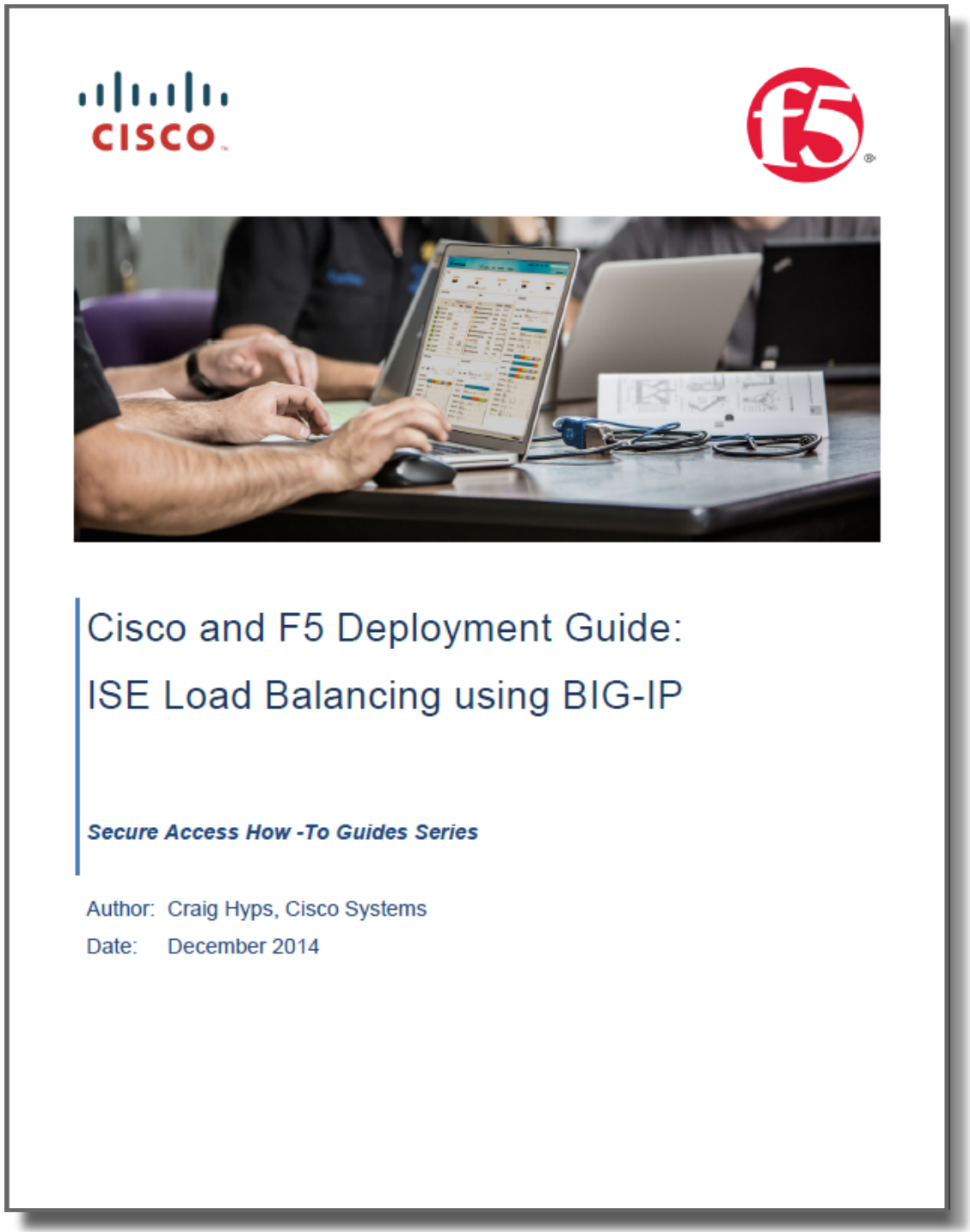
Configuring F5 LTM for Load Balancing Cisco Identity Service Engine (ISE)

Craig Hyps

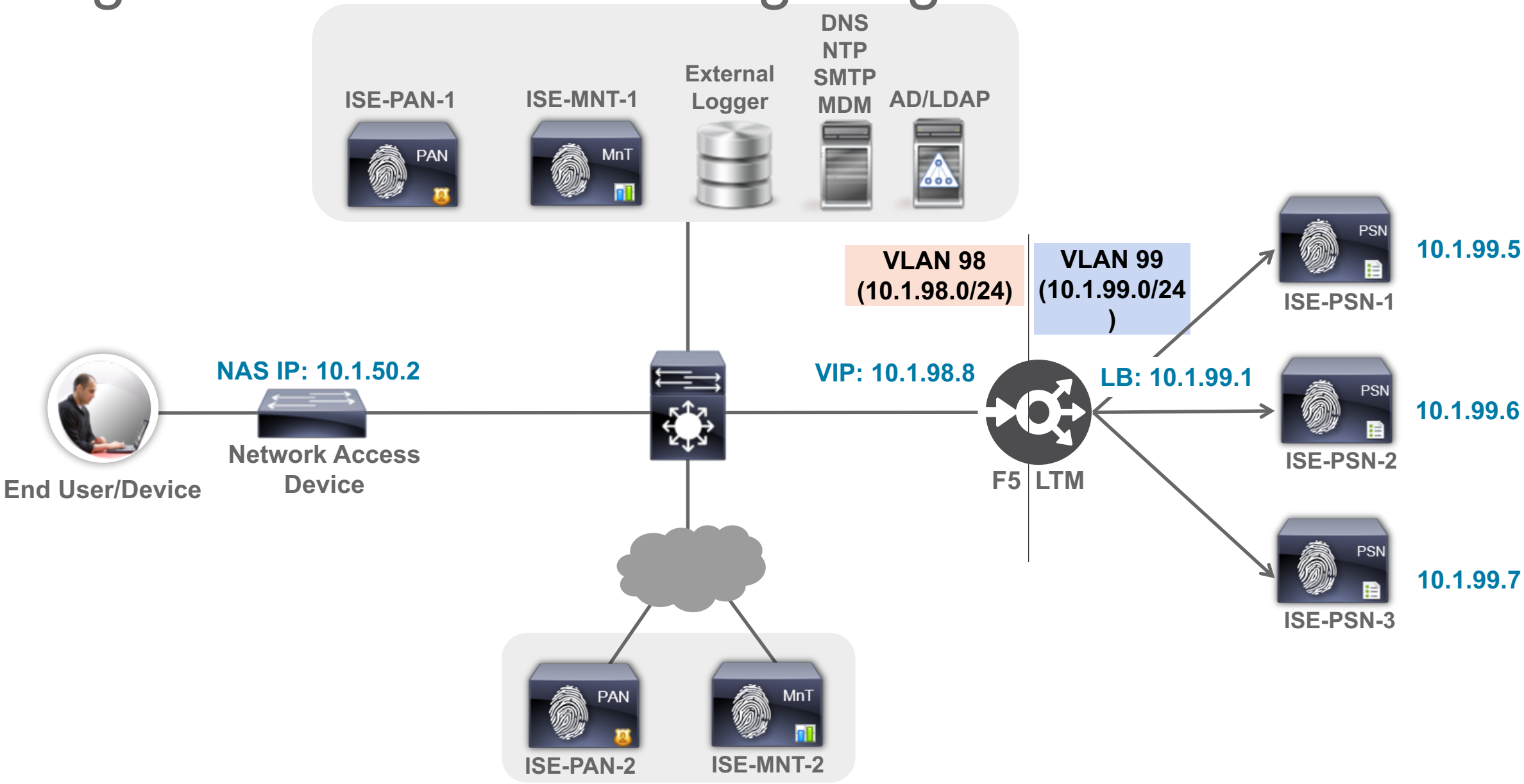
Principal Technical Marketing Engineer, Cisco Systems



- **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

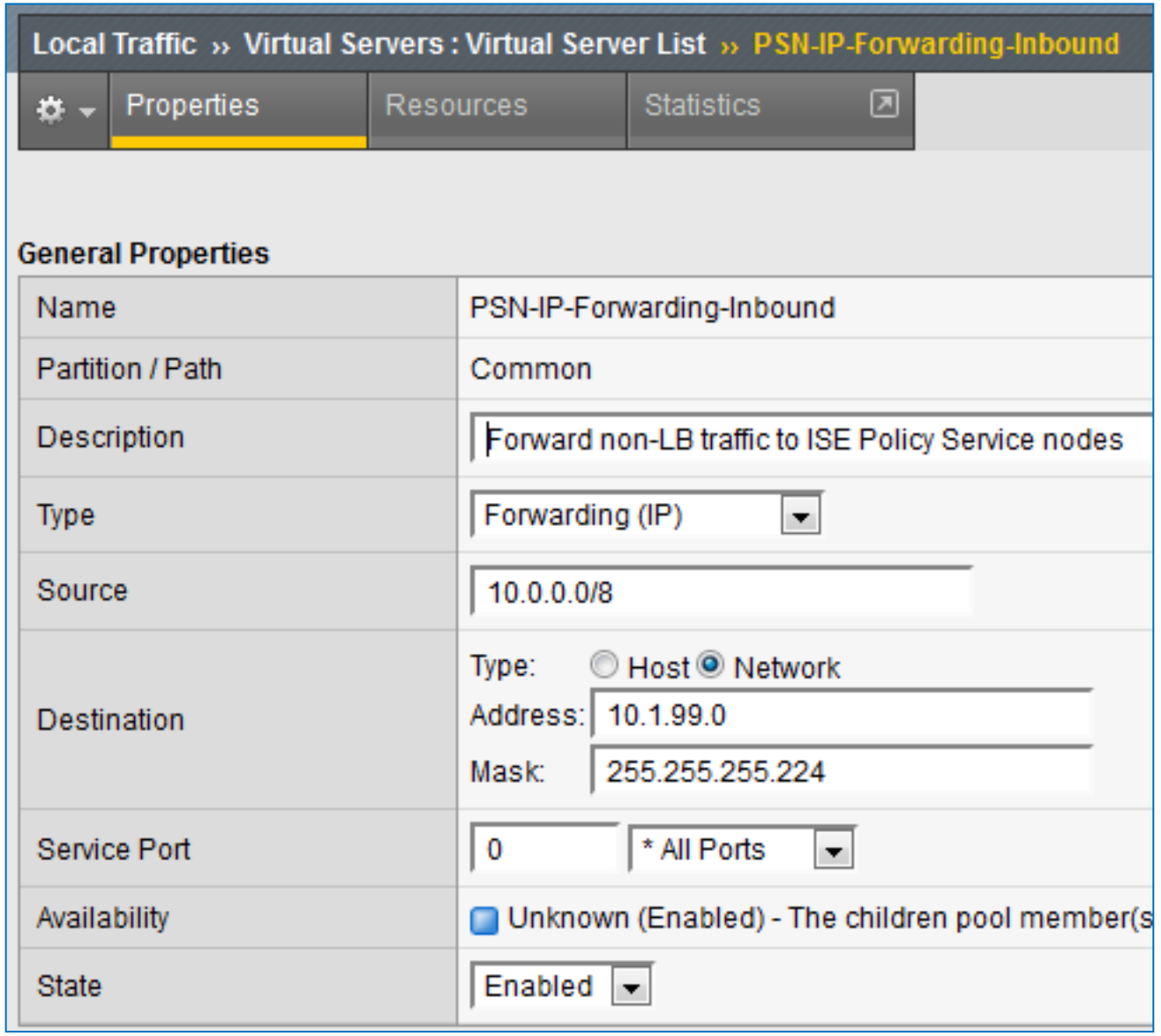
Inter-node/Management/Repository/ID Stores/Feeds/Profiling/Redirected Web/RADIUS CoA

- 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

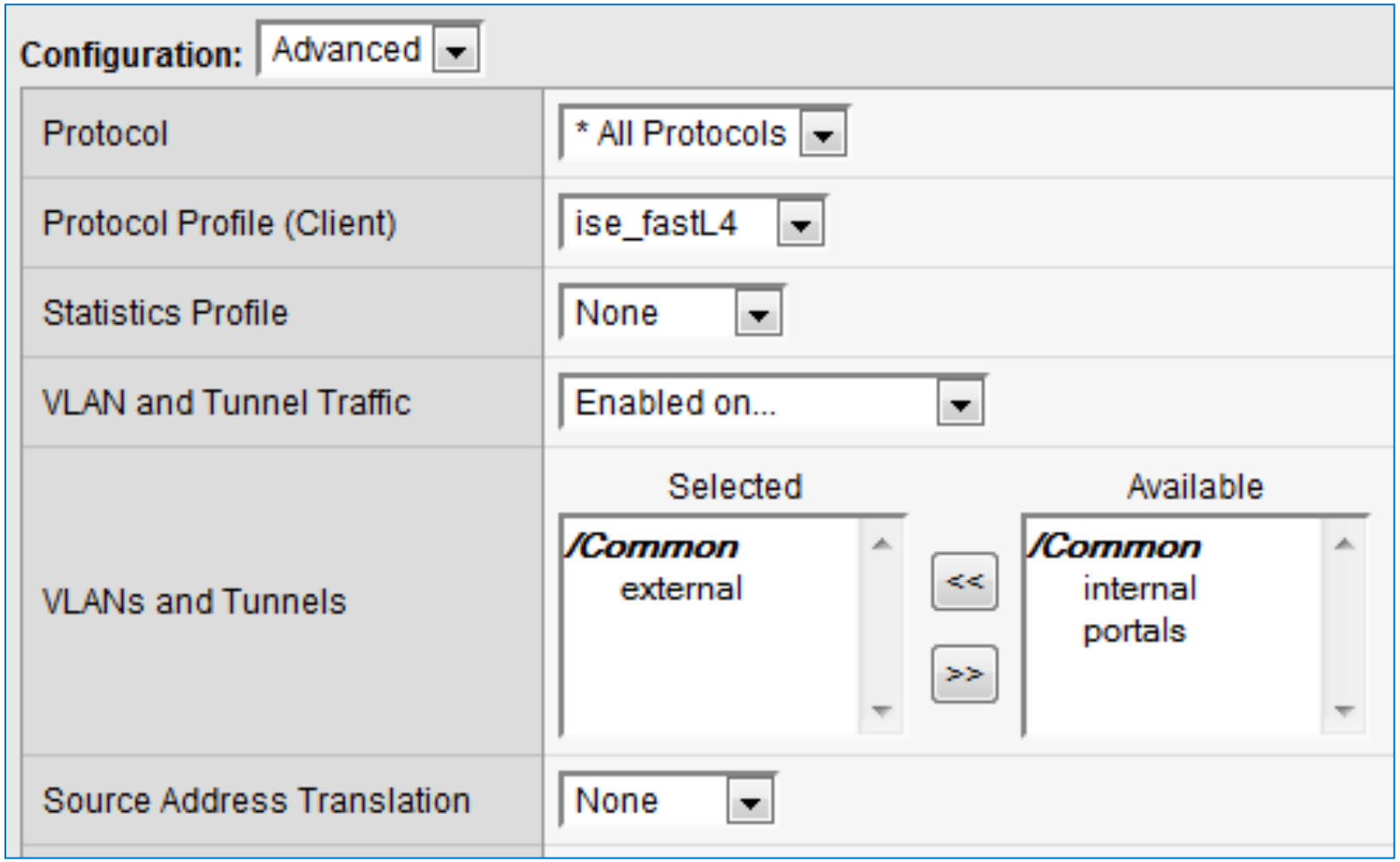
- **Applies to connections initiated from outside (external) network**
- Type = Forwarding (IP)
- Source = All traffic (0.0.0.0/0) or limit to specific network.
- Destination = PSN Network Addresses
- Service Port = 0 (All Ports)
- Availability = Unknown (No service validation via health monitors)



