

Configuring F5 LTM for Load Balancing Cisco Identity Service Engine (ISE)

Craig Hys

Principal Technical Marketing Engineer, Cisco Systems



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

Secure Access How-To Guides Series

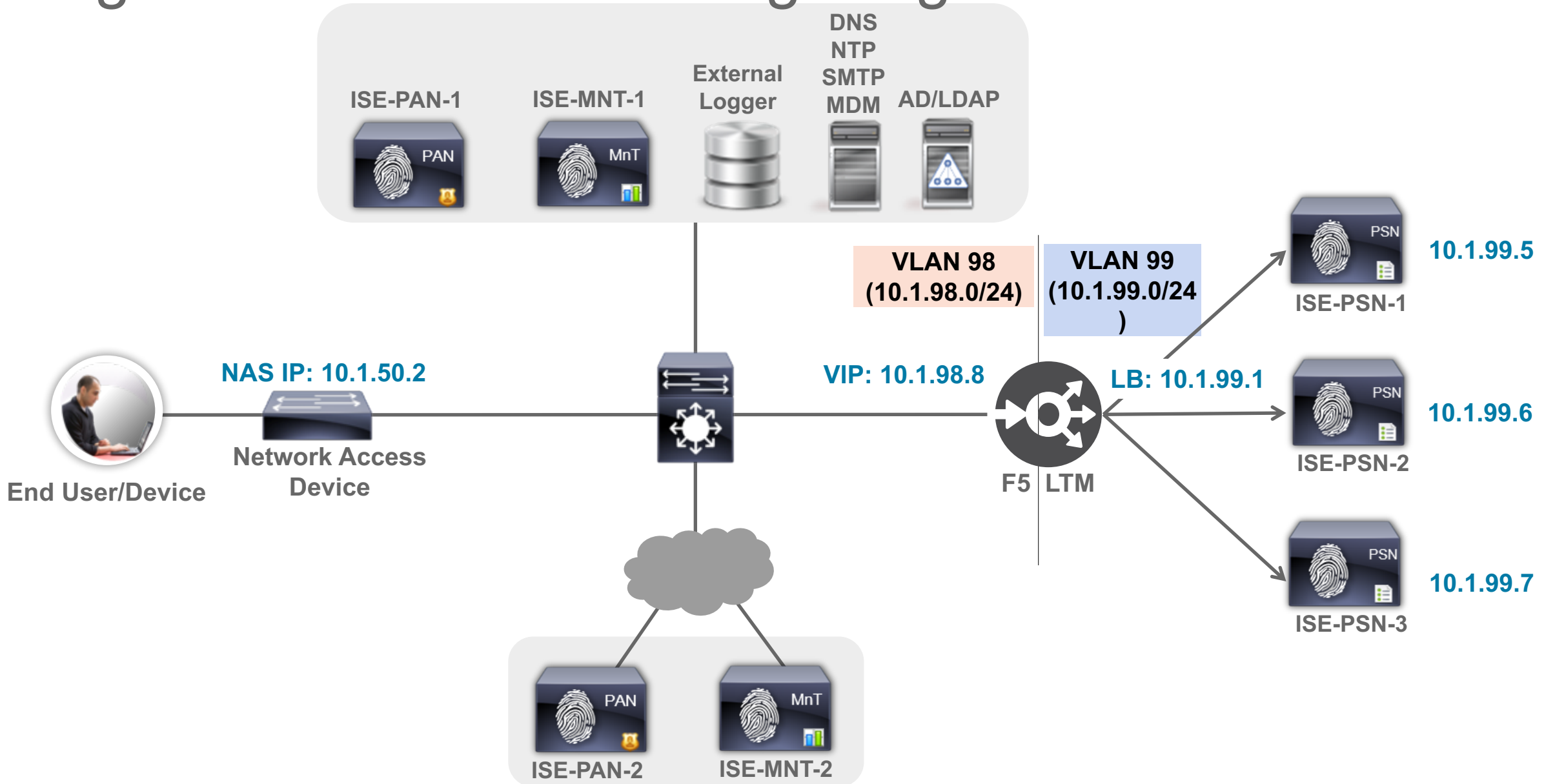
Author: Craig Hys, Cisco Systems

Date: December 2014

- **Cisco Communities**
<https://communities.cisco.com/docs/DOC-64434>
- **Cisco and F5 Deployment Guide: ISE Load Balancing using BIG-IP:**
<https://communities.cisco.com/docs/DOC-68198>
- **Linked from F5 website under Cisco Alliance page > White Papers:**
<https://f5.com/solutions/technology-alliances/cisco>

Forwarding Non-LB Traffic

High-Level Load Balancing Diagram



Non-LB Traffic that Requires IP Forwarding

Inter-node/Management/Repository/ID Stores/Feeds/Profiling/Redirected Web/RADIUS CoA

- PAN/MnT node communications
- 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 to/from PSN real IP addresses resulting from 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.

Virtual Server to Forward General Inbound IP Traffic

General Properties

- **Applies to connections initiated from outside (external) network**
- Type = Forwarding (IP)
- Source = All traffic (0.0.0.0/0) or limit to specific network.
- Destination = PSN Network Addresses
- Service Port = 0 (All Ports)
- Availability = Unknown (No service validation via health monitors)

Local Traffic » Virtual Servers : Virtual Server List » PSN-IP-Forwarding-Inbound

Properties Resources Statistics

General Properties

Name	PSN-IP-Forwarding-Inbound
Partition / Path	Common
Description	Forward non-LB traffic to ISE Policy Service nodes
Type	Forwarding (IP)
Source	10.0.0.0/8
Destination	Type: <input type="radio"/> Host <input checked="" type="radio"/> Network Address: 10.1.99.0 Mask: 255.255.255.224
Service Port	0 * All Ports
Availability	<input checked="" type="checkbox"/> Unknown (Enabled) - The children pool member(s)
State	Enabled

Virtual Server to Forward General Inbound IP Traffic Configuration (Advanced)

- Protocol = All Protocols
- Protocol Profile = fastL4
- Optionally limit to specific ingress VLAN(s).
- No SNAT

Configuration: Advanced							
Protocol	* All Protocols						
Protocol Profile (Client)	ise_fastL4						
Statistics Profile	None						
VLAN and Tunnel Traffic	Enabled on...						
VLANs and Tunnels	<table border="1"><thead><tr><th>Selected</th><th></th><th>Available</th></tr></thead><tbody><tr><td><i>/Common</i> external</td><td><< >></td><td><i>/Common</i> internal portals</td></tr></tbody></table>	Selected		Available	<i>/Common</i> external	<< >>	<i>/Common</i> internal portals
Selected		Available					
<i>/Common</i> external	<< >>	<i>/Common</i> internal portals					
Source Address Translation	None						

Virtual Server to Forward General Outbound IP Traffic

General Properties

- **Applies to connections initiated from PSN (internal) network**
- Type = Forwarding (IP)
- Source = PSN Network Addresses
- Destination = All traffic (0.0.0.0/0.0.0.0) or limit to specific network.
- Service Port = 0 (All Ports)
- Availability = Unknown (No service validation via health monitors)

The screenshot shows the configuration page for a Virtual Server in the F5 LTM GUI. The breadcrumb trail is 'Local Traffic >> Virtual Servers : Virtual Server List >> PSN-IP-Forwarding-Outbound'. The 'Properties' tab is selected. The 'General Properties' section is expanded, showing the following configuration:

General Properties	
Name	PSN-IP-Forwarding-Outbound
Partition / Path	Common
Description	Forward non-LB traffic from ISE Policy Service nodes
Type	Forwarding (IP)
Source	10.1.99.0/27
Destination	Type: <input type="radio"/> Host <input checked="" type="radio"/> Network Address: 0.0.0.0 Mask: 0.0.0.0
Service Port	0 * All Ports
Availability	<input checked="" type="checkbox"/> Unknown (Enabled) - The children pool member(s) e
State	Enabled

Virtual Server to Forward General Outbound IP Traffic Configuration (Advanced)

- Protocol = All Protocols
- Protocol Profile = fastL4
- Optionally limit to specific ingress VLAN(s).
- No SNAT

