEFAULT:+SHA:+3DES:+kEDH
  compatibility enabled
  defaults-from /Common/https
  destination *:443
  interval 5
  password xxx
  recv "HTTP/1.1 302 Found"
  send "GET /redir"
  time-until-up 0
  timeout 16
  username xxx
}
ltm monitor https /Common/ise13_https_8443 {
  cipherlist DEFAULT:+SHA:+3DES:+kEDH
  compatibility enabled
  defaults-from /Common/https
  destination *:8443
  interval 5
  password xxx
  recv "HTTP/1.1 200 OK"
  send "GET
/sponsorportal/PortalSetup.action\?portal=Sponsor%20Portal%20%28default%29"
  time-until-up 0
  timeout 16
  username xxx
}
```

```
}
ltm monitor https /Common/ise_https {
  cipherlist DEFAULT:+SHA:+3DES:+kEDH
  compatibility enabled
  defaults-from /Common/https
  destination *:443
  interval 5
  password xxx
  recv "HTTP/1.1 302 Found"
  send "GET /redir"
  time-until-up 0
  timeout 16
  username xxx
}
ltm monitor https /Common/ise_https_8443 {
  cipherlist DEFAULT:+SHA:+3DES:+kEDH
  compatibility enabled
  defaults-from /Common/https
  description "HTTPS Health Monitor for ISE Portal Services on TCP/8443"
  destination *:8443
  interval 5
  password xxx
  recv "HTTP/1.1 200 OK"
  send "GET /sponsorportal/"
  time-until-up 0
  timeout 16
  username xxx
}
ltm monitor radius /Common/radius_1812 {
  debug no
  defaults-from /Common/radius
  description "RADIUS Authentication Request Probe using UDP/1812"
  destination *:1812
  interval 10
  nas-ip-address 10.1.99.3
  password cisco123
  secret cisco123
  time-until-up 0
  timeout 31
  username f5-probe
}
ltm persistence source-addr /Common/https_sticky {
  app-service none
  defaults-from /Common/source_addr
  hash-algorithm default
  map-proxies enabled
  mask none
  match-across-pools disabled
  match-across-services enabled
  match-across-virtuals disabled
  override-connection-limit disabled
  timeout 1200
}
ltm persistence source-addr /Common/profiling_source_addr {
  app-service none
  defaults-from /Common/source_addr
  hash-algorithm default
  map-proxies enabled
  mask none
  match-across-pools disabled
}
```

```
match-across-services enabled
match-across-virtuals disabled
override-connection-limit disabled
timeout 3600
}
ltm persistence source-addr /Common/radius_source_addr {
  app-service none
  defaults-from /Common/source_addr
  hash-algorithm default
  map-proxies enabled
  mask none
  match-across-pools disabled
  match-across-services enabled
  match-across-virtuals disabled
  override-connection-limit disabled
  timeout 3600
}
ltm persistence universal /Common/dhcp_sticky {
  app-service none
  defaults-from /Common/universal
  match-across-pools disabled
  match-across-services enabled
  match-across-virtuals disabled
  override-connection-limit disabled
  rule /Common/dhcp_mac_sticky
  timeout 7200
}
ltm persistence universal /Common/radius_sticky {
  app-service none
  defaults-from /Common/universal
  match-across-pools disabled
  match-across-services enabled
  match-across-virtuals disabled
  override-connection-limit disabled
  rule /Common/radius_mac_sticky
  timeout 300
}
ltm profile fastl4 /Common/ise_fastL4 {
  app-service none
  defaults-from /Common/fastL4
  idle-timeout 300
  ip-tos-to-client pass-through
  ip-tos-to-server pass-through
  keep-alive-interval disabled
  link-qos-to-client pass-through
  link-qos-to-server pass-through
  loose-close enabled
  loose-initialization enabled
  mss-override 0
  reassemble-fragments enabled
  reset-on-timeout enabled
  rtt-from-client disabled
  rtt-from-server disabled
  software-syn-cookie disabled
  tcp-close-timeout 5
  tcp-generate-isn disabled
  tcp-handshake-timeout 5
  tcp-strip-sack disabled
  tcp-timestamp-mode preserve
  tcp-wscale-mode preserve
```