Virtual Server to Forward General Inbound IP Traffic

Configuration (Advanced)

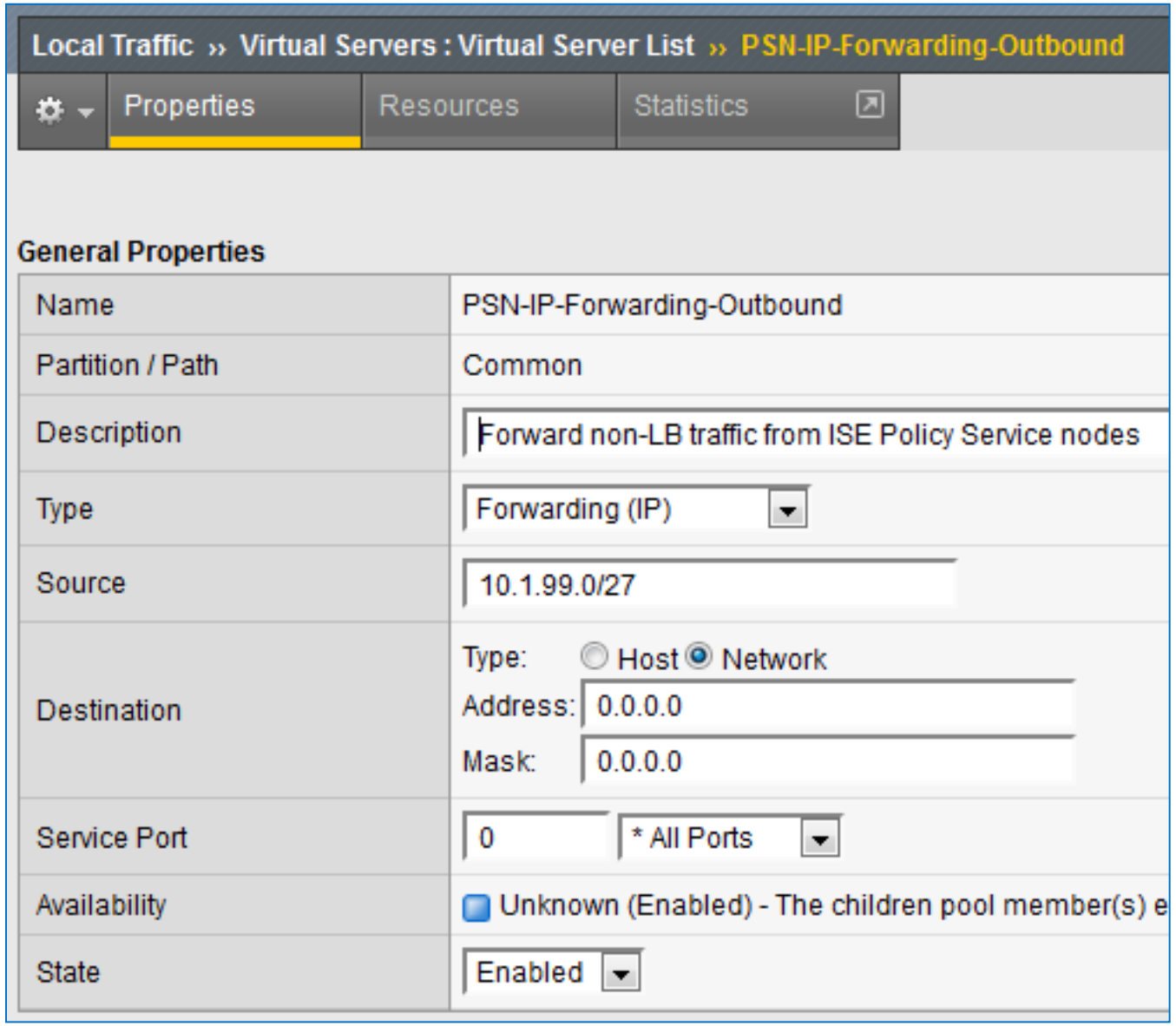
- Protocol = All Protocols
- Protocol Profile = fastL4
- Optionally limit to specific ingress VLAN(s).
- No SNAT



Virtual Server to Forward General Outbound IP Traffic

General Properties

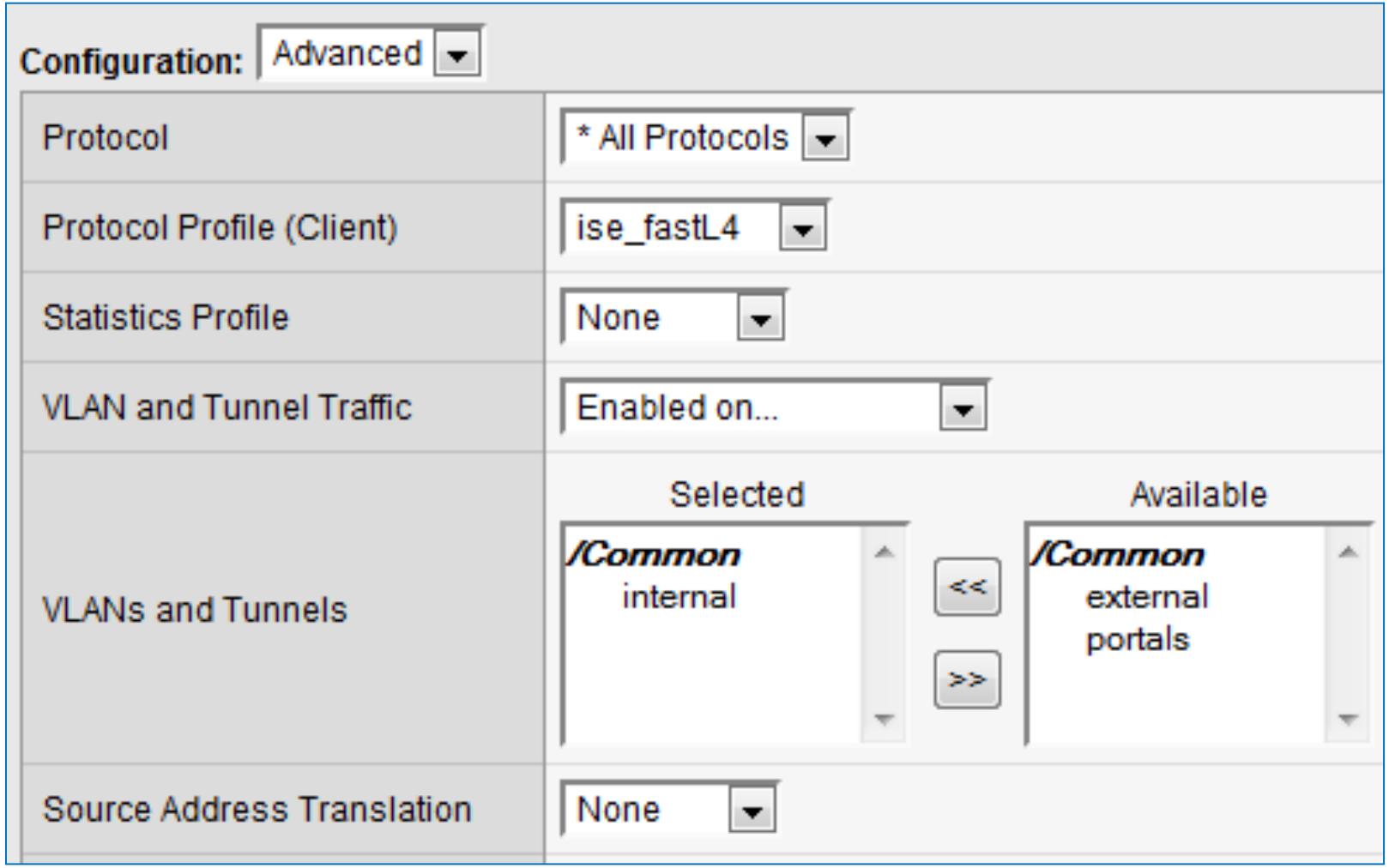
- **Applies to connections initiated from PSN (internal) network**
- Type = Forwarding (IP)
- Source = PSN Network Addresses
- Destination = All traffic (0.0.0.0/0.0.0.0) or limit to specific network.
- Service Port = 0 (All Ports)
- Availability = Unknown (No service validation via health monitors)



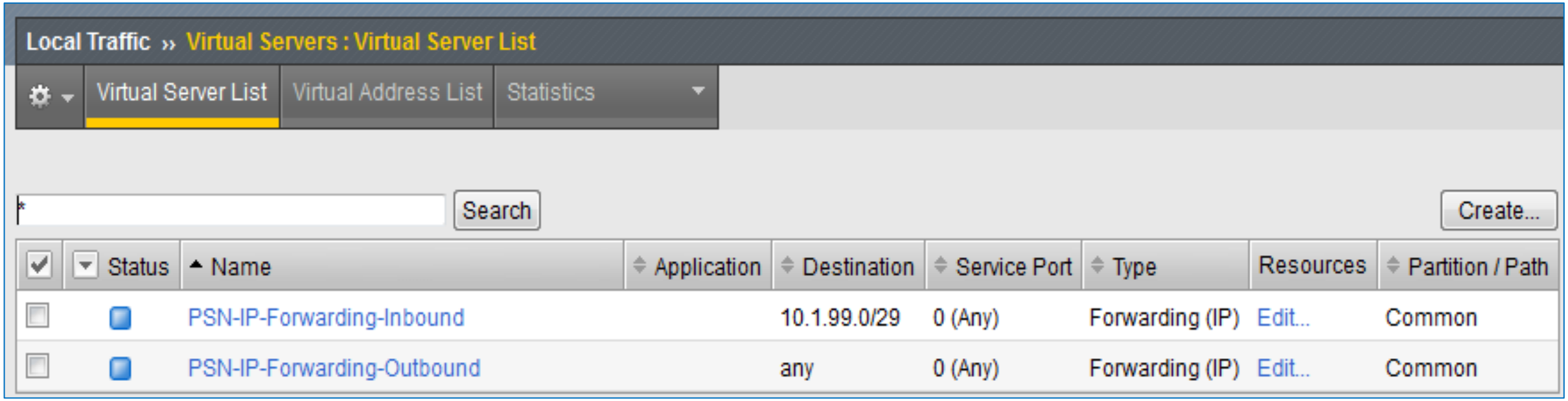
Virtual Server to Forward General Outbound IP Traffic

Configuration (Advanced)

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



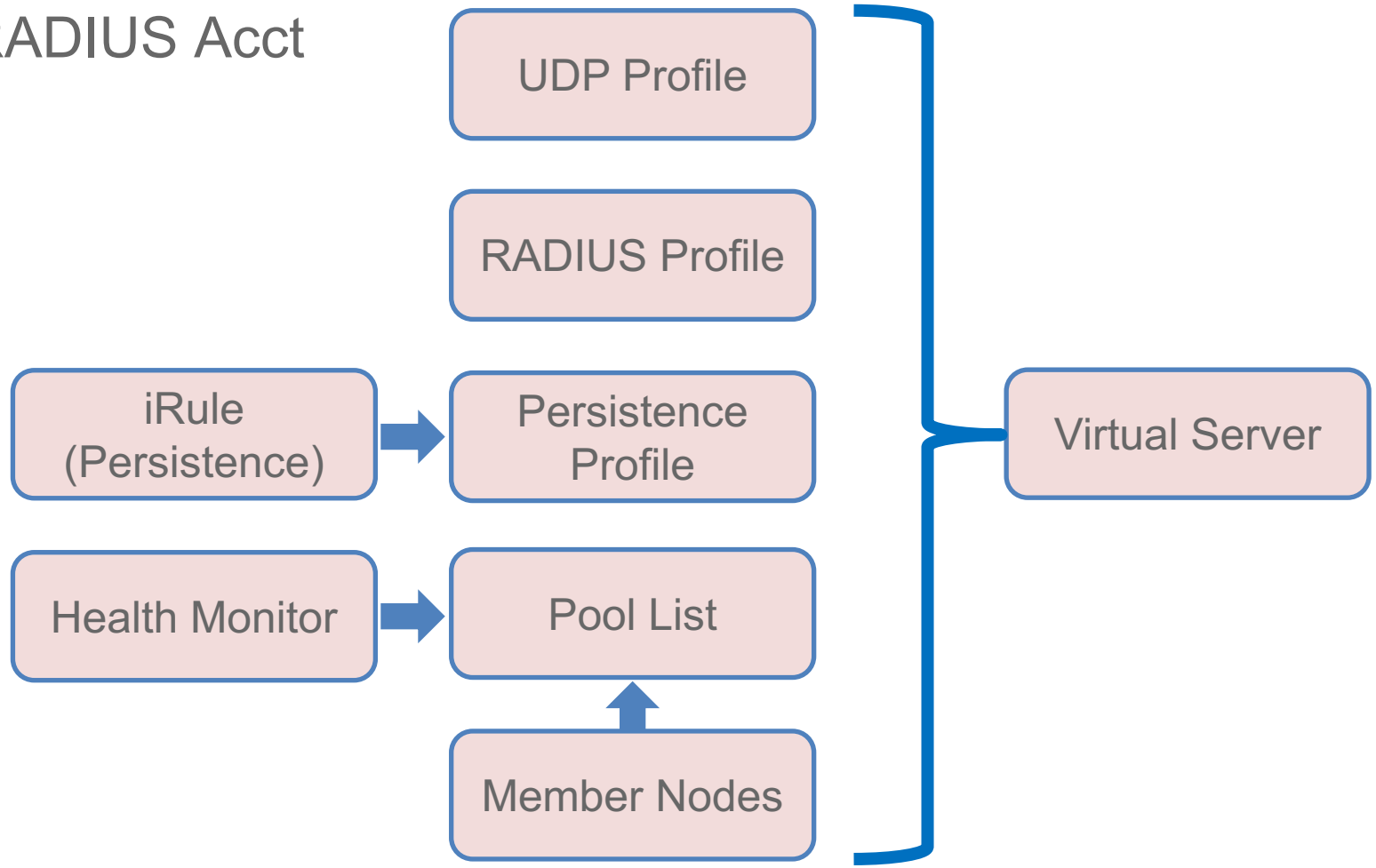
Example Inbound / Outbound IP Forwarding Servers



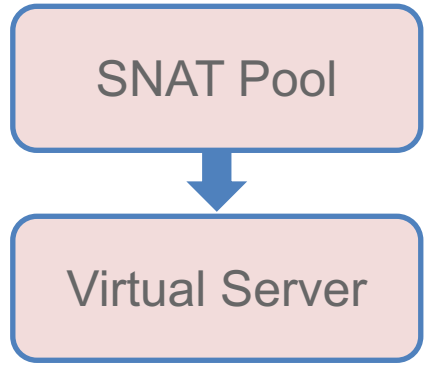
Load Balancing RADIUS

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.