Configuration: **Advanced** ▼

Protocol	* All Protocols ▼						
Protocol Profile (Client)	ise_fastL4 ▼						
Statistics Profile	None ▼						
VLAN and Tunnel Traffic	Enabled on... ▼						
VLANs and Tunnels	<table border="1"><thead><tr><th>Selected</th><th></th><th>Available</th></tr></thead><tbody><tr><td>/Common internal</td><td><< >></td><td>/Common external portals</td></tr></tbody></table>	Selected		Available	/Common internal	<< >>	/Common external portals
Selected		Available					
/Common internal	<< >>	/Common external portals					
Source Address Translation	None ▼						

Example Inbound / Outbound IP Forwarding Servers

Local Traffic » Virtual Servers : Virtual Server List

Virtual Server List Virtual Address List Statistics

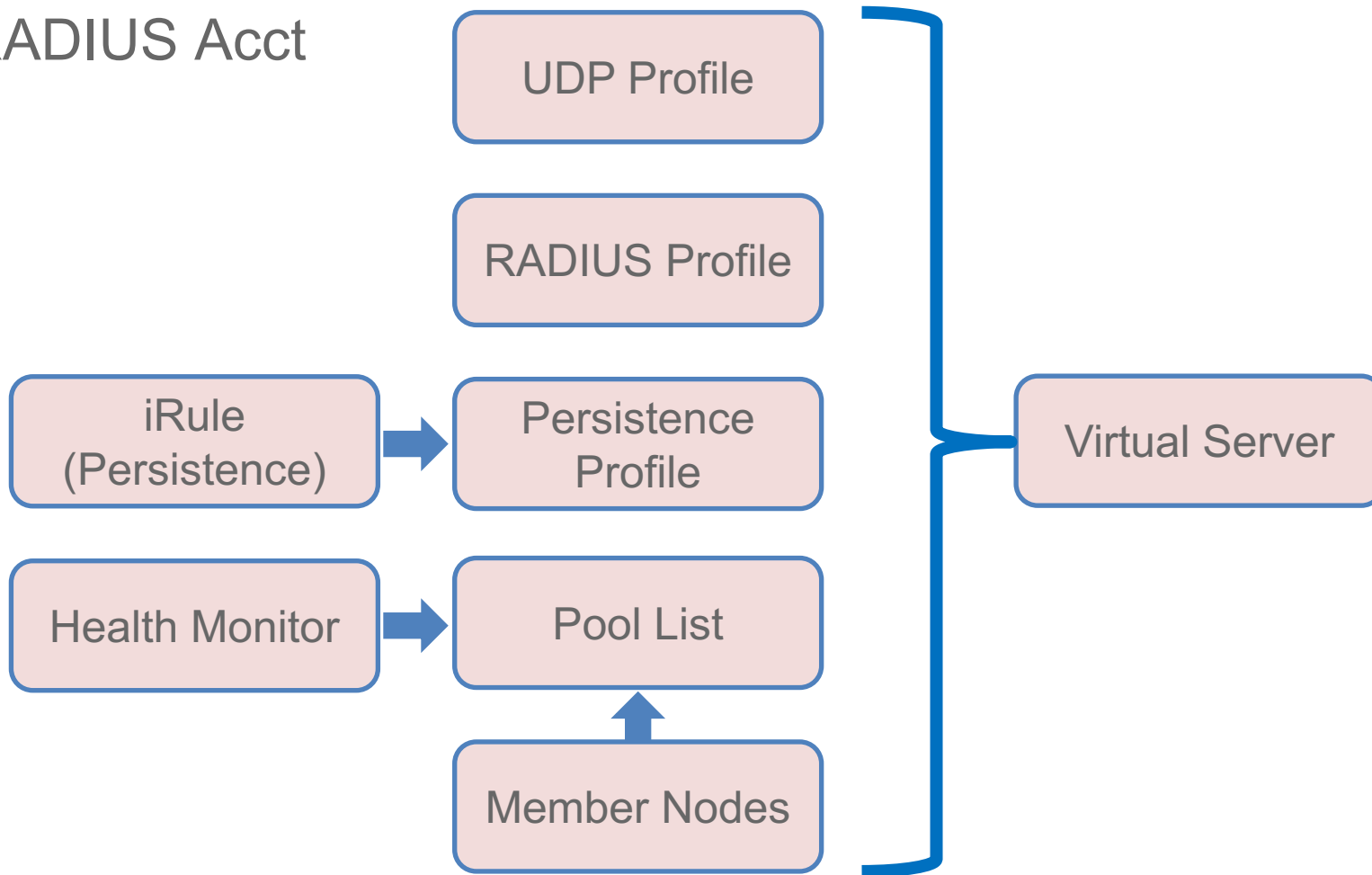
* Search Create...

<input checked="" type="checkbox"/>	Status	Name	Application	Destination	Service Port	Type	Resources	Partition / Path
<input type="checkbox"/>	<input checked="" type="checkbox"/>	PSN-IP-Forwarding-Inbound		10.1.99.0/29	0 (Any)	Forwarding (IP)	Edit...	Common
<input type="checkbox"/>	<input checked="" type="checkbox"/>	PSN-IP-Forwarding-Outbound		any	0 (Any)	Forwarding (IP)	Edit...	Common

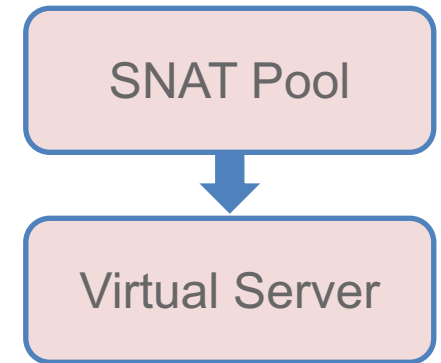
Load Balancing RADIUS

F5 LTM Configuration Components for RADIUS LB

- RADIUS Auth
- RADIUS Acct



- RADIUS CoA



RADIUS Health Monitors

Load Balancer Probes Determine RADIUS Server Health Status

- BIG-IP LTM RADIUS monitor has two key timer settings:
 - Interval = probe frequency (default = 10 sec)
 - Timeout = total time before monitor fails (default = 31 seconds)

Timeout = (3 * Interval) + 1

(Four health checks are attempted before declaring a node failure)

- Timers: Set low enough to ensure efficient failover but long enough to avoid excessive probing (AAA load); Start with defaults then tune to network.
- User Account: If valid user account to be used for monitor, be sure to configure user in ISE or external ID store with limited/no network access privileges.

Sample LTM RADIUS Health Monitor Config:

```
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
}
```

Configure RADIUS Health Monitor

Local Traffic > Monitors

- Same monitor can be leveraged for RADIUS Auth, Accounting, and Profiling to reduce probe load for multiple services.
- Be sure BIG-IP LTM configured as ISE NAD.

Local Traffic >> Monitors >> radius_1812

Properties Instances

General Properties

Name	radius_1812
Partition / Path	Common
Description	RADIUS Authentication Request Probe using UDP/1812
Type	RADIUS
Parent Monitor	radius

Configuration: Advanced

Interval	Specify... 10 seconds
Up Interval	Disabled
Time Until Up	0 seconds
Timeout	Specify... 31 seconds
Manual Resume	<input type="radio"/> Yes <input checked="" type="radio"/> No
User Name	f5-probe
Password
Secret
NAS IP Address	10.199.3
Alias Address	* All Addresses
Alias Service Port	1812
Debug	No

Optional: Configure UDP Profile for RADIUS

Local Traffic > Profiles > Protocol > UDP

- Start with default Idle Timeout
- Using a custom profile allows for tuning later if needed without impacting other services based on same parent UDP profile
- Disable Datagram LB

The screenshot shows the configuration page for a UDP profile named 'ise_radius_udp'. The breadcrumb navigation is 'Local Traffic >> Profiles : Protocol : UDP >> ise_radius_udp'. The 'Properties' tab is selected. The 'General Properties' section includes: Name (ise_radius_udp), Partition / Path (Common), and Parent Profile (udp). The 'Settings' section includes: Proxy Maximum Segment (unchecked), Idle Timeout (Specify... 60 seconds), IP ToS (Specify... 0), Link QoS (Specify... 0), Datagram LB (unchecked), and Allow No Payload (unchecked). Red boxes highlight the 'Idle Timeout' and 'Datagram LB' settings.