```
}
ltm profile http /Common/ise_http {
  app-service none
  defaults-from /Common/http
}
ltm profile httpclass /Common/httpclass {
  app-service none
  asm disabled
  cookies none
  headers none
  hosts none
  paths none
  pool none
  redirect https://sponsor.cts.local:8443/sponsorportal/
  web-accelerator disabled
}
ltm profile httpclass /Common/ise_httpclass {
  app-service none
  defaults-from /Common/httpclass
}
ltm profile radius /Common/ise_radiusLB {
  app-service none
  clients none
  defaults-from /Common/radiusLB
  persist-avp none
  subscriber-aware disabled
  subscriber-id-type calling-station-id
}
ltm profile radius /Common/radiusLB {
  app-service none
  clients none
  persist-avp 31
  subscriber-aware disabled
  subscriber-id-type 3gpp-imsi
}
ltm profile tcp /Common/ise_https_tcp {
  app-service none
  defaults-from /Common/tcp
}
ltm profile udp /Common/ise_profiling_udp {
  allow-no-payload disabled
  app-service none
  datagram-load-balancing disabled
  defaults-from /Common/udp
  idle-timeout immediate
  ip-tos-to-client 0
  link-qos-to-client 0
  proxy-mss disabled
}
ltm profile udp /Common/ise_radius_udp {
  allow-no-payload disabled
  app-service none
  datagram-load-balancing disabled
  defaults-from /Common/udp
  idle-timeout 60
  ip-tos-to-client 0
  link-qos-to-client 0
  proxy-mss disabled
}
net route /Common/external_default_gateway {
```

```
    gw 10.1.98.1
    network default
}
net ipsec ike-daemon /Common/iked daemon { }
sys file ssl-cert /Common/ise_wildcard_cert.crt {
    cache-path
    /config/filestore/files_d/Common_d/certificate_d/:Common:ise_wildcard_cert.crt_37380_1
    revision 1
}
sys file ssl-key /Common/ise_wildcard_key.key {
    cache-path
    /config/filestore/files_d/Common_d/certificate_key_d/:Common:ise_wildcard_key.key_37383_1
    revision 1
}
wom endpoint-discovery { }
```

Example F5 iRules for DHCP Persistence

This section highlights working iRule examples for DHCP Persistence.

DHCP Persistence iRule Example: dhcp_mac_sticky

This example shows how F5 scripting logic can be leveraged to parse specific fields in a client DHCP Discover or Request packet and extracts the MAC Address as persistence identifier. This allows DHCP requests to be load balanced to individual ISE PSNs on a per-host basis rather than a per-gateway basis (source IP address persistence). This provides better load distribution and when coupled with RADIUS persistence based on client MAC address (RADIUS Calling-Station-ID) provides optimal profiling collection by ensuring all RADIUS and DHCP traffic for a given endpoint is sent to the same PSN.

Persistence profile that references dhcp_mac_sticky iRule

```
ltm persistence universal /Common/dhcp_sticky {
    app-service none
    defaults-from /Common/universal
    match-across-pools disabled
    match-across-services enabled
    match-across-virtuals disabled
    override-connection-limit disabled
    rule /Common/dhcp_mac_sticky
    timeout 7200
}
```

iRule: dhcp_mac_sticky

```
# iRule dhcp_mac_sticky
#
# DHCP Option Field Parser rev 0.3 (2013/02/25)
#
#   Written By:  Shun Takahashi
#
#   Original By: Jun Chen (j.chen at f5.com)
```

```
# Original At: https://devcentral.f5.com/community/group/aft/25727/asg/50
#
# Description: iRule to demonstrate how to capture and binary scan UDP payload
# and store them into session table for logging enrichment and
# intelligent traffic steering decision.
#
# RFC2131 defines DHCP packet structure. This iRule is to scan
# UDP payload and store information into session tables with
# your_ip as a key.
#
# All the option and value is stored into following session table.
#
# [table set -subtable <your_ip_addr> <option> <value>]
#
# Requirement: The rule requires virtual server to listen on DHCP traffic in the
# middle either in inline or out of band.
#
# 1) In-Line to DHCP traffic
#
#         profile udp udp_dhcp {
#             allow-no-payload disabled
#             app-service none
#             datagram-load-balancing disabled
#             idle-timeout immediate
#             ip-tos-to-client 0
#             link-qos-to-client 0
#             proxy-mss disabled
#         }
#
#         ltm virtual vs_dhcp {
#             destination 0.0.0.0:bootps
#             ip-protocol udp
#             mask any
#             profiles {
#                 udp_dhcp { }
#             }
#             rules {
#                 dhcp_sampler
#             }
#             source 0.0.0.0/0
#             translate-address disabled
#             vlans {
#                 local
#             }
#             vlans-enabled
#         }
#
# 2) Receiving mirrored DHCP stream
#
# References: RFC 2132 DHCP Options and BOOTP Vendor Extensions
#             RFC 1533 DHCP Options and BOOTP Vendor Extensions (Obsoleted)
#             RFC 4702 The Dynamic Host Configuration Protocol (DHCP) Client
#                 Fully Qualified Domain Name (FQDN) Option
#
timing off
when CLIENT_ACCEPTED priority 100 {