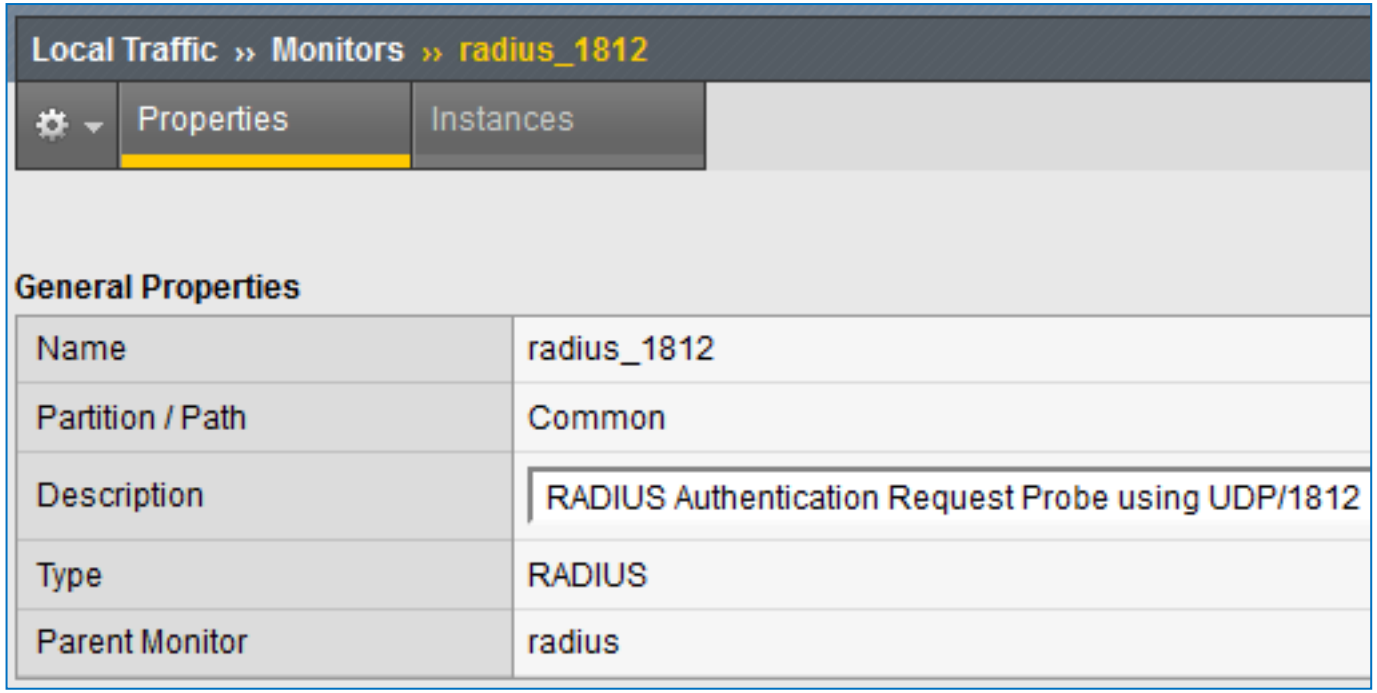
Sample LTM RADIUS Health Monitor Config:

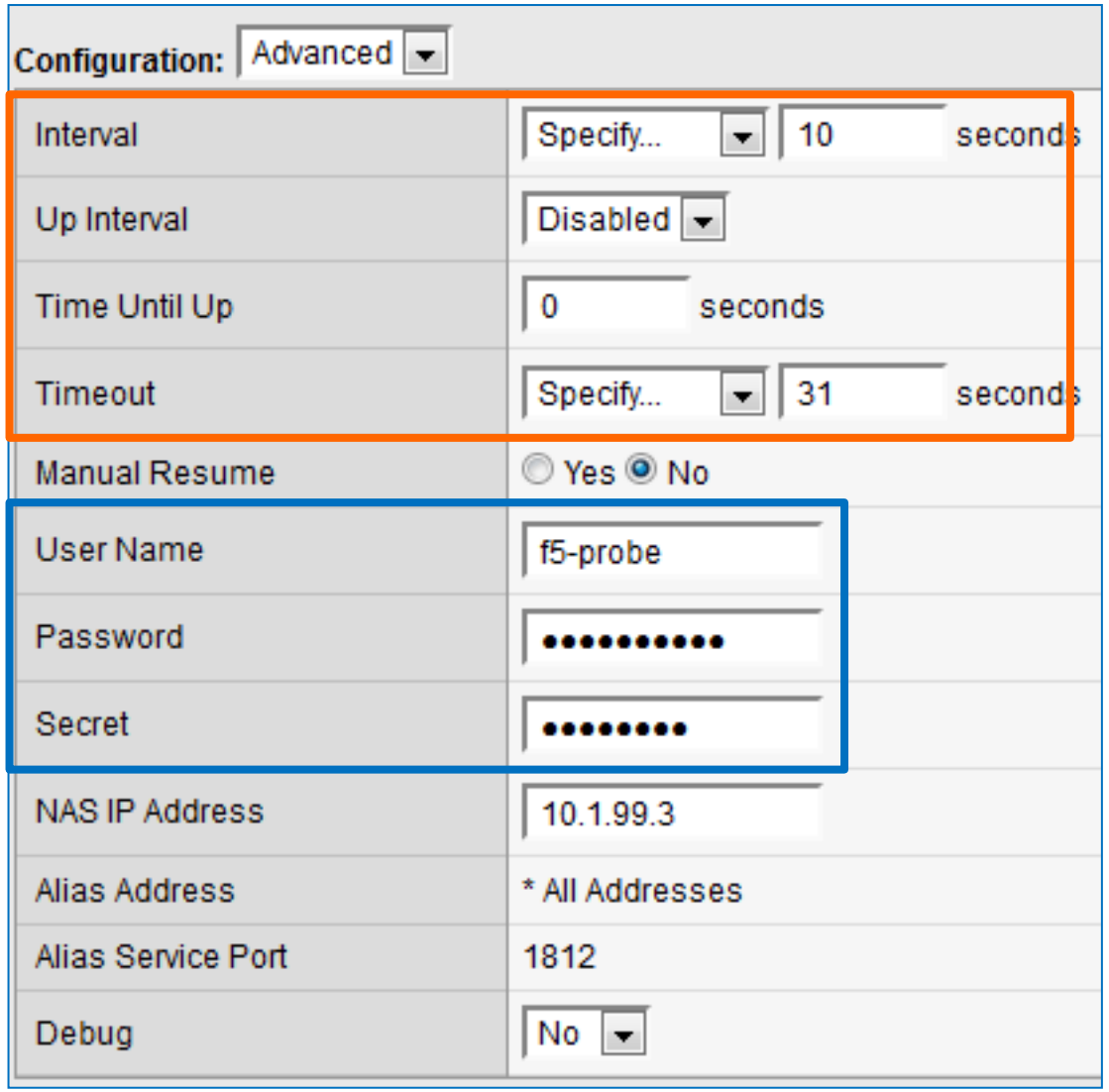
```
ltm monitor radius /Common/radius_1812 {
    debug no
    defaults-from /Common/radius
    destination *:1812
    interval 10
    password P@$$w0rd
    secret P@$$w0rd
    time-until-up 0
    timeout 31
    username f5-probe
}
```

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.

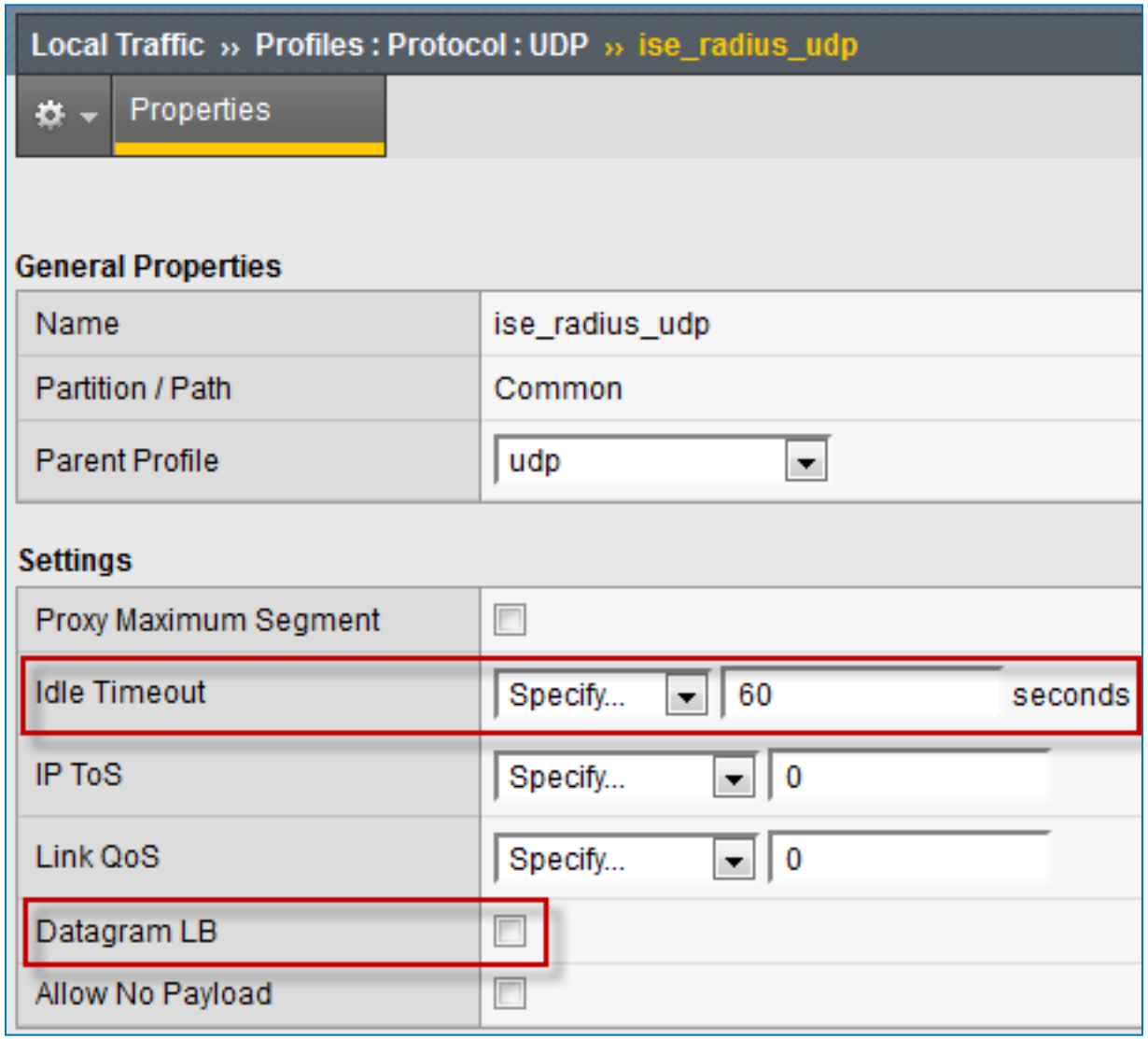




Optional: Configure UDP Profile for RADIUS

Local Traffic > Profiles > Protocol > UDP

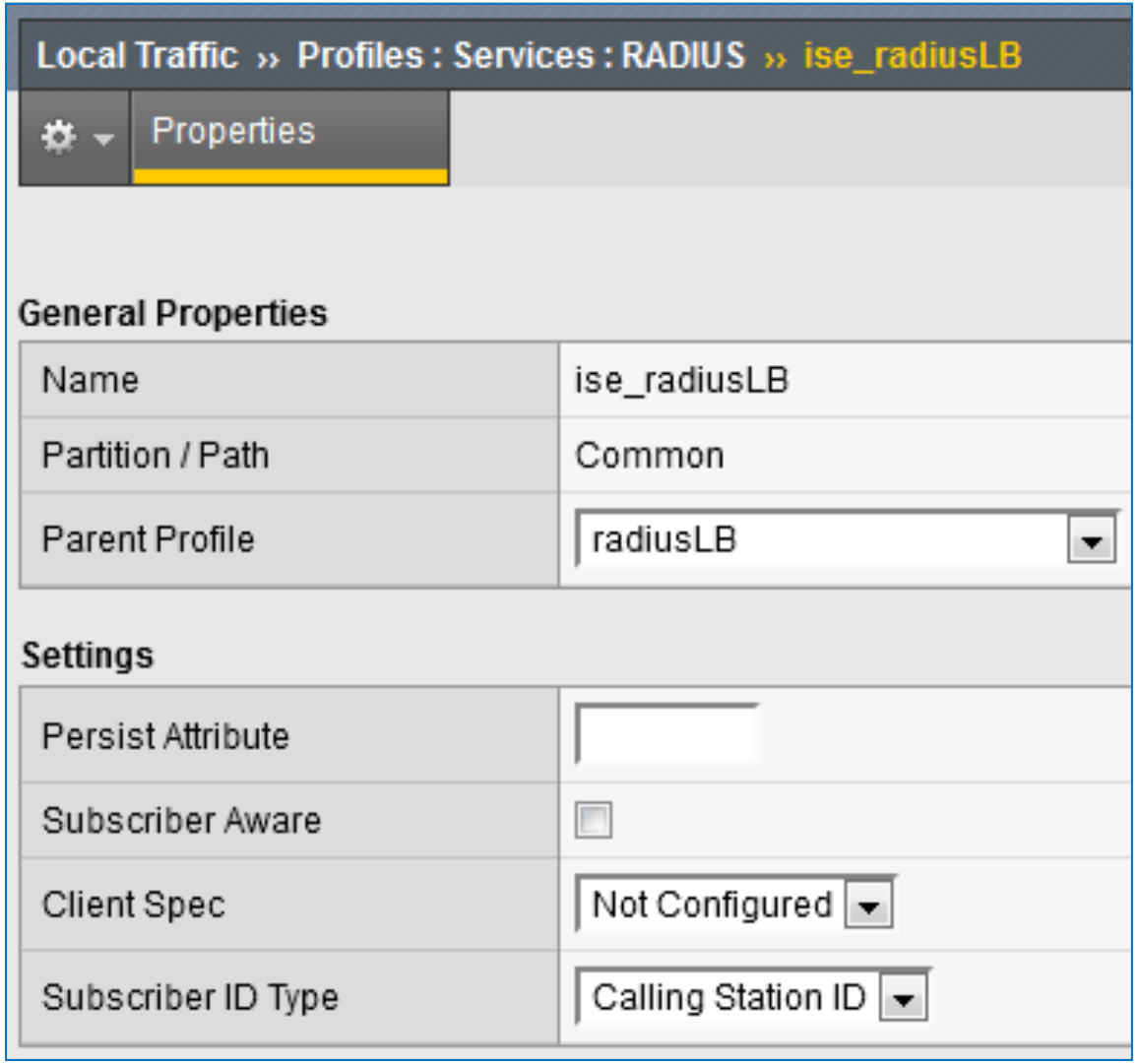
- Start with default Idle Timeout
- Using a custom profile allows for tuning later if needed without impacting other services based on same parent UDP profile
- Disable Datagram LB