General Properties	
Name	ise_radius_udp
Partition / Path	Common
Parent Profile	udp

Settings	
Proxy Maximum Segment	<input type="checkbox"/>
Idle Timeout	Specify... 60 seconds
IP ToS	Specify... 0
Link QoS	Specify... 0
Datagram LB	<input type="checkbox"/>
Allow No Payload	<input type="checkbox"/>

Optional: Configure RADIUS Profile

Local Traffic > Profiles > Services > RADIUS

- Start with default settings
- Using a custom profile allows for tuning later if needed without impacting other services based on same parent radiusLB profile

The screenshot shows the configuration page for a RADIUS profile named 'ise_radiusLB'. The breadcrumb navigation at the top reads 'Local Traffic >> Profiles : Services : RADIUS >> ise_radiusLB'. Below the breadcrumb is a 'Properties' tab with a gear icon. The main content is divided into two sections: 'General Properties' and 'Settings'.

General Properties	
Name	ise_radiusLB
Partition / Path	Common
Parent Profile	radiusLB

Settings	
Persist Attribute	<input type="text"/>
Subscriber Aware	<input type="checkbox"/>
Client Spec	Not Configured
Subscriber ID Type	Calling Station ID

Configure iRule for RADIUS Persistence

Local Traffic > iRules > iRule List

- Recommend iRule based on client MAC address
- RADIUS Attribute/Value Pair = 31 = Calling-Station-Id
- Recommend copy and paste working iRule into text area.

The screenshot shows the configuration page for an iRule named 'radius_mac_sticky'. The breadcrumb navigation is 'Local Traffic >> iRules : iRule List >> radius_mac_sticky'. There are two tabs: 'Properties' (selected) and 'Statistics'. The 'Properties' section contains a table with the following information:

Name	radius_mac_sticky
Partition / Path	Common
Definition	<pre># ISE persistence iRule based on Calling-Station-Id 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"} } } </pre>
Ignore Signature/Checksum	<input type="checkbox"/>

At the bottom of the 'Definition' text area, there are two checkboxes: 'Extend Text Area' and 'Wrap Text', both of which are currently unchecked.

F5 iRule Editor



For Your Reference

<https://devcentral.f5.com/d/tag/irules%20editor>

- Manage iRules and config files
- Syntax checker
- Generate HTTP traffic
- Quick links to tech resources

Configuring RADIUS Persistence

RADIUS Profile Example

- RADIUS Sticky on Calling-Station-ID (client MAC address)
- Simple option but does not support advanced logging and other enhanced parsing options like iRule
- Profile must be applied to Standard Virtual Server based on UDP Protocol

```
ltm profile radius /Common/radiusLB {  
  app-service none  
  clients none  
  persist-avp 31  
  subscriber-aware disabled  
  subscriber-id-type 3gpp-imsi  
}
```

Local Traffic » Profiles : Services : RADIUS » radiusLB

Properties

General Properties

Name	radiusLB
Partition / Path	Common

Settings

Persist Attribute	31
Subscriber Aware	<input type="checkbox"/>
Client Spec	Not Configured
Subscriber ID Type	3GPP IMSI

iRule for RADIUS Persistence Based on Client MAC

Persistence based on Calling-Station-Id (MAC Address) with fallback to NAS-IP-Address

- iRule assigned to Persistence Profile
- Persistence Profile assigned to Virtual Server under Resources section

```
when CLIENT_ACCEPTED {  
  # 0: No Debug Logging  1: Debug Logging  
  set debug 0  
  
  # 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"}  
  }  
}
```

- Optional debug logging
- Enable for troubleshooting only to reduce processing load

- Configurable persistence timeout based on media type
 - Wireless Default = 1 hour
 - Wired Default = 8 hours

RADIUS Persistence iRule Based on MAC (cont.)

```
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 "$nas_ip any virtual"]
        log local0.alert "No MAC Address found - Using NAS IP as persist
id. Username=[RADIUS::avp 1] NAS IP=$nas_ip MEDIA=$access_media
TARGET=$target"
    }
}
}
```

Configure Persistence Profile for RADIUS

Local Traffic > Profiles > Persistence

- Enable **Match Across Services**
- If different Virtual Server IP addresses used for RADIUS Auth and Accounting, then enable Match Across Virtual Servers (not recommended)
- Specify RADIUS Persistence iRule
- iRule persistence timer overrides profile setting.

The screenshot shows the configuration page for a persistence profile named 'radius_sticky'. The breadcrumb path is 'Local Traffic >> Profiles : Persistence >> radius_sticky'. The 'Properties' tab is selected. The 'General Properties' section includes: Name (radius_sticky), Partition / Path (Common), Persistence Type (Universal), and Parent Profile (universal). The 'Configuration' section is set to 'Custom' and includes several options: 'Match Across Services' (checked/Enabled), 'Match Across Virtual Servers' (unchecked), 'Match Across Pools' (unchecked), 'iRule' (set to /Common/radius_mac_sticky), 'Timeout' (set to 300 seconds), and 'Override Connection Limit' (unchecked). Red boxes highlight the 'Match Across Services' checkbox and the 'iRule' dropdown menu.

General Properties	
Name	radius_sticky
Partition / Path	Common
Persistence Type	Universal
Parent Profile	universal

Configuration		Custom <input checked="" type="checkbox"/>
Match Across Services	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/>
Match Across Virtual Servers	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Match Across Pools	<input type="checkbox"/>	<input checked="" type="checkbox"/>
iRule	/Common/radius_mac_sticky	<input checked="" type="checkbox"/>
Timeout	Specify... 300 seconds	<input checked="" type="checkbox"/>
Override Connection Limit	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Configure Server Pool for RADIUS Auth

Local Traffic > Pools > Pool List

- Health Monitor = RADIUS Monitor
- SNAT = No
- Action on Service Down = Reselect
 - Ensures existing connections are moved to an alternate server.

The screenshot shows the configuration page for a server pool named 'radius_auth_pool'. The breadcrumb path is 'Local Traffic >> Pools : Pool List >> radius_auth_pool'. The 'Properties' tab is selected. The 'General Properties' section includes:

Name	radius_auth_pool
Partition / Path	Common
Description	PSN Pool for RADIUS Authenticaion and Authorization
Availability	● Available (Enabled) - The pool is available

The 'Configuration' section is set to 'Advanced'. It features two lists of health monitors:

- Active:** A list containing '/Common/radius_1812', which is highlighted with an orange box.
- Available:** A list containing '/Common/gateway_icmp', '/Common/http', '/Common/http_head_f5', and '/Common/https'.

Navigation arrows (<< and >>) are present between the two lists. Below the lists, the following settings are configured:

Availability Requirement	All Health Monitor(s)
Allow SNAT	No
Allow NAT	Yes
Action On Service Down	Reselect

Configure Member Nodes in RADIUS Auth Pool

Local Traffic > Pools > Pool List > Members

- Load Balancing Method options:
 - Least Connections (node)
 - Least Connections (member)
- Server Port: 1812 or 1645

Local Traffic >> Pools : Pool List >> radius_auth_pool

Properties Members Statistics

Load Balancing

Load Balancing Method: Least Connections (node)

Priority Group Activation: Disabled

Update

Current Members Add...

<input checked="" type="checkbox"/>	Status	Member	Address	Ratio	Priority Group	Connection Limit	Partition / Path
<input type="checkbox"/>	●	ise-psn-1 1812	10.1.99.15	1	0 (Active)	0	Common
<input type="checkbox"/>	●	ise-psn-2 1812	10.1.99.16	1	0 (Active)	0	Common
<input type="checkbox"/>	●	ise-psn-3 1812	10.1.99.17	1	0 (Active)	0	Common

Configure Server Pool for RADIUS Accounting

Local Traffic > Pools > Pool List

- Health Monitor = RADIUS Monitor (same monitor used for RADIUS Auth)
- SNAT = No
- Action on Service Down = Reselect
 - Ensures existing connections are moved to an alternate server.