    # Rule Name and Version shown in the log
    set static::RULE_NAME "Simple DHCP Parser v0.3"
    set static::RULE_ID "dhcp_parser"
```

```

# 0: No Debug Logging 1: Debug Logging
set debug 1
# Persist timeout (seconds)
set persist_ttl 7200

# Using High-Speed Logging in thie rule
set log_prefix "\[$static::RULE_ID\]([IP::client_addr])"
set log_prefix_d "$log_prefix(debug)"

if {$debug}{log local0.debug "$log_prefix_d ***** iRule: \
    $static::RULE_NAME executed *****"}

if { [UDP::payload length] < 200 } {
    log local0.info "$log_prefix Ignored due to length\(less than 200 octet\)"
    drop
    return
} else {
    # BOOTP
    binary scan [UDP::payload] cccch8SB1xa4a4a4a4H2H2H2H2H2H2 \
        msg_type hw_type hw_len hops transaction_id seconds \
        bootp_flags client_ip_hex your_ip_hex server_ip_hex \
        relay_ip_hex m(a) m(b) m(c) m(d) m(e) m(f)

    # Put client address into variables for session key
    set your_ip [IP::addr $your_ip_hex mask 255.255.255.255]
    set client_mac "$m(a):$m(b):$m(c):$m(d):$m(e):$m(f)"

    binary scan [UDP::payload] H32H64H128H8 \
        padding server_host_name boot_file magic_cookie

    if {$debug}{log local0.debug "$log_prefix_d BOOTP: $your_ip $client_mac"}

    # DHCP
    binary scan [UDP::payload] x240H* dhcp_option_payload

    set option_hex 0
    set options_length [expr {[UDP::payload length] -240} * 2 ]
    for {set i 0} {$i < $options_length} {incr i [expr { $length * 2 + 2 }]} {

        # extract option value and convert into decimal
        # for human readability
        binary scan $dhcp_option_payload x[expr $i]a2 option_hex
        set option [expr 0x$option_hex]

        # move index to get length field
        incr i 2

        # extract length value and convert length from Hex string to decimal
        binary scan $dhcp_option_payload x[expr $i]a2 length_hex
        set length [expr 0x$length_hex]

        # extract value field in hexadecimal format
        binary scan $dhcp_option_payload x[expr $i + 2]a[expr { $length * 2 } ]
value_hex

        set value ""

```

```

switch $option {
    61 {
        # Client Identifier
        # This option is used by DHCP clients to specify their unique
        # identifier. DHCP servers use this value to index their database of
        # address bindings. This value is expected to be unique for all
        # clients in an administrative domain.
        #
        binary scan $value_hex a2a* ht id
        switch $ht {
            01 {
                binary scan $id a2a2a2a2a2 m(a) m(b) m(c) m(d) m(e) m(f)
                set value "$m(a)-$m(b)-$m(c)-$m(d)-$m(e)-$m(f) "
                set option61 "$value"
                # Normalize MAC address to upper case
                set mac_up [string toupper $option61]
            }

            default {
                set value "$id"
            }
        }
    }
}

persist uie $mac_up $persist_ttl
set target [persist lookup uie $mac_up]
if {$debug}{log local0.debug "$log_prefix_d ***** iRule: $static::RULE_NAME
competed ***** MAC=$option61 Normal MAC=$mac_up TARGET=$target"}
}

```

Since the persistence TTL value is set within the iRule, it will take precedence over other the Persistence Profile timeout setting. The iRule also includes a logging option to assist with debugging. Set the debug variable to “1” to enable debug logging. Set the debug variable to “0” to disable debug logging.

Here is sample output when these debug logging is enabled:

```

Sat Sep 27 13:40:08 EDT 2014  debug f5      tmm[9443]
Rule /Common/dhcp_mac_sticky <CLIENT_ACCEPTED>: [dhcp_parser] (10.1.10.1) (debug)
***** iRule: Simple DHCP Parser v0.3 competed *****
MAC=00-50-56-a0-0b-3a Normal MAC=00-50-56-A0-0B-3A TARGET=