Optional: Configure RADIUS Profile

Local Traffic > Profiles > Services > RADIUS

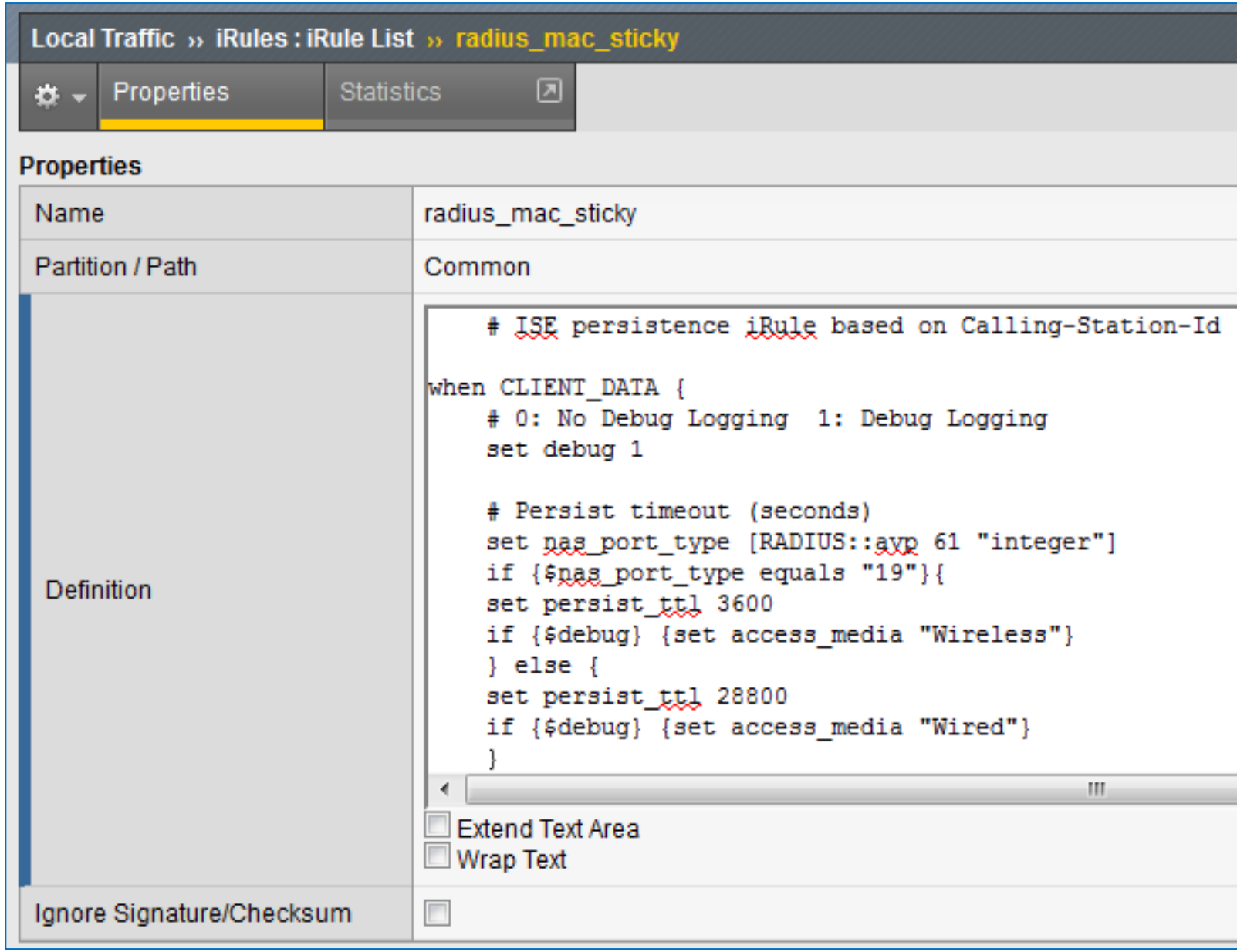
- Start with default settings
- Using a custom profile allows for tuning later if needed without impacting other services based on same parent radiusLB profile



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.

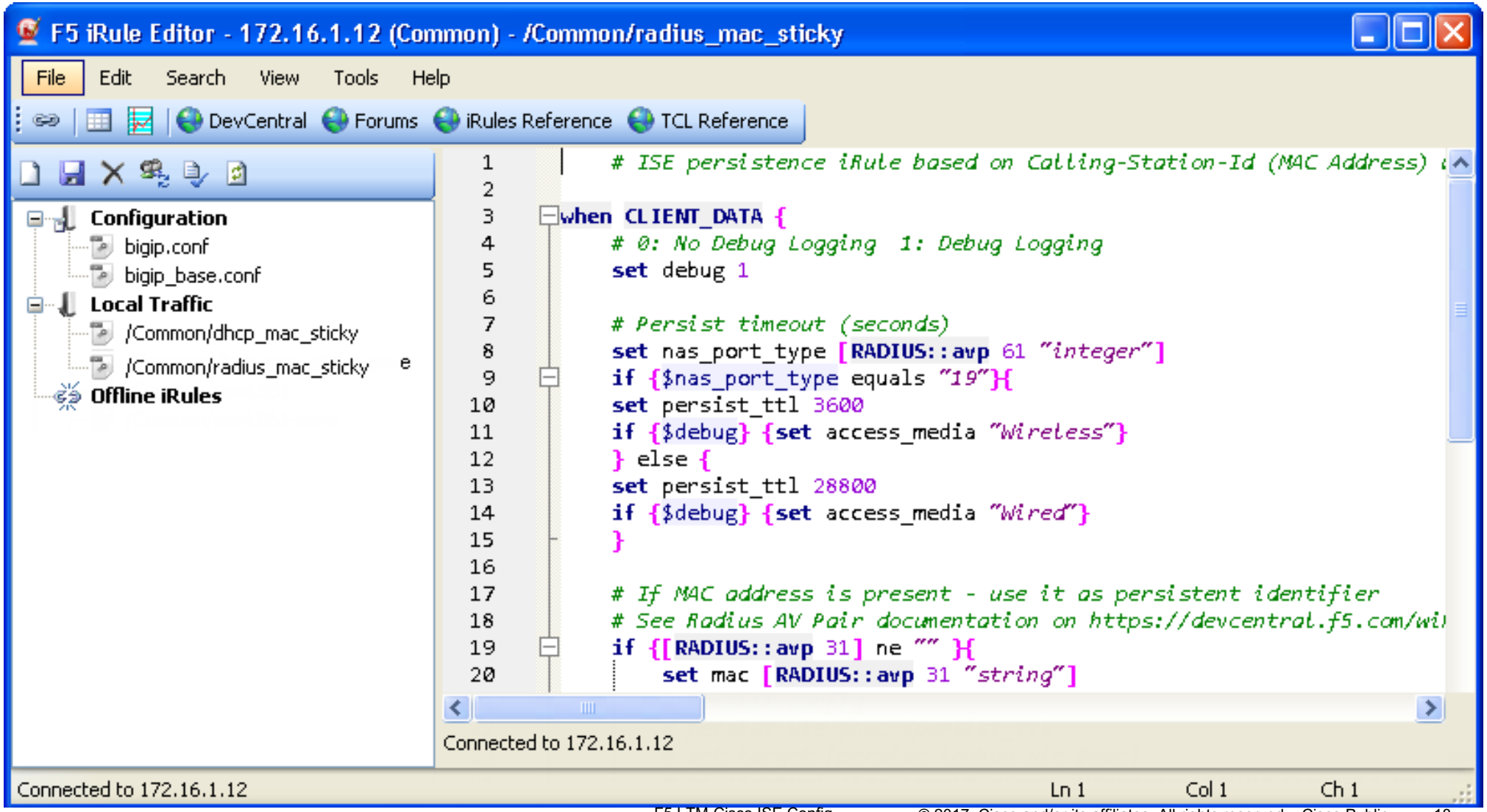


F5 iRule Editor

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

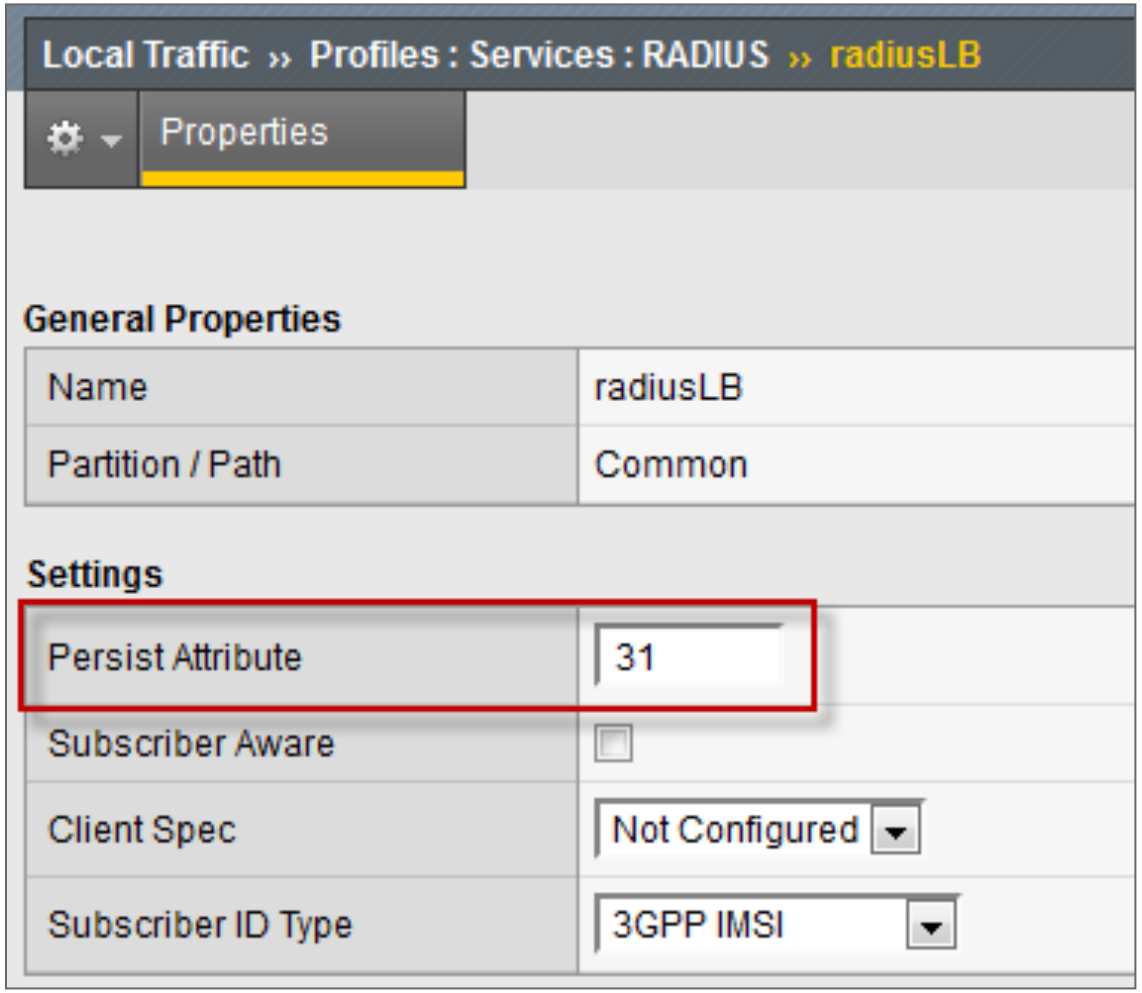


Configuring RADIUS Persistence

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
```



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

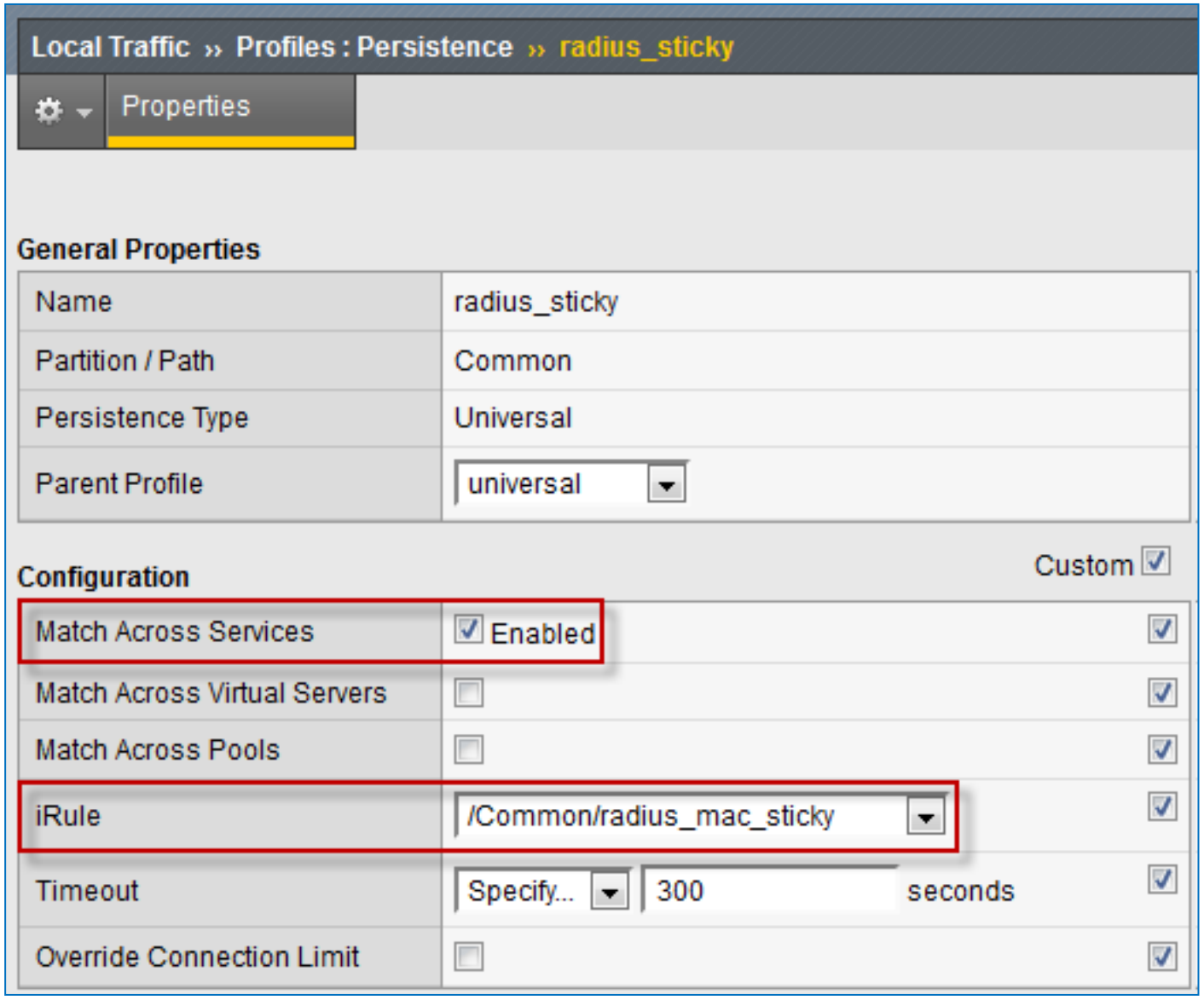
RADIUS Persistence iRule Based on MAC (cont.)