The screenshot shows the configuration page for a server pool named 'radius_acct_pool'. The breadcrumb path is 'Local Traffic >> Pools : Pool List >> radius_acct_pool'. The 'Properties' tab is selected, showing the following details:

General Properties	
Name	radius_acct_pool
Partition / Path	Common
Description	PSN Pool for RADIUS Accounting
Availability	● Available (Enabled) - The pool is available

The 'Configuration' section is set to 'Advanced' and shows the following settings:

	Active	Available
Health Monitors	<i>/Common</i> radius_1812	<i>/Common</i> gateway_icmp http http_head_f5 https
Availability Requirement	All	Health Monitor(s)
Allow SNAT	No	
Allow NAT	Yes	
Action On Service Down	Reselect	

Configure Member Nodes in RADIUS Accounting Pool

Local Traffic > Pools > Pool List > Members

- Load Balancing Method options:
 - Least Connections (node)
 - Least Connections (member)
 - Fastest (application)
- Server Port: 1813 or 1646

Local Traffic >> Pools : Pool List >> radius_acct_pool

Properties Members Statistics

Load Balancing

Load Balancing Method: Least Connections (node)

Priority Group Activation: Disabled

Update

Current Members Add...

<input checked="" type="checkbox"/>	Status	Member	Address	Ratio	Priority Group	Connection Limit	Partition / Path
<input type="checkbox"/>	●	ise-psn-1 1813	10.1.99.15	1	0 (Active)	0	Common
<input type="checkbox"/>	●	ise-psn-2 1813	10.1.99.16	1	0 (Active)	0	Common
<input type="checkbox"/>	●	ise-psn-3 1813	10.1.99.17	1	0 (Active)	0	Common

Configure Virtual Server for RADIUS Auth (Properties)

Local Traffic > Virtual Servers > Virtual Server List

- Type = Standard
- Source = 0.0.0.0/0 (all hosts) or specific network address.
- Destination = RADIUS Virtual IP
- Service Port = 1812 or 1645

Local Traffic >> Virtual Servers : Virtual Server List >> ise_radius_auth	
Settings	Properties Resources Statistics
General Properties	
Name	ise_radius_auth
Partition / Path	Common
Description	ISE PSN RADIUS Authentication and Authorization
Type	Standard
Source	10.0.0.0/8
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.1.98.8
Service Port	1812 Other: [Dropdown]
Availability	<input checked="" type="radio"/> Available (Enabled) - The virtual server is available
State	Enabled

Configure Virtual Server for RADIUS Auth (Advanced)

Local Traffic > Virtual Servers

- Protocol = UDP
- Protocol Profile = udp or custom UDP profile
- RADIUS Profile = radiusLB or custom RADIUS profile
- Optional: Limit traffic to specific VLAN(s)
- **SNAT = None**

Configuration: Advanced	
Protocol	UDP
Protocol Profile (Client)	ise_radius_udp
Protocol Profile (Server)	(Use Client Profile)

RADIUS Profile	ise_radiusLB									
SIP Profile	None									
Statistics Profile	None									
VLAN and Tunnel Traffic	Enabled on...									
VLANs and Tunnels	<table><thead><tr><th>Selected</th><th></th><th>Available</th></tr></thead><tbody><tr><td>/Common external</td><td><<</td><td>/Common internal portals</td></tr><tr><td></td><td>>></td><td></td></tr></tbody></table>	Selected		Available	/Common external	<<	/Common internal portals		>>	
Selected		Available								
/Common external	<<	/Common internal portals								
	>>									
Source Address Translation	None									

Configure Virtual Server RADIUS Auth (Resources)

Local Traffic > Virtual Servers > Virtual Server List > Resources

- Default Pool = RADIUS Auth Pool
- Default Persistence Profile = RADIUS persistence profile
- Fallback Persistence Profile:
 - RADIUS iRule setting overrides value set here.
 - If not configured in iRule, set optional value here. Example: **radius_source_addr**

Recommend create new persistence profile based on Source Address Affinity to allow custom timers and match settings.

Local Traffic >> Virtual Servers : Virtual Server List >> ise_radius_auth

Properties Resources Statistics

Load Balancing

Default Pool	radius_auth_pool
Default Persistence Profile	radius_sticky
Fallback Persistence Profile	None

Update

iRules

Name

No records to display.

Configure Virtual Server for RADIUS Accounting

Local Traffic > Virtual Servers > Virtual Server List

- Same settings as RADIUS Auth Virtual Server but different service port and pool

Local Traffic >> Virtual Servers : Virtual Server List >> ise_radius_acct

Properties Resources Statistics

General Properties

Name	ise_radius_acct
Partition / Path	Common
Description	ISE PSN RADIUS Accounting
Type	Standard
Source	10.0.0.0/8
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.1.98.8
Service Port	1813 Other: <input type="text"/>
Availability	<input checked="" type="radio"/> Available (Enabled) - The virtual server is available
State	Enabled <input type="text"/>

RADIUS VIP

Local Traffic >> Virtual Servers : Virtual Server List >> ise_radius_acct

Properties Resources Statistics

Load Balancing

Default Pool	radius_acct_pool
Default Persistence Profile	radius_sticky
Fallback Persistence Profile	None

Update

iRules

Name	
------	--

No records to display.

Configure SNAT Pool List for RADIUS CoA

Local Traffic > Address Translation > SNAT Pool List

- CoA traffic is initiated by PSN to NADs on UDP/1700
- Define SNAT Pool List with RADIUS Server Virtual IP as a pool member

The screenshot shows the configuration page for a SNAT Pool List named 'radius_coa_snatpool'. The breadcrumb path is 'Local Traffic >> Address Translation : SNAT Pool List >> radius_coa_snatpool'. There are two tabs: 'Properties' (selected) and 'Statistics'. The 'General Properties' section shows the name 'radius_coa_snatpool' and the partition/path 'Common'. The 'Configuration' section includes an 'IP Address' input field, an 'Add' button, a list box containing '10.1.98.8', and 'Edit' and 'Delete' buttons.

General Properties	
Name	radius_coa_snatpool
Partition / Path	Common

Configuration	
Member List	IP Address: <input type="text"/>
	<input type="button" value="Add"/>
	<div style="border: 1px solid gray; padding: 5px;">10.1.98.8</div>
	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Configure Virtual Server to SNAT RADIUS CoA (Properties)

Local Traffic > Virtual Servers > Virtual Server List

- CoA traffic is initiated by PSN to NADs on UDP/1700
- Type = Standard
- Source = PSN Network
- Destination = 0.0.0.0 / 0.0.0.0 (all hosts) or specific network for all NADs
- Service Port = 1700

The screenshot displays the configuration page for a virtual server named 'RADIUS-COA-SNAT'. The breadcrumb trail at the top reads 'Local Traffic >> Virtual Servers : Virtual Server List >> RADIUS-COA-SNAT'. Below the breadcrumb is a navigation bar with tabs for 'Properties', 'Resources', and 'Statistics'. The 'Properties' tab is selected and highlighted in yellow.

The main content area is titled 'General Properties' and contains a table of configuration fields:

Name	RADIUS-COA-SNAT
Partition / Path	Common
Description	
Type	Standard
Source	10.1.99.0/27
Destination	Type: <input type="radio"/> Host <input checked="" type="radio"/> Network Address: 10.0.0.0 Mask: 255.0.0.0
Service Port	1700 Other: <input type="text"/>
Availability	<input checked="" type="checkbox"/> Unknown (Enabled) - The children pool memb
State	Enabled

The 'Service Port' field is highlighted with an orange border, showing the value '1700' and an 'Other:' dropdown menu.

Configure Virtual Server to SNAT RADIUS CoA (Advanced)

Local Traffic > Virtual Servers

- Protocol = UDP
- Optional: Limit traffic to specific VLAN(s)
- Source Address Translation = SNAT
- SNAT Pool = CoA SNAT Pool List
- Resources = None

Local Traffic >> Virtual Servers : Virtual Server List >> RADIUS-COA-SNAT

Properties Resources Statistics

Load Balancing

Default Pool	None
Default Persistence Profile	None
Fallback Persistence Profile	None

Configuration: Advanced

Protocol	UDP
Protocol Profile (Client)	udp
Protocol Profile (Server)	(Use Client Profile)

VLAN and Tunnel Traffic

Enabled on...