Sat Sep 27 13:40:08 EDT 2014  debug f5      tmm[9443]
Rule /Common/dhcp_mac_sticky <CLIENT_ACCEPTED>: [dhcp_parser] (10.1.10.1) (debug)
BOOTP: 0.0.0.0 00:50:56:a0:0b:3a

Sat Sep 27 13:40:08 EDT 2014  debug f5      tmm[9443]
Rule /Common/dhcp_mac_sticky <CLIENT_ACCEPTED>: [dhcp_parser] (10.1.10.1) (debug)
***** iRule: Simple DHCP Parser v0.3 executed *****

Sat Sep 27 13:39:45 EDT 2014  debug f5      tmm[9443]
Rule /Common/dhcp_mac_sticky <CLIENT_ACCEPTED>: [dhcp_parser] (10.1.40.1) (debug)

```



```
***** iRule: Simple DHCP Parser v0.3 competed *****
MAC=f0-25-b7-08-33-9d Normal MAC=F0-25-B7-08-33-9D TARGET=

Sat Sep 27 13:39:45 EDT 2014  debug f5      tmm[9443]
Rule /Common/dhcp_mac_sticky <CLIENT_ACCEPTED>: [dhcp_parser] (10.1.40.1) (debug)
BOOTP: 0.0.0.0 f0:25:b7:08:33:9d

Sat Sep 27 13:39:45 EDT 2014  debug f5      tmm[9443]
Rule /Common/dhcp_mac_sticky <CLIENT_ACCEPTED>: [dhcp_parser] (10.1.40.1) (debug)
***** iRule: Simple DHCP Parser v0.3 executed *****

Sat Sep 27 13:36:49 EDT 2014  debug f5      tmm[9443]
Rule /Common/dhcp_mac_sticky <CLIENT_DATA>: [dhcp_parser] (10.1.40.1) (debug)
***** iRule: Simple DHCP Parser v0.3 competed *****
MAC=7c-6d-62-e3-d5-05 Normal MAC=7C-6D-62-E3-D5-05 TARGET=

Sat Sep 27 13:36:49 EDT 2014  debug f5      tmm[9443]
Rule /Common/dhcp_mac_sticky <CLIENT_DATA>: [dhcp_parser] (10.1.40.1) (debug)
BOOTP: 0.0.0.0 7c:6d:62:e3:d5:05

Sat Sep 27 13:36:49 EDT 2014  debug f5      tmm[9443]
Rule /Common/dhcp_mac_sticky <CLIENT_DATA>: [dhcp_parser] (10.1.40.1) (debug)
***** iRule: Simple DHCP Parser v0.3 executed *****
```

Appendix B: Configuration Checklist

Table 9. Configuration Checklist

Item	Setting				Notes
F5 Prerequisite Configuration					
Internal Interface	Name	IP address/Mask	VLAN #	Tagged?	•
Internal Interface					•
External Interface					•
Web Interface (Optional)					•
Default Gateway (External Interface)					•
ISE Prerequisite Configuration					
Node Group					•
Name					•
Multicast Address					• Applicable to ISE 1.2 and below
F5 Appliance NAD configuration					•
Access Device Name					• This is the name assigned to F5 as a NAD in ISE – typically hostname
IP address/Mask					• This is the source of RADIUS monitor requests – typically the Internal interface Self IP • Mask = 255.255.255.255
RADIUS Secret					• This is specific to RADIUS Monitor
Internal User Account					• This is specific to RADIUS Monitor
Username					•
Password					•
DNS – FQDNs to be added in addition to each ISE GE 0 host entry					• Each ISE node's FQDN should be configured as part of every standard deployment.
Sponsor Portal					•

My Devices Portal		<ul style="list-style-type: none"> •
PSN Web Interfaces		<ul style="list-style-type: none"> • Applicable if PSNs configured with dedicated interfaces for web services • In ISE, the FQDNs are configured using the CLI 'ip host' command
PSN Certificates		<ul style="list-style-type: none"> •
SAN Wildcard or UCC Used?		<ul style="list-style-type: none"> •
Subject CN		<ul style="list-style-type: none"> • Example: ise.company.com
SAN		<ul style="list-style-type: none"> • Include Subject CN FQDN • SAN Wildcard cert must include domain used in Subject CN • UCC – Include all PSN FQDNs; include Web Portal FQDNs for Sponsor, My Devices, and dedicated interface FQDNs if used.