```
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

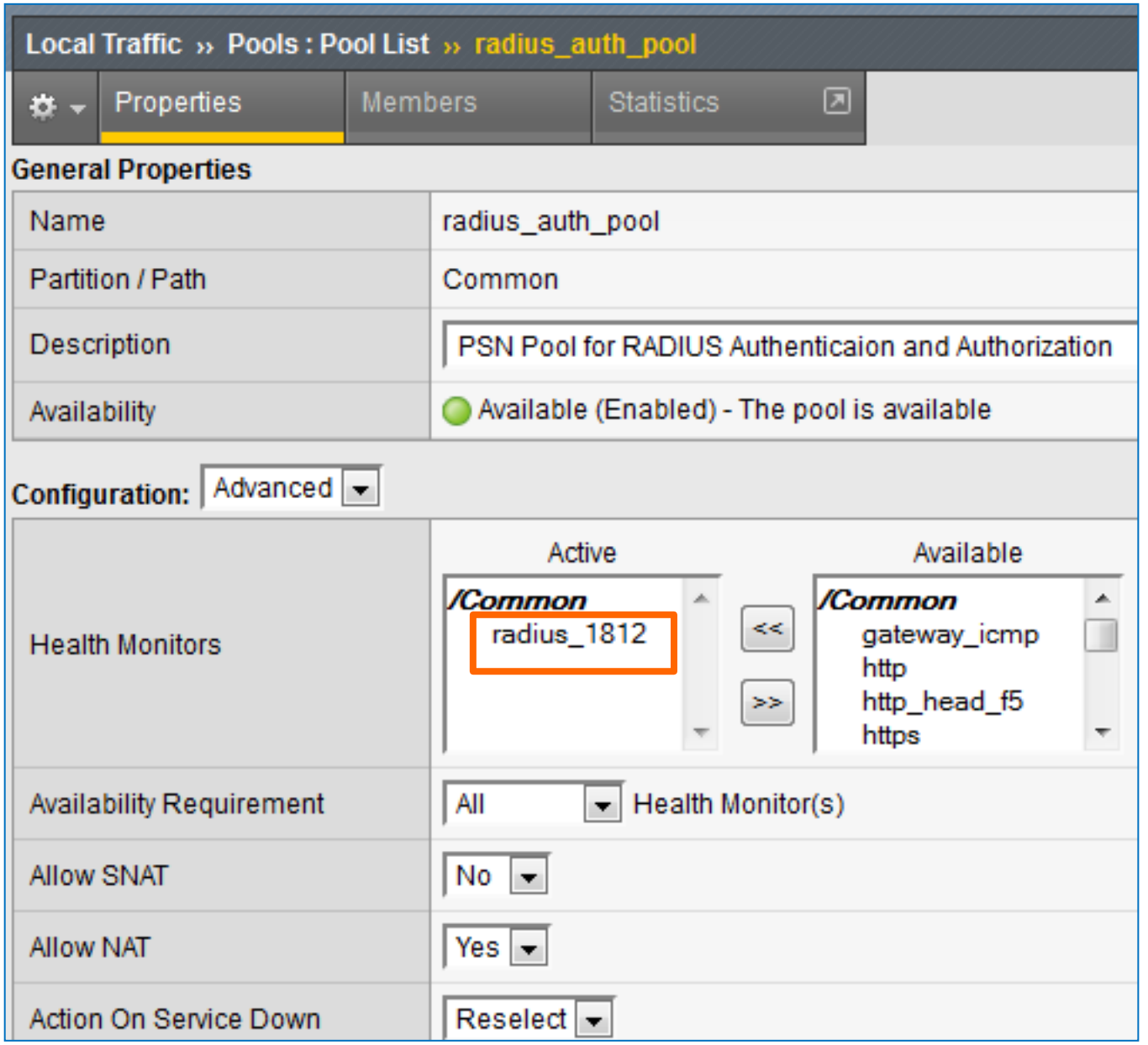
- Enable **Match Across Services**
- If different Virtual Server IP addresses used for RADIUS Auth and Accounting, then enable Match Across Virtual Servers (not recommended)
- Specify RADIUS Persistence iRule
- iRule persistence timer overrides profile setting.



Configure Server Pool for RADIUS Auth

Local Traffic > Pools > Pool List

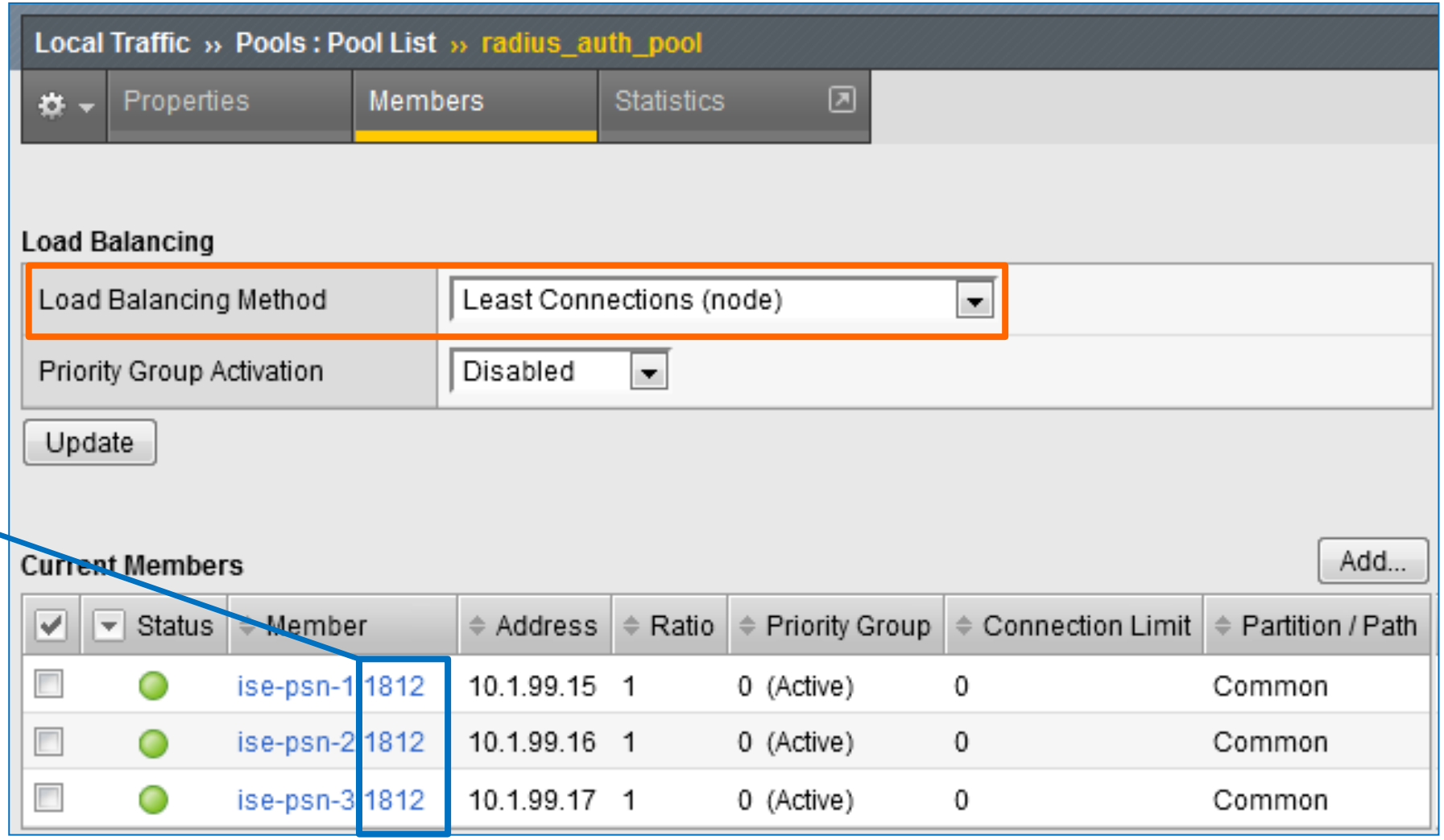
- Health Monitor = RADIUS Monitor
- SNAT = No
- Action on Service Down = Reselect
  - Ensures existing connections are moved to an alternate server.



Configure Member Nodes in RADIUS Auth Pool

Local Traffic > Pools > Pool List > Members

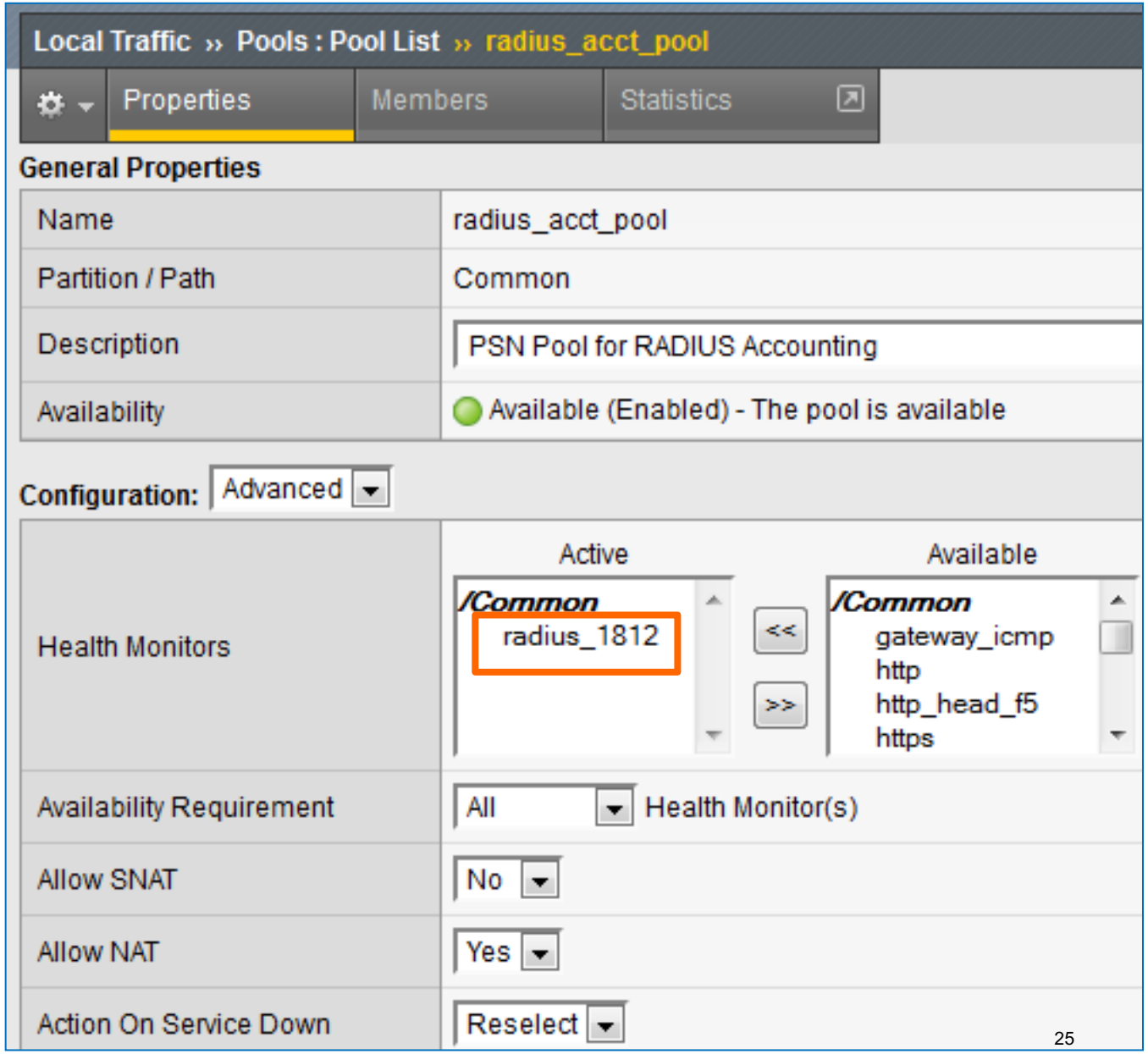
- Load Balancing Method options:
  - Least Connections (node)
  - Least Connections (member)
- Server Port: 1812 or 1645