VLANs and Tunnels

Selected	Available
/Common internal	/Common external portals

Source Address Translation

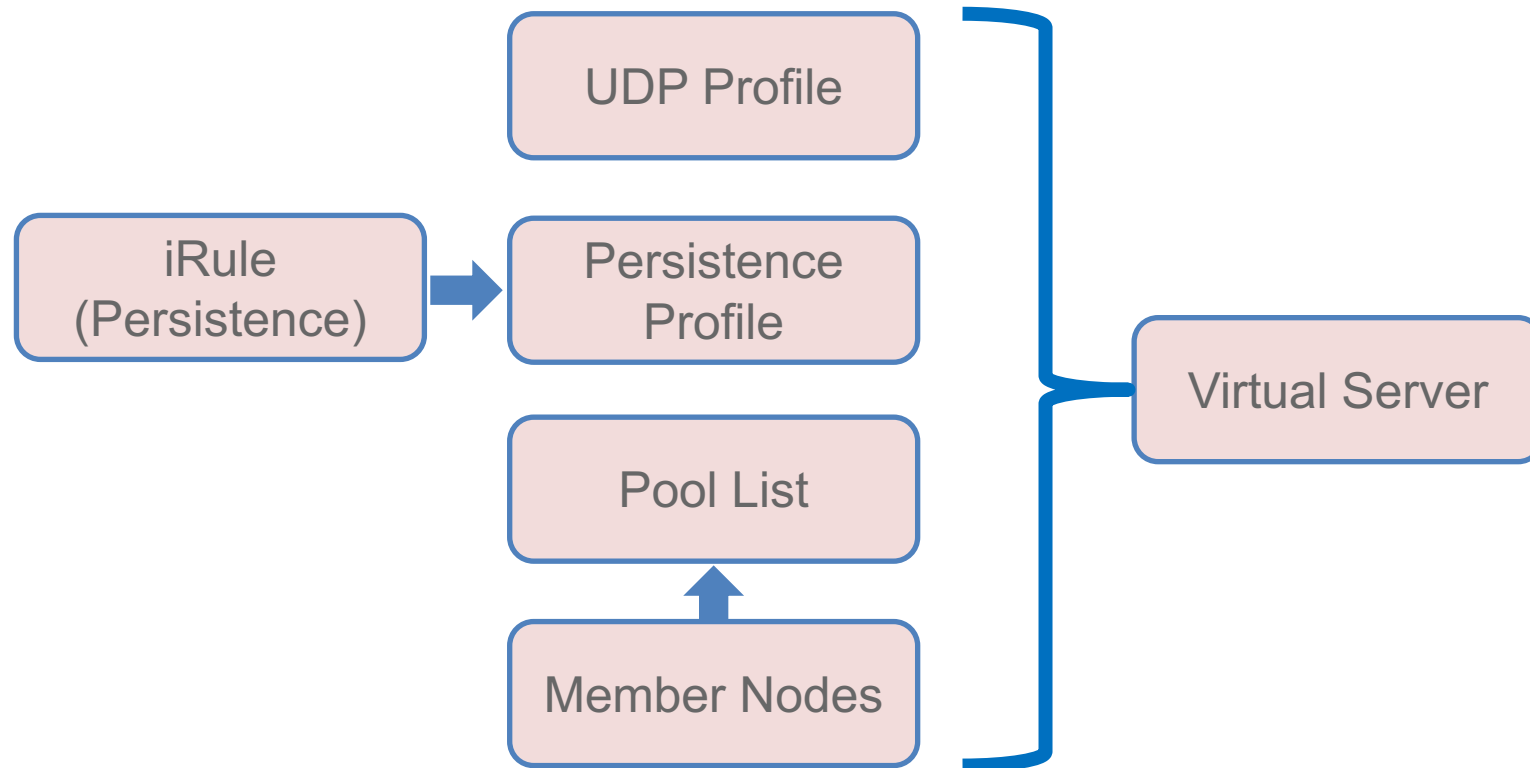
SNAT

SNAT Pool

radius_coa_snatpool

Load Balancing ISE Profiling

F5 LTM Configuration Components for Profiling LB



Configure UDP Profile for Profiling

Local Traffic > Profiles > Protocol > UDP

- Set Idle Timeout to Immediate
Profiling traffic from DHCP and SNMP Traps are one-way flows to PSNs—no response sent to these packets.
- Be sure to create new UDP profile to ensure these settings are applied only to Profiling.
- Using a custom profile allows for tuning later if needed without impacting other services based on same parent UDP profile
- Disable Datagram LB

Local Traffic >> Profiles : Protocol : UDP >> ise_profiling_udp	
Properties	
General Properties	
Name	ise_profiling_udp
Partition / Path	Common
Parent Profile	udp
Settings Custom <input checked="" type="checkbox"/>	
Proxy Maximum Segment	<input type="checkbox"/> <input checked="" type="checkbox"/>
Idle Timeout	Immediate <input checked="" type="checkbox"/>
IP ToS	Specify... 0 <input checked="" type="checkbox"/>
Link QoS	Specify... 0 <input checked="" type="checkbox"/>
Datagram LB	<input type="checkbox"/> <input checked="" type="checkbox"/>
Allow No Payload	<input type="checkbox"/> <input checked="" type="checkbox"/>

iRule for DHCP Persistence Based on Client MAC (1 of 2)

Persistence based on DHCP Option 61 – Client Identifier (MAC Address)

- iRule assigned to Persistence Profile
- Persistence Profile assigned to Virtual Server under Resources section

```
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
```

- Optional debug logging
- Enable for troubleshooting only to reduce processing load

- Configurable persistence timeout

iRule for DHCP Persistence Based on Client MAC (2 of 2)

```
# extract value filed 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
    binary scan $value_hex a2a* ht id
    switch $ht {
    01 {
      binary scan $id a2a2a2a2a2 m(a) m(b) m(c) m(d) m(e) m(f)
      set value [string toupper "$m(a)-$m(b)-$m(c)-$m(d)-$m(e)-$m(f)"]
    }                                # Normalize MAC address to upper case
    default {
      set value "$id"
    }
  }
  }
  persist uie $value $static::persist_ttl
  if {$static::debug}{
    log local0.debug "$log_prefix_d ***** iRule: $static::RULE_NAME
completed ***** OPTION61=$value TARGET=[persist lookup uie "$value any
virtual"]"
```

Note: Example is excerpt only—Not complete iRule

iRule for DHCP Persistence – Sample Debug Output

```
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=
```


Optional: Configure Persistence Profile for Profiling

Local Traffic > Profiles > Persistence

- Enable **Match Across Services**
- If different Virtual Server IP addresses used for DHCP Profiling and RADIUS, then enable Match Across Virtual Servers. (Recommend use same IP address)
- Specify DHCP Persistence iRule
- iRule persistence timer overrides profile setting.

The screenshot shows the configuration page for a persistence profile named 'dhcp_sticky'. The breadcrumb navigation is 'Local Traffic >> Profiles : Persistence >> dhcp_sticky'. The 'Properties' tab is selected. The 'General Properties' section includes: Name (dhcp_sticky), Partition / Path (Common), Persistence Type (Universal), and Parent Profile (universal). The 'Configuration' section is set to 'Custom' and includes: Match Across Services (checked/Enabled), Match Across Virtual Servers (unchecked), Match Across Pools (unchecked), iRule (/Common/dhcp_mac_sticky), Timeout (Specify... 300 seconds), and Override Connection Limit (unchecked).

General Properties	
Name	dhcp_sticky
Partition / Path	Common
Persistence Type	Universal
Parent Profile	universal

Configuration		Custom <input checked="" type="checkbox"/>
Match Across Services	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/>
Match Across Virtual Servers	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Match Across Pools	<input type="checkbox"/>	<input checked="" type="checkbox"/>
iRule	/Common/dhcp_mac_sticky	<input checked="" type="checkbox"/>
Timeout	Specify... 300 seconds	<input checked="" type="checkbox"/>
Override Connection Limit	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Configure Server Pool for DHCP Profiling

Local Traffic > Pools > Pool List

- Health Monitor = RADIUS Monitor
 - If PSN not configured for User Services (RADIUS auth), then can use default **gateway_icmp** monitor.
- Action on Service Down = Reselect
 - Ensures existing connections are moved to an alternate server.

The screenshot shows the configuration page for a server pool named 'profiling_dhcp_pool'. The breadcrumb path is 'Local Traffic >> Pools : Pool List >> profiling_dhcp_pool'. The 'Properties' tab is selected. The 'General Properties' section shows the pool name, partition, description, and availability status. The 'Configuration' section is set to 'Advanced' and shows health monitors, availability requirements, and actions on service down. Two orange boxes highlight the 'radius_1812' health monitor in the 'Active' list and the 'Reselect' action on service down.

Local Traffic >> Pools : Pool List >> profiling_dhcp_pool			
⚙️	Properties	Members	Statistics
General Properties			
Name	profiling_dhcp_pool		
Partition / Path	Common		
Description	PSN Pool for DHCP Profiling		
Availability	● Available (Enabled) - The pool is available		
Configuration: Advanced			
Health Monitors	Active	<<	Available
	/Common radius_1812	>>	/Common gateway_icmp http http_head_f5 https
Availability Requirement	All	Health Monitor(s)	
Allow SNAT	Yes		
Allow NAT	Yes		
Action On Service Down	Reselect		

Configure Member Nodes in DHCP Profiling Pool

Local Traffic > Pools > Members

- Load Balancing Method = Round Robin
- Server Port = 67 (DHCP Server)

Local Traffic >> Pools : Pool List >> profiling_dhcp_pool

Properties Members Statistics

Load Balancing

Load Balancing Method: Round Robin

Priority Group Activation: Disabled

Update

Current Members Add...

<input checked="" type="checkbox"/>	Status	Member	Address	Ratio	Priority Group	Connection Limit	Partition / Path
<input type="checkbox"/>	●	ise-psn-1 67	10.1.99.15	1	0 (Active)	0	Common
<input type="checkbox"/>	●	ise-psn-2 67	10.1.99.16	1	0 (Active)	0	Common
<input type="checkbox"/>	●	ise-psn-3 67	10.1.99.17	1	0 (Active)	0	Common

Configure Server Pool for SNMP Trap Profiling

Local Traffic > Pools

- Same settings as DHCP Profiling Pool except members configured for UDP Port 162.

Local Traffic >> Pools : Pool List >> profiling_snmptrap_pool

Properties Members Statistics

Load Balancing

Load Balancing Method: Round Robin

Priority Group Activation: Disabled

Update

Current Members Add...

<input checked="" type="checkbox"/>	Status	Member	Address	Ratio	Priority Group	Connection Limit	Partition / Path
<input type="checkbox"/>	●	ise-psn-1 162	10.1.99.15	1	0 (Active)	0	Common
<input type="checkbox"/>	●	ise-psn-2 162	10.1.99.16	1	0 (Active)	0	Common
<input type="checkbox"/>	●	ise-psn-3 162	10.1.99.17	1	0 (Active)	0	Common

Configure Virtual Server for DHCP Profiling (Properties)

Local Traffic > Virtual Servers > Virtual Server List

- Type = Standard
- Source = 0.0.0.0/0 (all hosts) or specific network address.
- Destination = Can be same as RADIUS Virtual IP or unique IP.

Be sure to configure DHCP Relays/ IP Helpers to point to this IP address

- Service Port = 67

Local Traffic >> Virtual Servers : Virtual Server List >> ise_profiling_dhcp	
⚙️	Properties Resources Statistics
General Properties	
Name	ise_profiling_dhcp
Partition / Path	Common
Description	ISE PSN DHCP Profiling
Type	Standard
Source	10.0.0.0/8
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.1.98.8
Service Port	67 Other:
Availability	● Available (Enabled) - The virtual server is available
State	Enabled

Configure Virtual Server for DHCP Profiling (Advanced)

Local Traffic > Virtual Servers

- Protocol = UDP
- Protocol Profile = udp or custom UDP profile
- Optional: Limit traffic to specific VLAN(s)

Configuration: <input type="text" value="Advanced"/>	
Protocol	<input type="text" value="UDP"/>
Protocol Profile (Client)	<input type="text" value="ise_profiling_udp"/>
Protocol Profile (Server)	<input type="text" value="(Use Client Profile)"/>

VLAN and Tunnel Traffic	<input type="text" value="Enabled on..."/>						
VLANs and Tunnels	<table border="1"><thead><tr><th>Selected</th><th></th><th>Available</th></tr></thead><tbody><tr><td>/Common external</td><td><< >></td><td>/Common internal portals</td></tr></tbody></table>	Selected		Available	/Common external	<< >>	/Common internal portals
Selected		Available					
/Common external	<< >>	/Common internal portals					
Source Address Translation	<input type="text" value="None"/>						

Configure Virtual Server for DHCP Profiling (Resources)

Local Traffic > Virtual Servers > Resources

- Default Pool = DHCP Profiling Pool
- Default Persistence Profile = Persistence Profile based on Source Address Affinity, *OR* DHCP persistence profile
- Fallback Persistence Profile:
 - DHCP iRule setting overrides value set here.
 - If not configured in iRule, set optional value here. Example: **profiling_source_addr**
- If persistence profile based on Source Address Affinity (source_addr), recommend create new profile to allow custom timers and “Match Across” settings.

Local Traffic >> Virtual Servers : Virtual Server List >> ise_profiling_dhcp

Properties Resources Statistics

Load Balancing

Default Pool	profiling_dhcp_pool
Default Persistence Profile	profiling_source_addr
Fallback Persistence Profile	None

Local Traffic >> Virtual Servers : Virtual Server List >> ise_profiling_dhcp

Properties Resources Statistics

Load Balancing

Default Pool	profiling_dhcp_pool
Default Persistence Profile	dhcp_sticky
Fallback Persistence Profile	None

Configure Virtual Server for SNMP Trap Profiling

Local Traffic > Virtual Servers

Local Traffic >> Virtual Servers : Virtual Server List >> ise_profiling_snmptrap

Properties Resources Statistics

General Properties

Name	ise_profiling_snmptrap
Partition / Path	Common
Description	ISE PSN SNMP Trap Profiling
Type	Standard
Source	10.0.0.0/8
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.1.98.8
Service Port	162 SNMP-TRAP
Availability	● Available (Enabled) - The virtual server is available
State	Enabled

- Same settings as DHCP Profiling Virtual Server but different service port and pool.

Additionally, Default Persistence Profile should be based on Source Address Affinity (NAD IP address).