Configure Server Pool for RADIUS Accounting

Local Traffic > Pools > Pool List

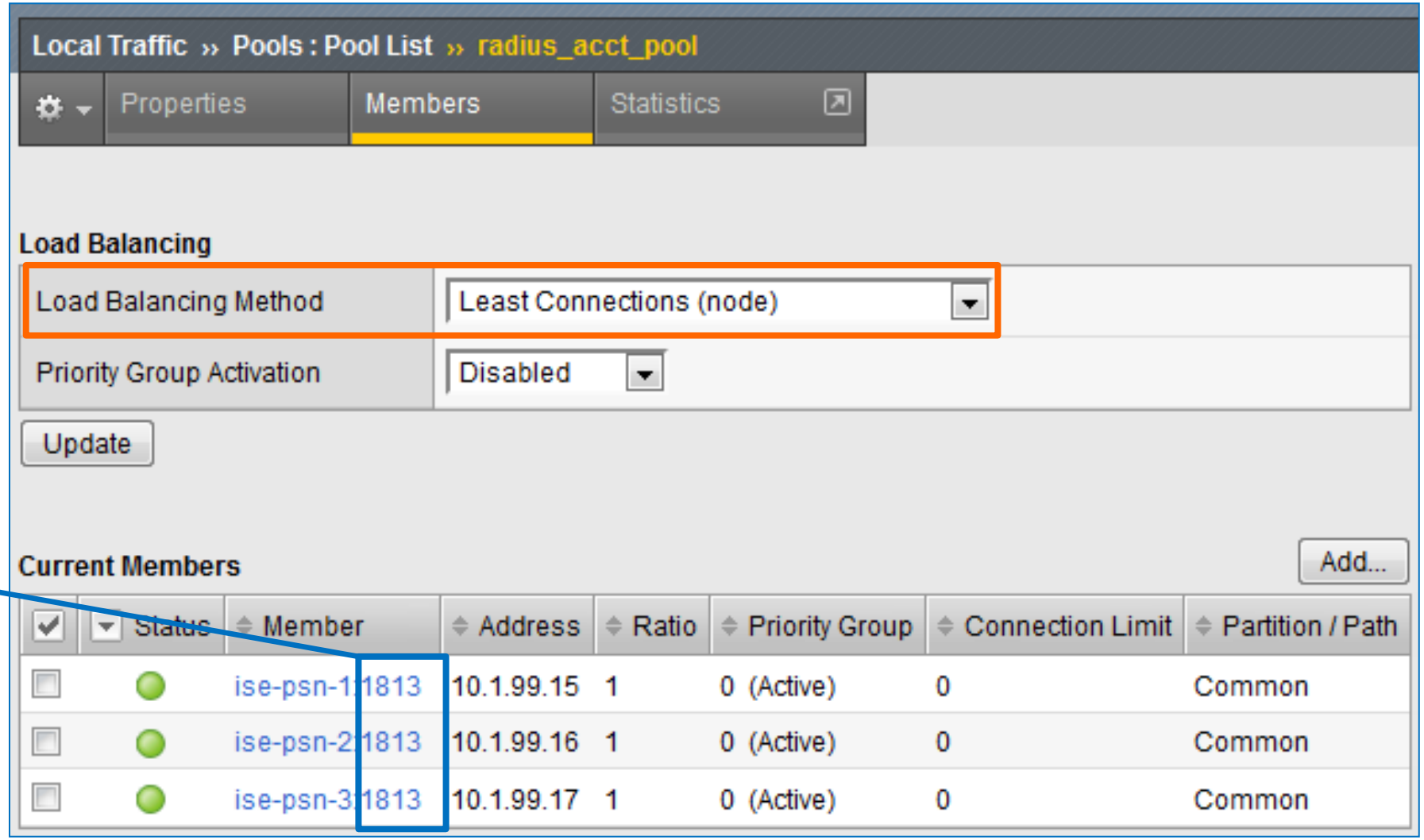
- Health Monitor = RADIUS Monitor (same monitor used for RADIUS Auth)
- SNAT = No
- Action on Service Down = Reselect
  - Ensures existing connections are moved to an alternate server.



Configure Member Nodes in RADIUS Accounting Pool

Local Traffic > Pools > Pool List > Members

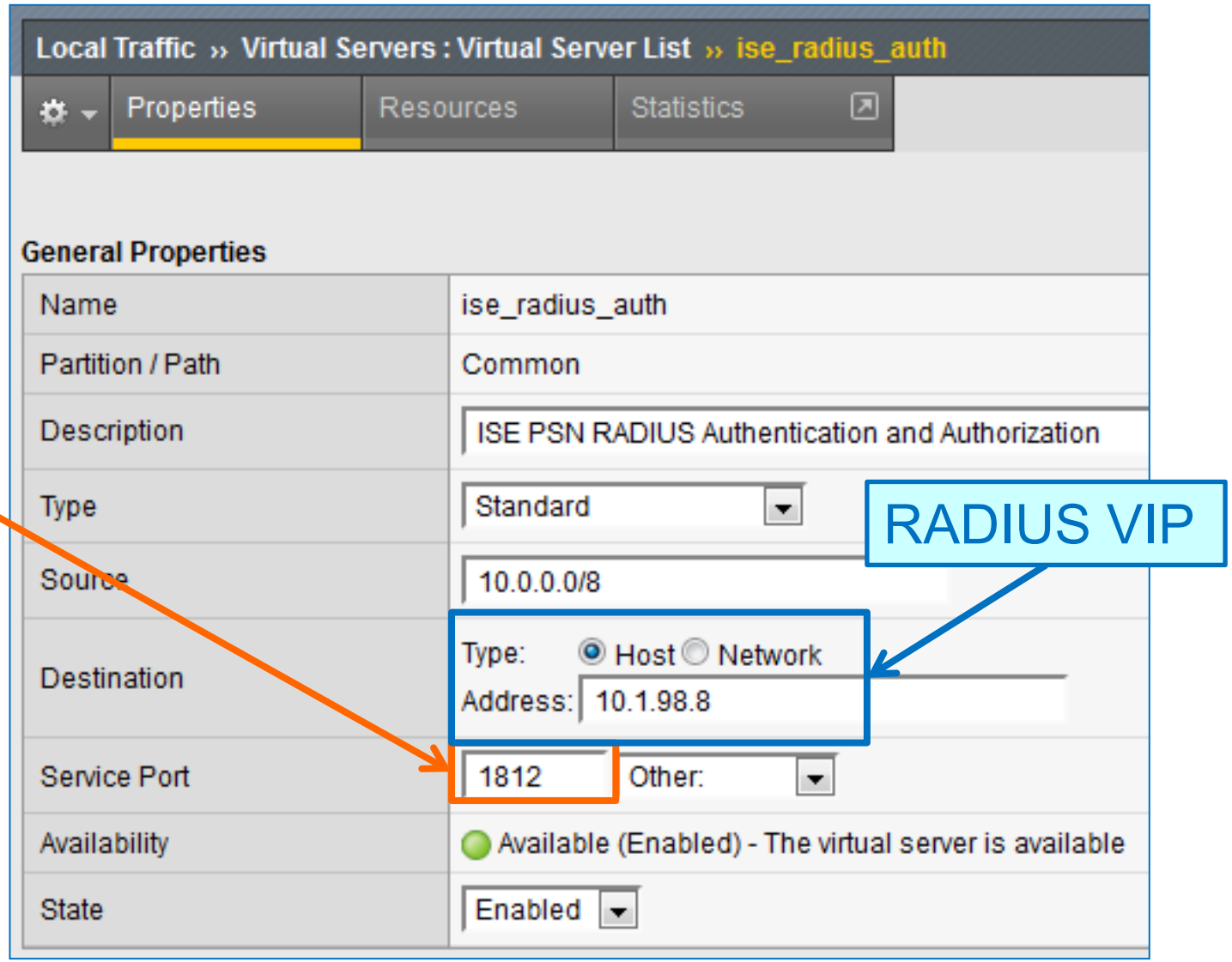
- Load Balancing Method options:
  - Least Connections (node)
  - Least Connections (member)
  - Fastest (application)
- Server Port: 1813 or 1646



Configure Virtual Server for RADIUS Auth (Properties)

Local Traffic > Virtual Servers > Virtual Server List

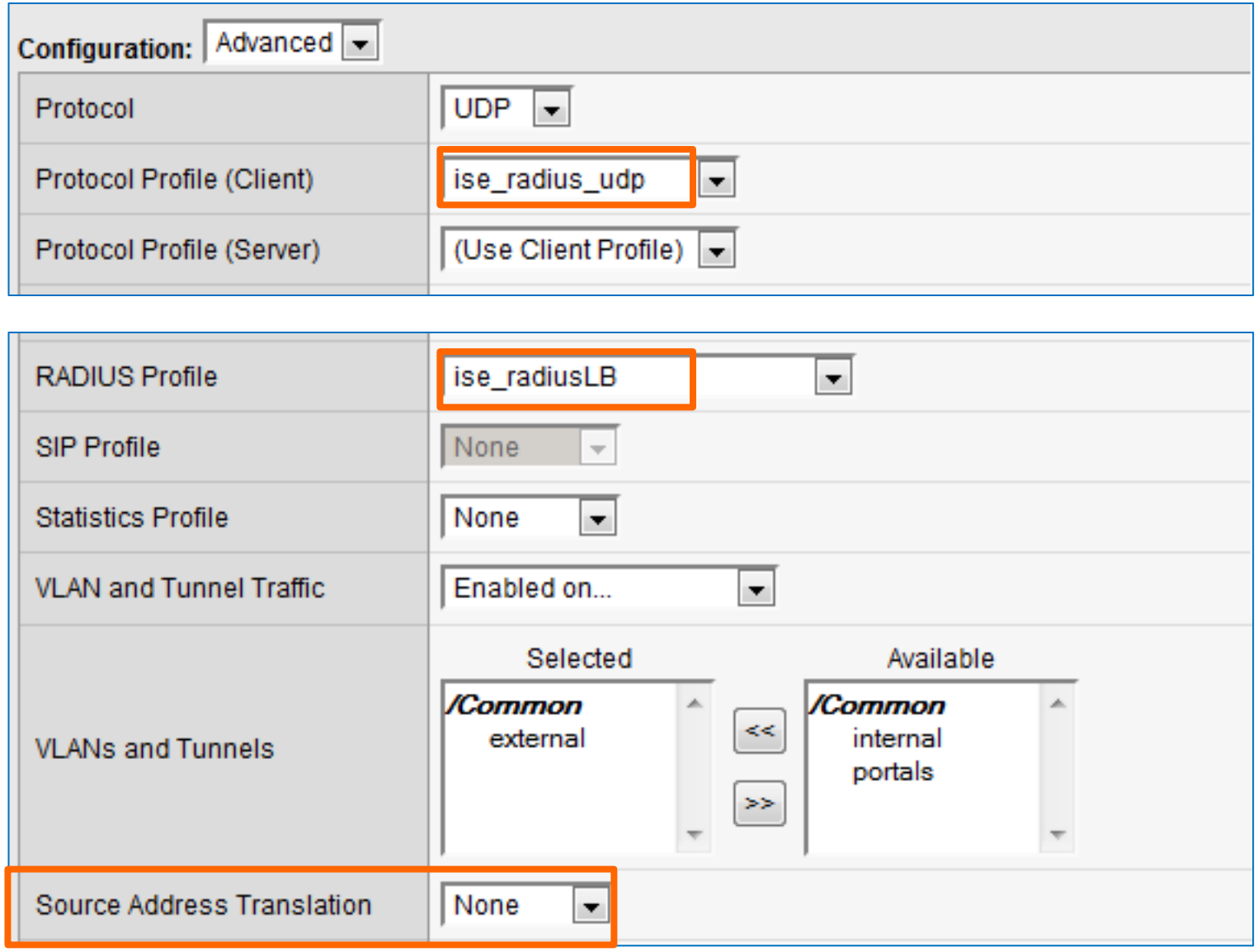
- Type = Standard
- Source = 0.0.0.0/0 (all hosts) or specific network address.
- Destination = RADIUS Virtual IP
- Service Port = 1812 or 1645



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**

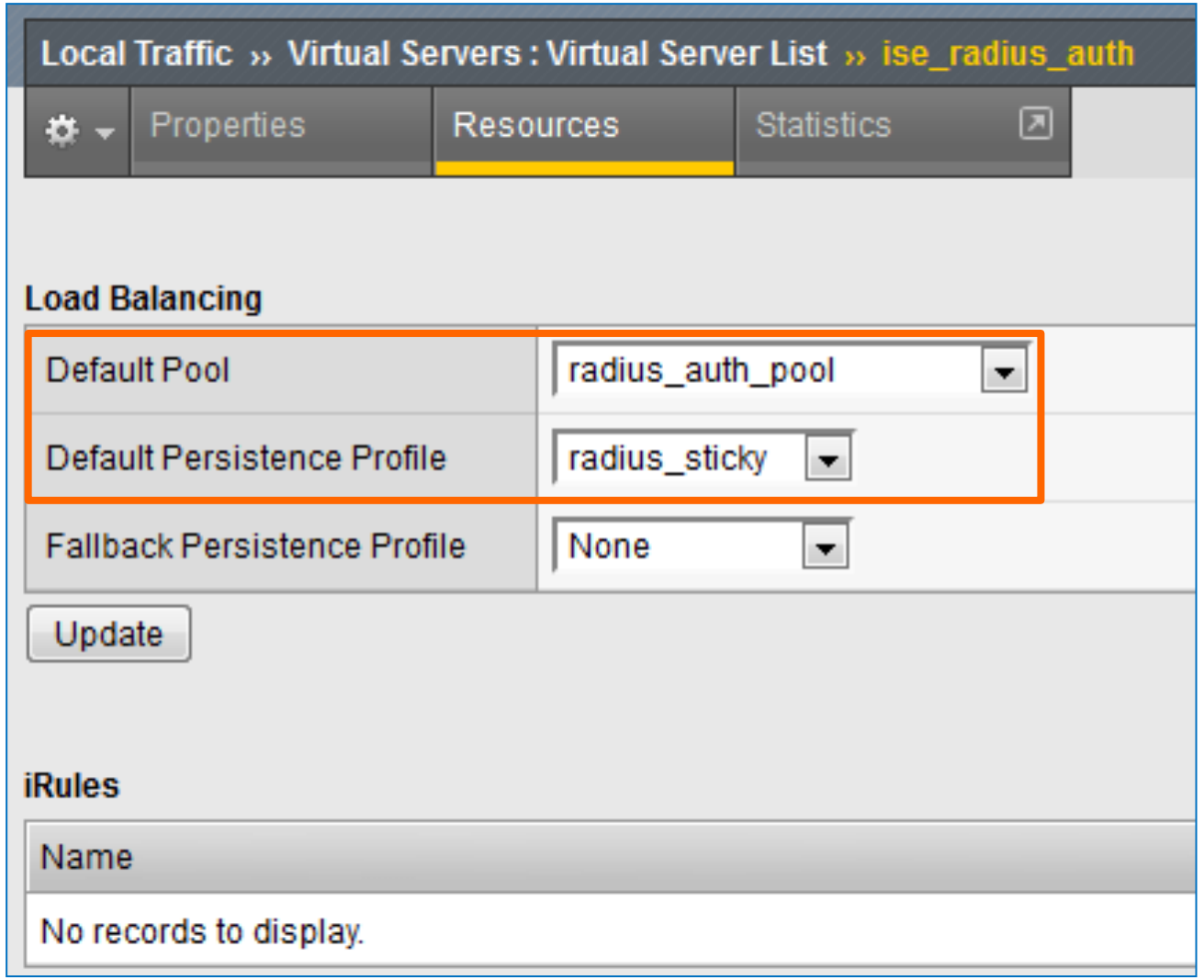


Configure Virtual Server RADIUS Auth (Resources)