Local Traffic >> Virtual Servers : Virtual Server List >> ise_profiling_

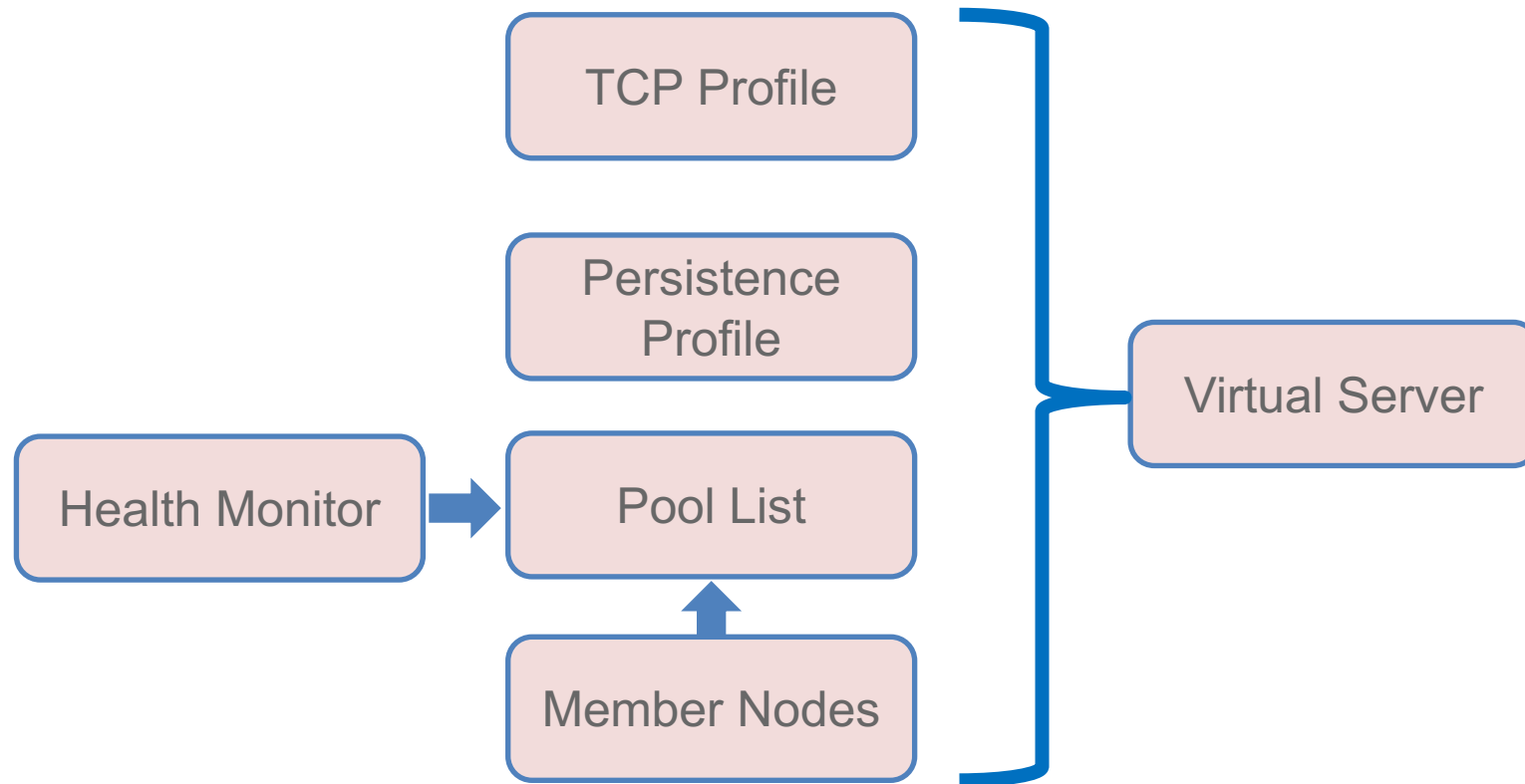
Properties Resources Statistics

Load Balancing

Default Pool	profiling_snmptrap_pool
Default Persistence Profile	profiling_source_addr
Fallback Persistence Profile	None

Load Balancing ISE Web Services

F5 LTM Configuration Components for HTTP/S LB



Configure HTTPS Health Monitor

Local Traffic > Monitors

- Configure Send and Receive Strings appropriate to ISE version
- Set UserName and Password to *any* value (does not have to be valid user account)
- Alias Service Port = Portal Port configured in ISE

Local Traffic >> Monitors >> ise_https_8443

⚙️ Properties Instances

General Properties

Name	ise_https_8443
Partition / Path	Common
Description	HTTPS Health Monitor for ISE Portal Services
Type	HTTPS
Parent Monitor	https

Configuration: Advanced

Interval	Specify... 5 seconds
Up Interval	Disabled
Time Until Up	0 seconds
Timeout	Specify... 16 seconds
Manual Resume	<input type="radio"/> Yes <input checked="" type="radio"/> No
Send String	GET /sponsorportal/
Receive String	HTTP/1.1 200 OK
Receive Disable String	
Cipher List	DEFAULT:+SHA:+3DES:+kEDH
User Name	xxx
Password
Compatibility	Enabled
Client Certificate	None
Client Key	None
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No
Alias Address	* All Addresses
Alias Service Port	8443

HTTPS Health Monitor Examples

Local Traffic > Monitors

- ISE 1.2 Example
 - Send String: `GET /sponsorportal/`
 - Receive String: `HTTP/1.1 200 OK`
- ISE 1.3+ Example
 - Send String:
`GET /sponsorportal/PortalSetup.action?portal=Sponsor%20Portal%20%28default%29`
 - Receive String: `HTTP/1.1 200 OK`

Optional: Configure TCP Profile for HTTPS

Local Traffic > Profiles > Protocol > TCP

- Start with default Idle Timeout
- Using a custom profile allows for tuning later if needed without impacting other services based on same parent TCP profile

The screenshot shows the configuration page for a TCP profile named 'ise_https_tcp'. The breadcrumb path is 'Local Traffic >> Profiles : Protocol : TCP >> ise_https_tcp'. The 'Properties' tab is selected. The 'General Properties' section shows the profile name, partition, and parent profile. The 'Settings' section is set to 'Custom' and includes various TCP-related options with checkboxes and input fields.

General Properties	
Name	ise_https_tcp
Partition / Path	Common
Parent Profile	tcp

Settings		Custom <input checked="" type="checkbox"/>
Reset On Timeout	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/>
Time Wait Recycle	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/>
Delayed Acks	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/>
Proxy Maximum Segment	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Proxy Options	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Proxy Buffer Low	32768 bytes	<input checked="" type="checkbox"/>
Proxy Buffer High	49152 bytes	<input checked="" type="checkbox"/>
Idle Timeout	Specify... 300 seconds	<input checked="" type="checkbox"/>

Configure Persistence Profile for HTTPS

Local Traffic > Profiles > Persistence

- Enable **Match Across Services**
- If different Virtual Server IP addresses used for Web Services, then enable Match Across Virtual Servers

Generally recommend use same VIP address for all portals

- Timeout = Persistence timer

Value of 1200 seconds = 20 minutes (default Sponsor Portal idle timeout setting in ISE)

The screenshot shows the configuration page for a persistence profile named 'https_sticky'. The breadcrumb navigation is 'Local Traffic >> Profiles : Persistence >> https_sticky'. The 'Properties' tab is selected. The 'General Properties' section includes: Name (https_sticky), Partition / Path (Common), Persistence Type (Source Address Affinity), and Parent Profile (source_addr). The 'Configuration' section is set to 'Custom' and includes several options: Match Across Services (checked/Enabled), Match Across Virtual Servers (unchecked), Match Across Pools (unchecked), Hash Algorithm (Default), Timeout (Specify... dropdown, 1200 seconds), Mask (None), Map Proxies (checked/Enabled), and Override Connection Limit (unchecked). The 'Match Across Services' and 'Timeout' rows are highlighted with orange boxes.

General Properties	
Name	https_sticky
Partition / Path	Common
Persistence Type	Source Address Affinity
Parent Profile	source_addr

Configuration		Custom <input checked="" type="checkbox"/>
Match Across Services	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/>
Match Across Virtual Servers	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Match Across Pools	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Hash Algorithm	Default	<input checked="" type="checkbox"/>
Timeout	Specify... 1200 seconds	<input checked="" type="checkbox"/>
Mask	None	<input checked="" type="checkbox"/>
Map Proxies	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/>
Override Connection Limit	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Configure Server Pool for Web Services

Local Traffic > Pools > Pool List

- Health Monitor = HTTPS Monitor
- Action on Service Down = None

The screenshot shows the configuration page for a server pool named 'web_portals_pool'. The breadcrumb navigation is 'Local Traffic >> Pools : Pool List >> web_portals_pool'. The 'Properties' tab is selected. The 'General Properties' section shows the pool name, partition/path, description, and availability status. The 'Configuration' section is set to 'Advanced' and shows health monitors, availability requirements, and other settings.

General Properties	
Name	web_portals_pool
Partition / Path	Common
Description	Shared pool for LB of all ISE web portal traffic
Availability	● Available (Enabled) - The pool is available

Configuration: Advanced

	Active	Available
Health Monitors	<i>/Common</i> ise_https_8443	<i>/Common</i> gateway_icmp http http_head_f5 https
Availability Requirement	All	Health Monitor(s)
Allow SNAT	Yes	
Allow NAT	Yes	
Action On Service Down	None	

Configure Member Nodes in Web Services Pool

Local Traffic > Pools > Pool List > Members

- Load Balancing Method options:
 - Least Connections (node)
 - Least Connections (member)
 - Fastest (application)
- Server Port = 0 (all ports)

Local Traffic >> Pools : Pool List >> web_portals_pool

Properties Members Statistics

Load Balancing

Load Balancing Method: Least Connections (node)

Priority Group Activation: Disabled

Update

Current Members Add...