Local Traffic > Virtual Servers > Virtual Server List > Resources

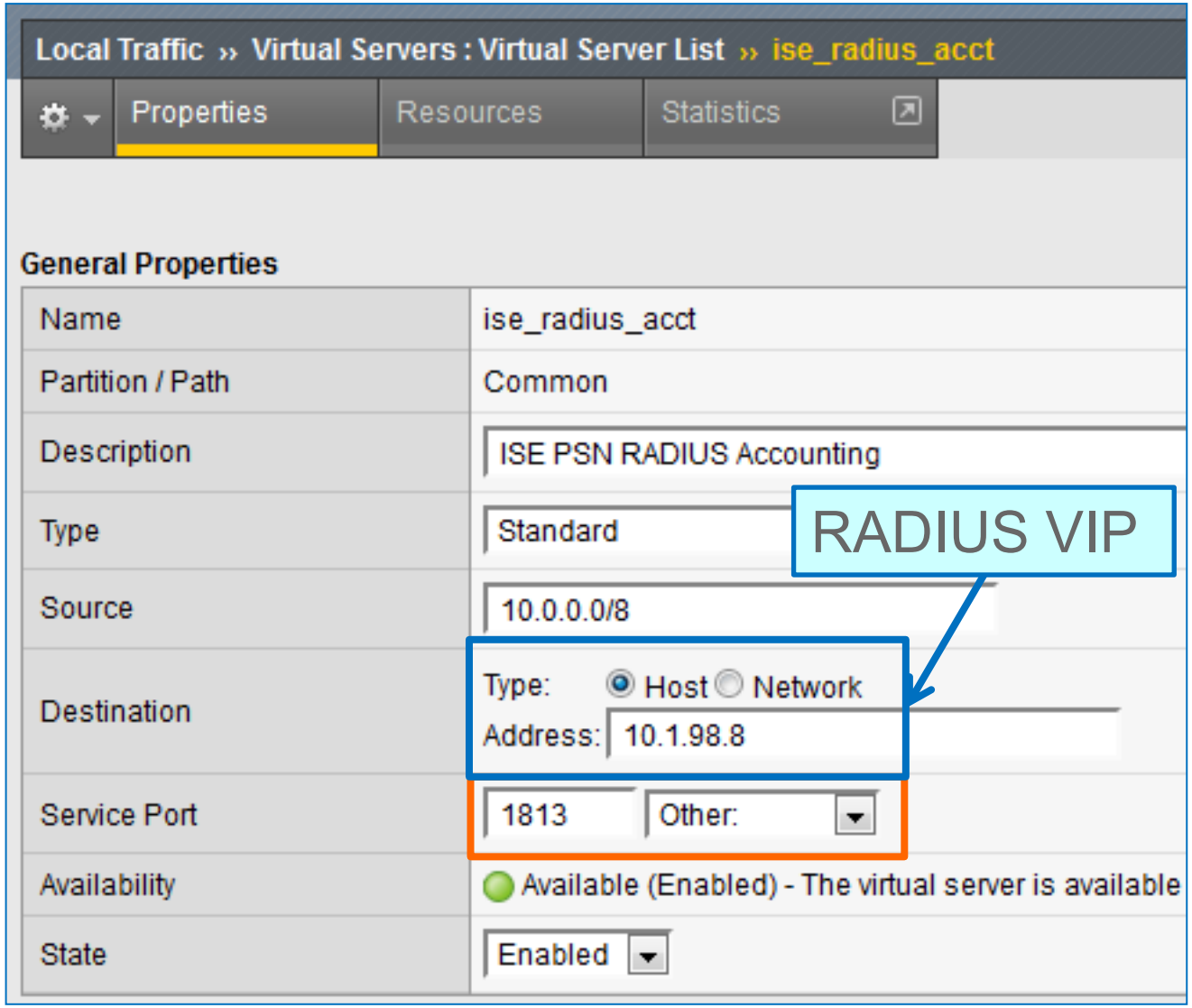
- Default Pool = RADIUS Auth Pool
- Default Persistence Profile = RADIUS persistence profile
- Fallback Persistence Profile:
  - RADIUS iRule setting overrides value set here.
  - If not configured in iRule, set optional value here. Example: **radius_source_addr**

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

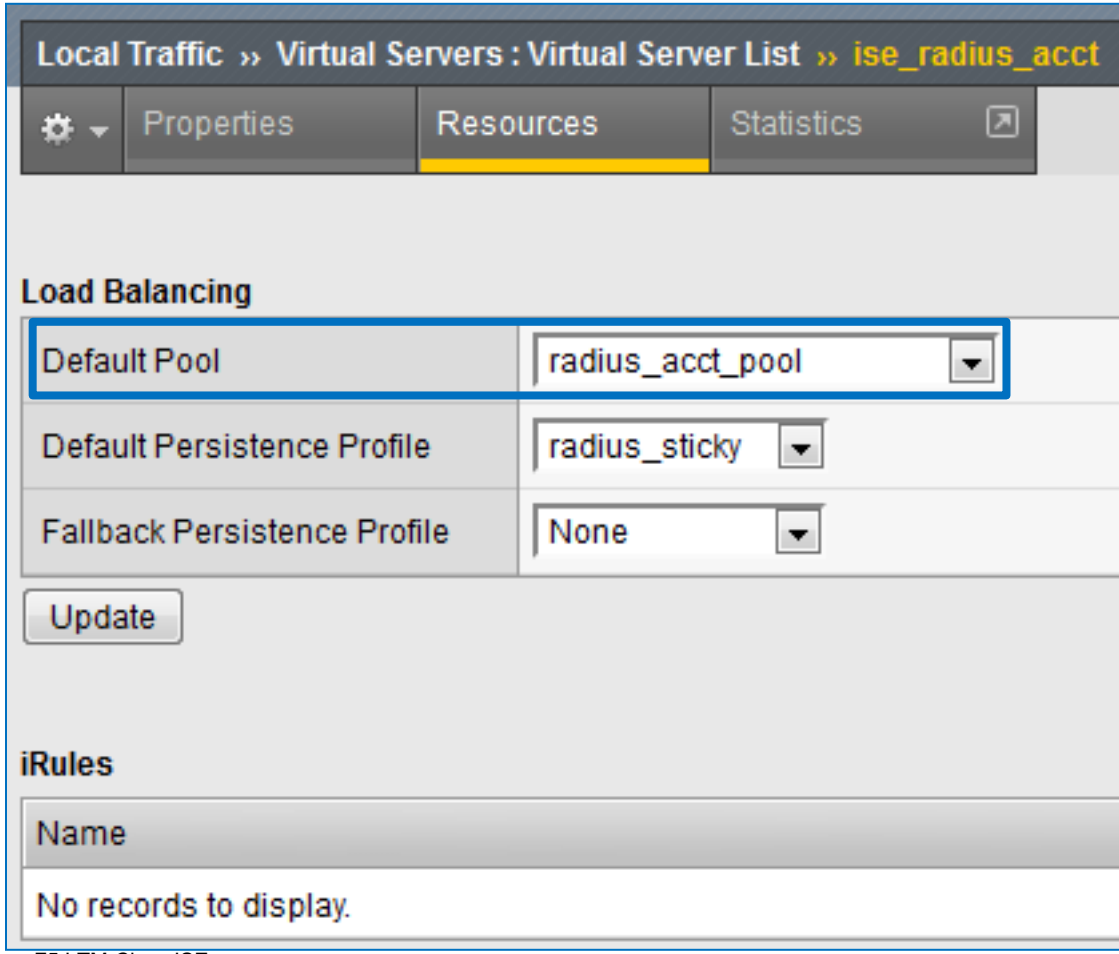


Configure Virtual Server for RADIUS Accounting

Local Traffic > Virtual Servers > Virtual Server List



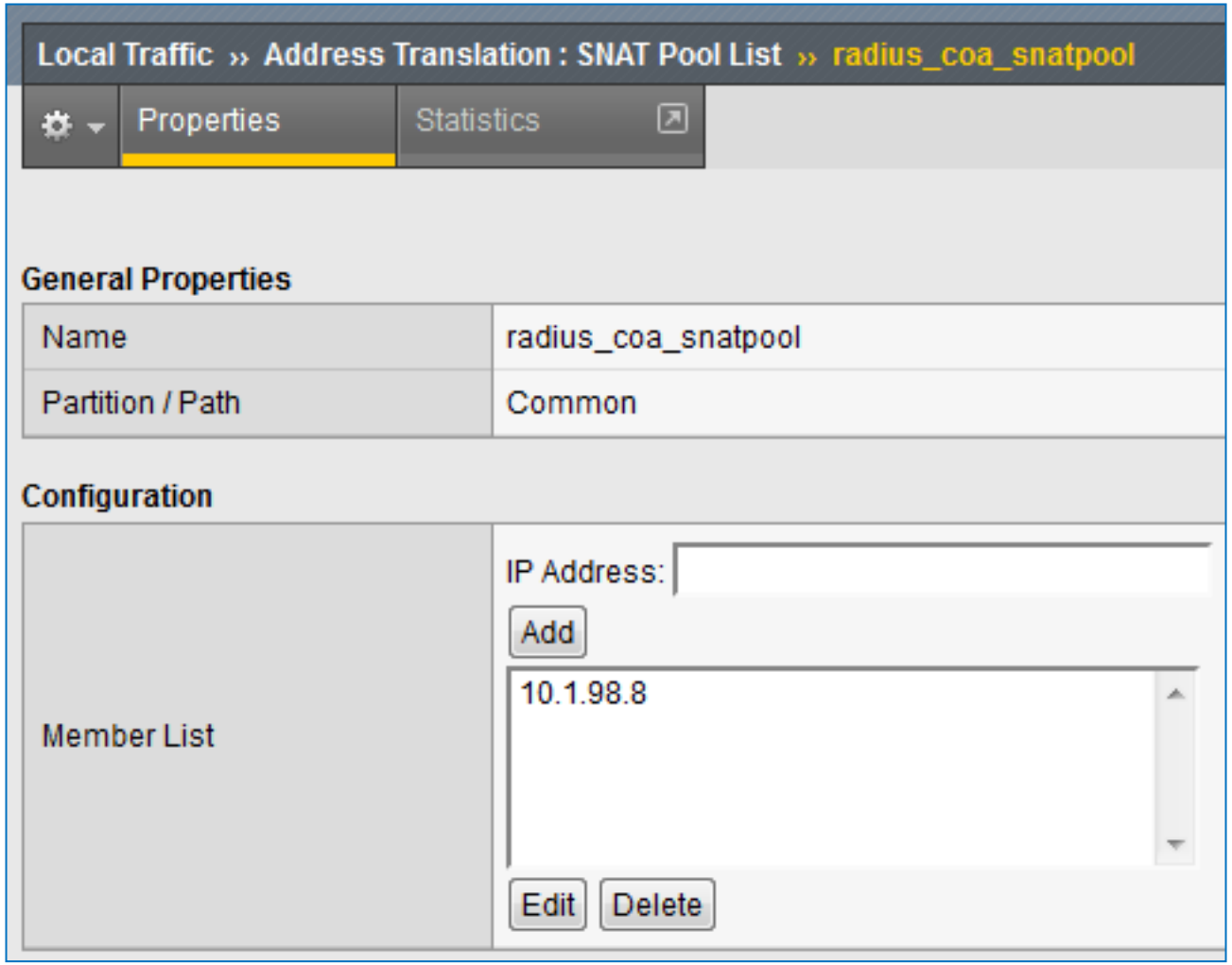
- Same settings as RADIUS Auth Virtual Server but different service port and pool



Configure SNAT Pool List for RADIUS CoA

Local Traffic > Address Translation > SNAT Pool List

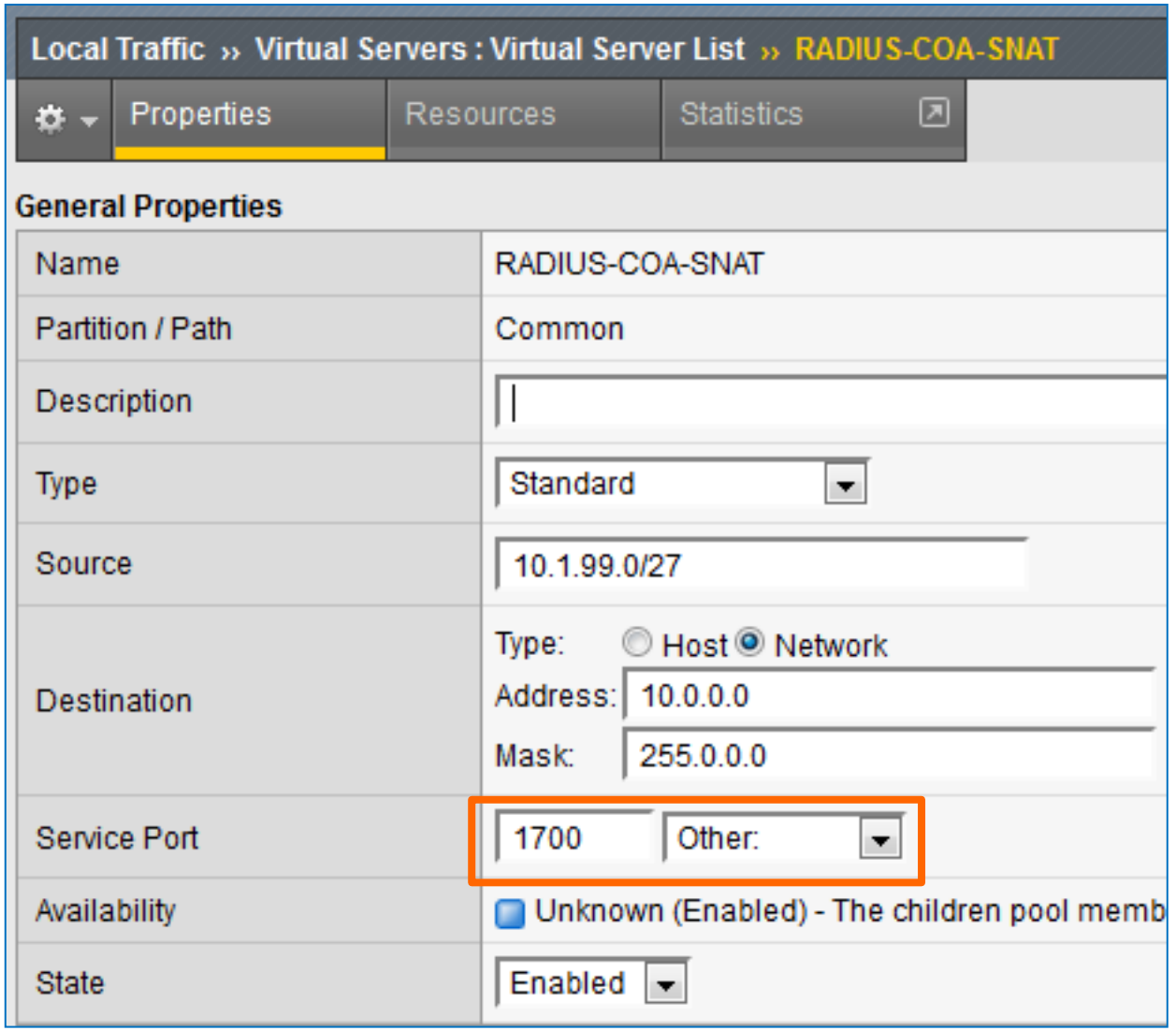
- CoA traffic is initiated by PSN to NADs on UDP/1700
- Define SNAT Pool List with RADIUS Server Virtual IP as a pool member