<input checked="" type="checkbox"/>	Status	Member	Address	Ratio	Priority Group	Connection Limit	Partition / Path
<input type="checkbox"/>	●	ise-psn-1-web 0	10.1.91.15	1	0 (Active)	0	Common
<input type="checkbox"/>	●	ise-psn-2-web 0	10.1.91.16	1	0 (Active)	0	Common
<input type="checkbox"/>	●	ise-psn-3-web 0	10.1.91.17	1	0 (Active)	0	Common

Configure Virtual Server for Web Portals (Properties)

Local Traffic > Virtual Servers > Virtual Server List

- Type = Standard
- Source = 0.0.0.0/0 (all hosts) or specific network address.
- Destination = Web Portal Virtual IP
- Service Port = Web Portal Port configured in ISE (default 8443)

The screenshot shows the configuration page for a virtual server. The breadcrumb path is 'Local Traffic >> Virtual Servers : Virtual Server List >> ise_https8443_portals'. The 'Properties' tab is selected. The 'General Properties' section contains the following fields:

Name	ise_https8443_portals
Partition / Path	Common
Description	ISE PSN Web Portals on TCP/8443
Type	Standard
Source	10.0.0.0/8
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.1.98.8
Service Port	8443 Other: <input type="text"/>
Availability	<input checked="" type="radio"/> Available (Enabled) - The virtual server is available
State	Enabled

Configure Virtual Server for HTTPS Portals (Advanced)

Local Traffic > Virtual Servers

- Protocol = TCP
- Protocol Profile = tcp or custom TCP profile
- Optional: Limit traffic to specific VLAN(s)
- Source Address Translation (SNAT)
 - Single PSN interface: **None**
 - Dedicated PSN interface (ISE 1.2): **Auto Map**
 - Dedicated PSN interface (ISE 1.3): **None or Auto Map**

Configuration: **Advanced** ▼

Protocol	TCP ▼
Protocol Profile (Client)	ise_https_tcp ▼
Protocol Profile (Server)	(Use Client Profile) ▼
OneConnect Profile	None ▼
NTLM Conn Pool	None ▼
HTTP Profile	None ▼

VLAN and Tunnel Traffic	Enabled on... ▼									
VLANs and Tunnels	<table><thead><tr><th>Selected</th><th></th><th>Available</th></tr></thead><tbody><tr><td>/Common external</td><td><<</td><td>/Common internal portals</td></tr><tr><td></td><td>>></td><td></td></tr></tbody></table>	Selected		Available	/Common external	<<	/Common internal portals		>>	
Selected		Available								
/Common external	<<	/Common internal portals								
	>>									
Source Address Translation	Auto Map ▼									

Configure Virtual Server HTTPS Portals (Resources)

Local Traffic > Virtual Servers > Virtual Server List > Resources

- Default Pool = Web Portals Pool
- Default Persistence Profile = HTTPS persistence profile
- Fallback Persistence Profile: Not required

The screenshot shows the configuration page for a Virtual Server in Cisco ISE. The breadcrumb navigation is 'Local Traffic >> Virtual Servers : Virtual Server List >> ise_https_portals'. The 'Resources' tab is selected. Under the 'Load Balancing' section, three dropdown menus are visible: 'Default Pool' set to 'web_portals_pool', 'Default Persistence Profile' set to 'https_sticky', and 'Fallback Persistence Profile' set to 'None'. An 'Update' button is located below these settings. Below the 'Load Balancing' section are two empty tables: 'iRules' and 'HTTP Class Profiles', both showing 'No records to display.'

Load Balancing	
Default Pool	web_portals_pool
Default Persistence Profile	https_sticky
Fallback Persistence Profile	None

iRules	
Name	
No records to display.	

HTTP Class Profiles	
Name	
No records to display.	

Configure Virtual Server for Web Portals on TCP/443

Local Traffic > Virtual Servers > Virtual Server List

- Virtual Server used to forward web traffic sent to portal FQDN on default HTTPS port 443
- PSNs will automatically redirect traffic to FQDN to specific portal port / URL.
- Service Port = 443 (HTTPS)
Default HTTPS port used in initial portal request by end user.
- All other Virtual Server settings the same port-specific Virtual Server (Example: ise_https8443_portals)

Local Traffic >> Virtual Servers : Virtual Server List >> ise_https_portals

Properties Resources Statistics

General Properties

Name	ise_https_portals
Partition / Path	Common
Description	ISE PSN Web Portals on TCP/443
Type	Standard
Source	10.0.0.0/8
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.1.98.8
Service Port	443 HTTPS
Availability	<input checked="" type="radio"/> Available (Enabled) - The virtual server is available
State	Enabled

Configure Virtual Server for Web Portals on TCP/80

Local Traffic > Virtual Servers > Virtual Server List

- Virtual Server used to forward web traffic sent to portal FQDN on default HTTP port 80
- PSNs will automatically redirect traffic to FQDN to specific portal port / URL.
- Service Port = 80 (HTTP)
Default HTTP port used in initial portal request by end user.
- All other Virtual Server settings the same port-specific Virtual Server (Example: ise_https8443_portals)

The screenshot displays the configuration page for a virtual server named 'ise_http_portals'. The breadcrumb navigation at the top reads 'Local Traffic >> Virtual Servers : Virtual Server List >> ise_http_portals'. Below the navigation are tabs for 'Properties', 'Resources', and 'Statistics', with 'Properties' selected. The main content area is titled 'General Properties' and contains a table of configuration details.

General Properties	
Name	ise_http_portals
Partition / Path	Common
Description	ISE PSN Web Portals on TCP/80
Type	Standard
Source	10.0.0.0/8
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.1.98.8
Service Port	80 HTTP
Availability	● Available (Enabled) - The virtual server is available
State	Enabled

Configure Virtual Server for Web Portals on TCP/80

Optional HTTP -> HTTPS Redirect by F5 LTM

To configure F5 LTM to perform automatic HTTP to HTTPS redirect instead of PSNs:

- Configure new http profile under Profiles > Services > HTTP using default settings
- Configure new http class under Profiles > Protocol > HTTP Class. Under Actions, set redirect URL.
- Under Virtual Server for HTTP (TCP/80):
 - Specify HTTP Profile under Advanced Configuration
 - Specify new HTTP Class under Resources > HTTP Class Profiles.

Actions	
Send To	Redirect to... ▼
Redirect to Location	https://sponsor.cts.local:8443/sponsorportal/

Configuration: Advanced ▼	
Protocol	TCP ▼
Protocol Profile (Client)	ise_https_tcp ▼
Protocol Profile (Server)	(Use Client Profile) ▼
OneConnect Profile	None ▼
NTLM Conn Pool	None ▼
HTTP Profile	ise_http ▼

HTTP Class Profiles	
Name	
ise_httpclass	

Virtual Server List

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"/>		PSN-IP-Forwarding-Inbound		10.1.99.0/27	0 (Any)	Forwarding (IP)	Edit...	Common
<input type="checkbox"/>		PSN-IP-Forwarding-Inbound-Web		10.1.91.0/27	8443	Forwarding (IP)	Edit...	Common
<input type="checkbox"/>		PSN-IP-Forwarding-Outbound		any	0 (Any)	Forwarding (IP)	Edit...	Common
<input type="checkbox"/>		RADIUS-COA-SNAT		10.0.0.0/8	1700	Standard	Edit...	Common
<input type="checkbox"/>		ise13_https_portals		10.1.98.88	0 (Any)	Standard	Edit...	Common
<input type="checkbox"/>		ise_http_portals		10.1.98.8	80 (HTTP)	Standard	Edit...	Common
<input type="checkbox"/>		ise_https8443_portals		10.1.98.8	8443	Standard	Edit...	Common
<input type="checkbox"/>		ise_https_portals		10.1.98.8	443 (HTTPS)	Standard	Edit...	Common
<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

Server Pool List

Local Traffic >> Pools : Pool List

Pool List Statistics

* Search Create...

<input checked="" type="checkbox"/>	Status	Name	Application	Members	Partition / Path
<input type="checkbox"/>	●	http_portals_pool		3	Common
<input type="checkbox"/>	●	https8443_portals_pool		3	Common
<input type="checkbox"/>	●	https_portals_pool		3	Common
<input type="checkbox"/>	●	profiling_dhcp_pool		3	Common
<input type="checkbox"/>	●	profiling_netflow_pool		3	Common
<input type="checkbox"/>	●	profiling_snmptrap_pool		3	Common
<input type="checkbox"/>	●	radius_acct_pool		3	Common
<input type="checkbox"/>	●	radius_auth_pool		3	Common
<input type="checkbox"/>	●	web_portals_pool		3	Common

Thank You