Configure Virtual Server to SNAT RADIUS CoA (Properties)

Local Traffic > Virtual Servers > Virtual Server List

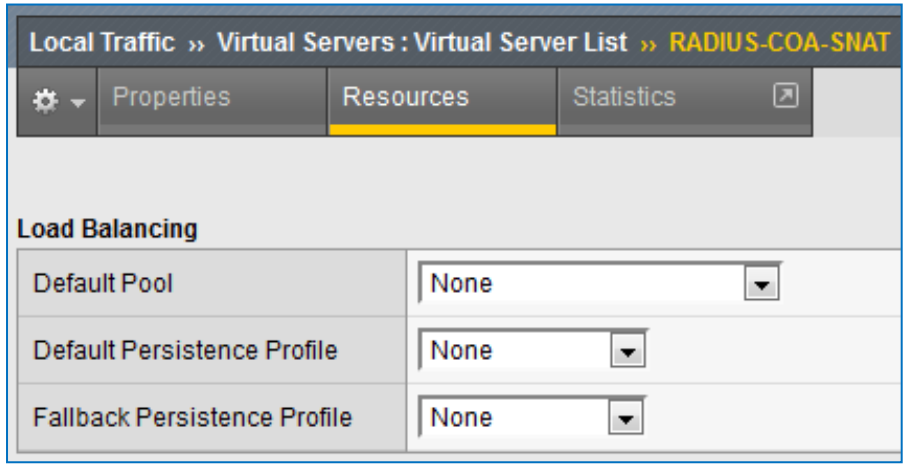
- CoA traffic is initiated by PSN to NADs on UDP/1700
- Type = Standard
- Source = PSN Network
- Destination = 0.0.0.0 / 0.0.0.0 (all hosts) or specific network for all NADs
- Service Port = 1700

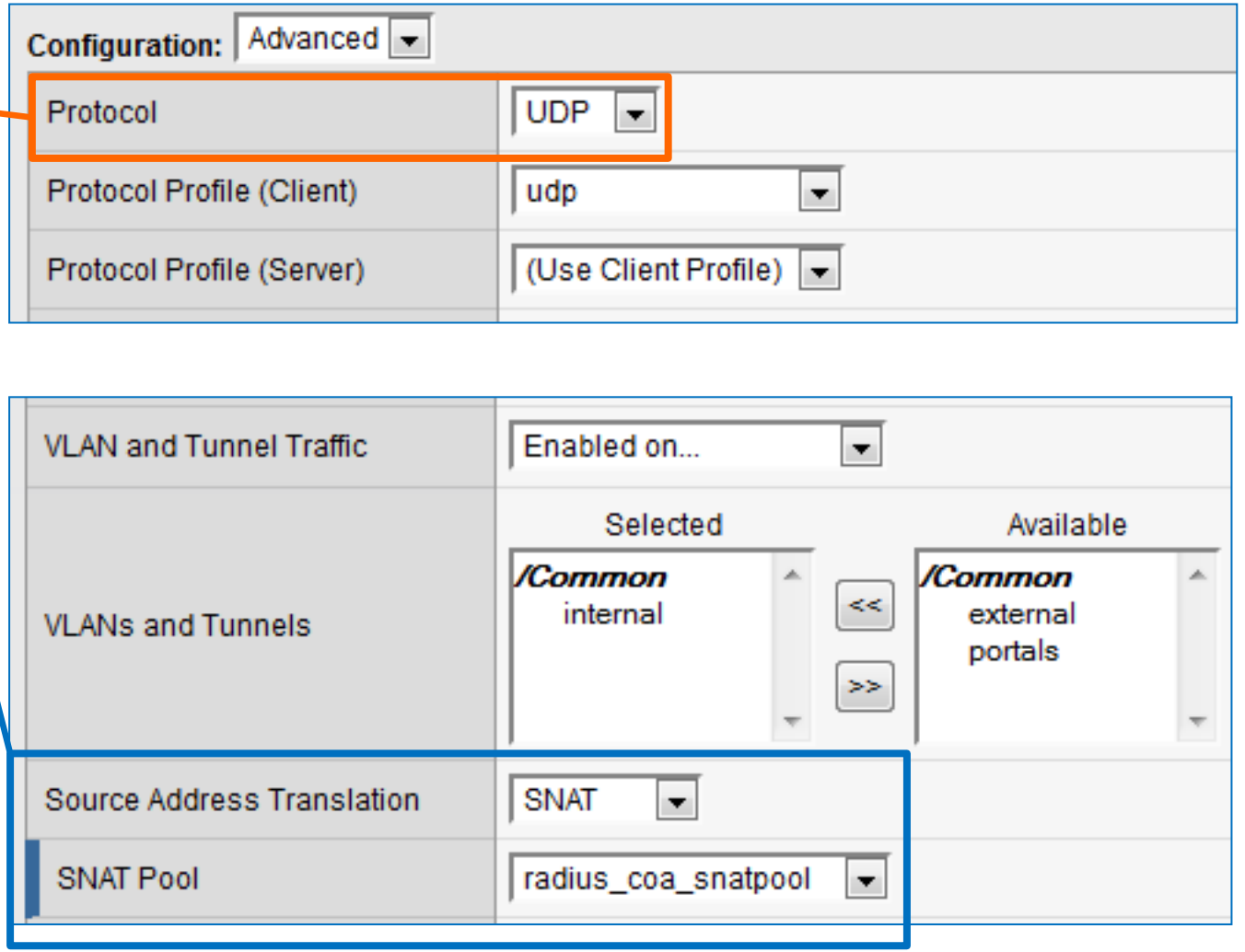


Configure Virtual Server to SNAT RADIUS CoA (Advanced)

Local Traffic > Virtual Servers

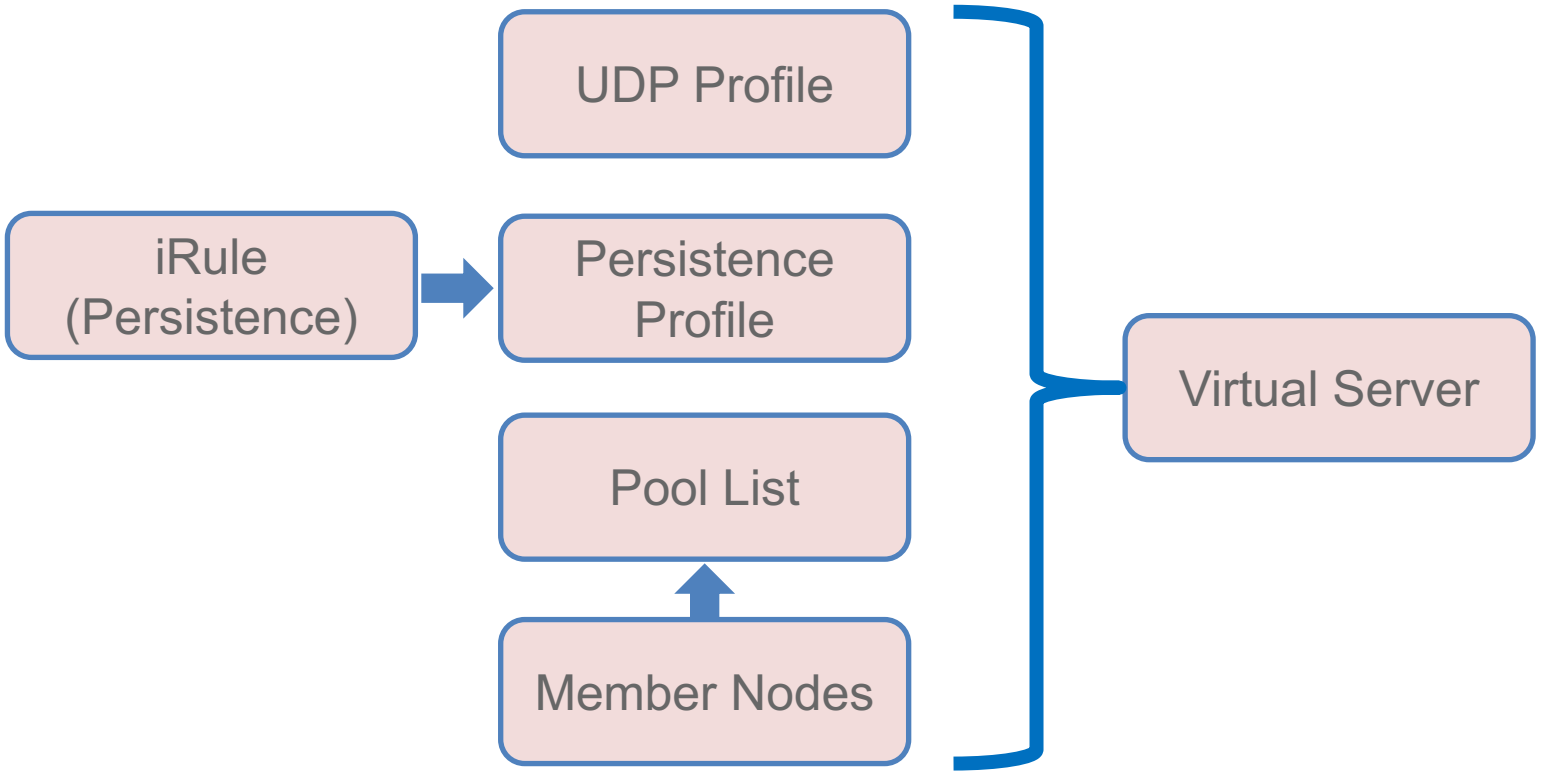
- Protocol = UDP
- Optional: Limit traffic to specific VLAN(s)
- Source Address Translation = SNAT
- SNAT Pool = CoA SNAT Pool List
- Resources = None





Load Balancing ISE Profiling

F5 LTM Configuration Components for Profiling LB



Configure UDP Profile for Profiling

Local Traffic > Profiles > Protocol > UDP

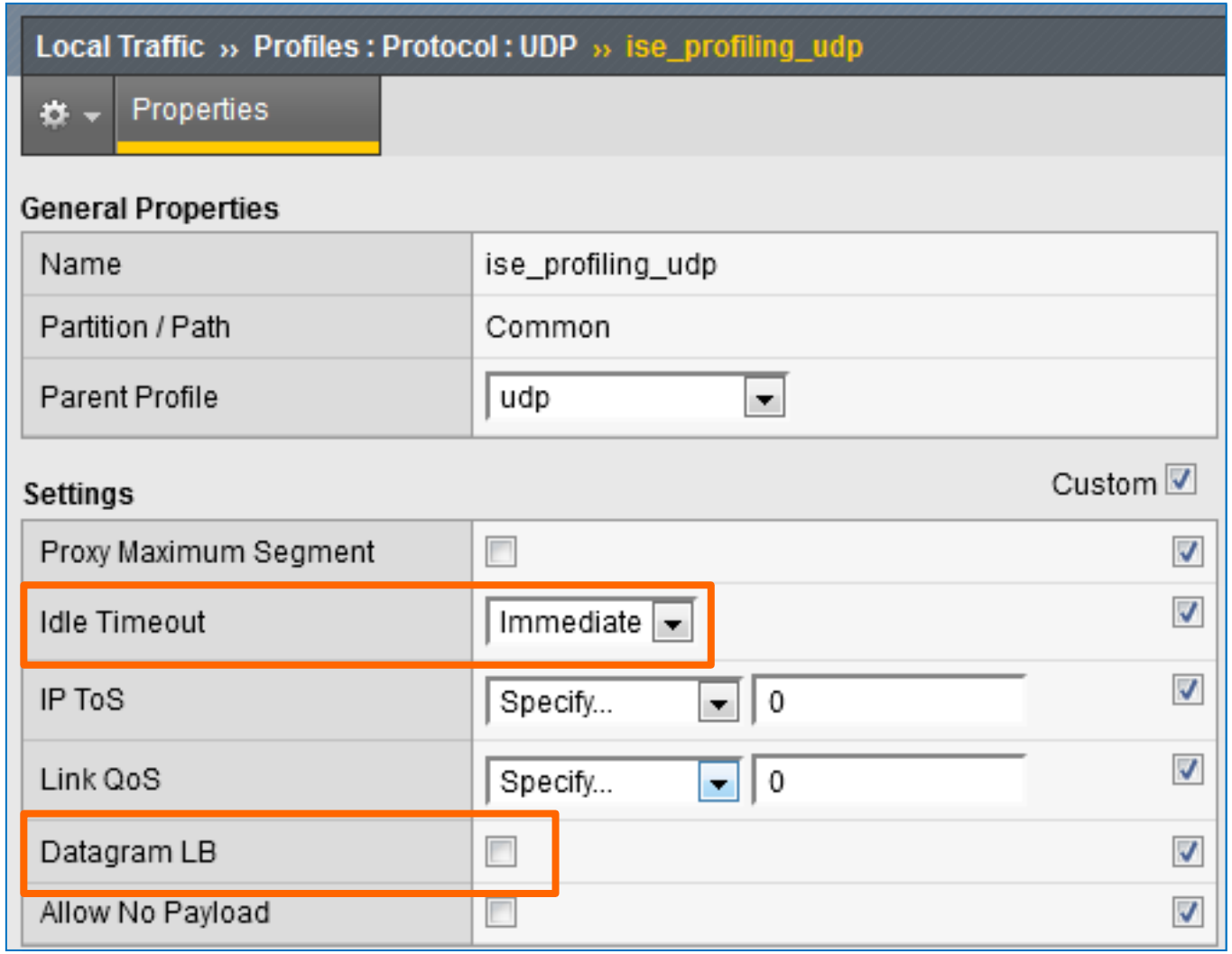
- Set Idle Timeout to Immediate

  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



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 $id a2a2a2a2a2a2 m(a) m(b) m(c) m(d) m(e) m(f)
            set value [string toupper "$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

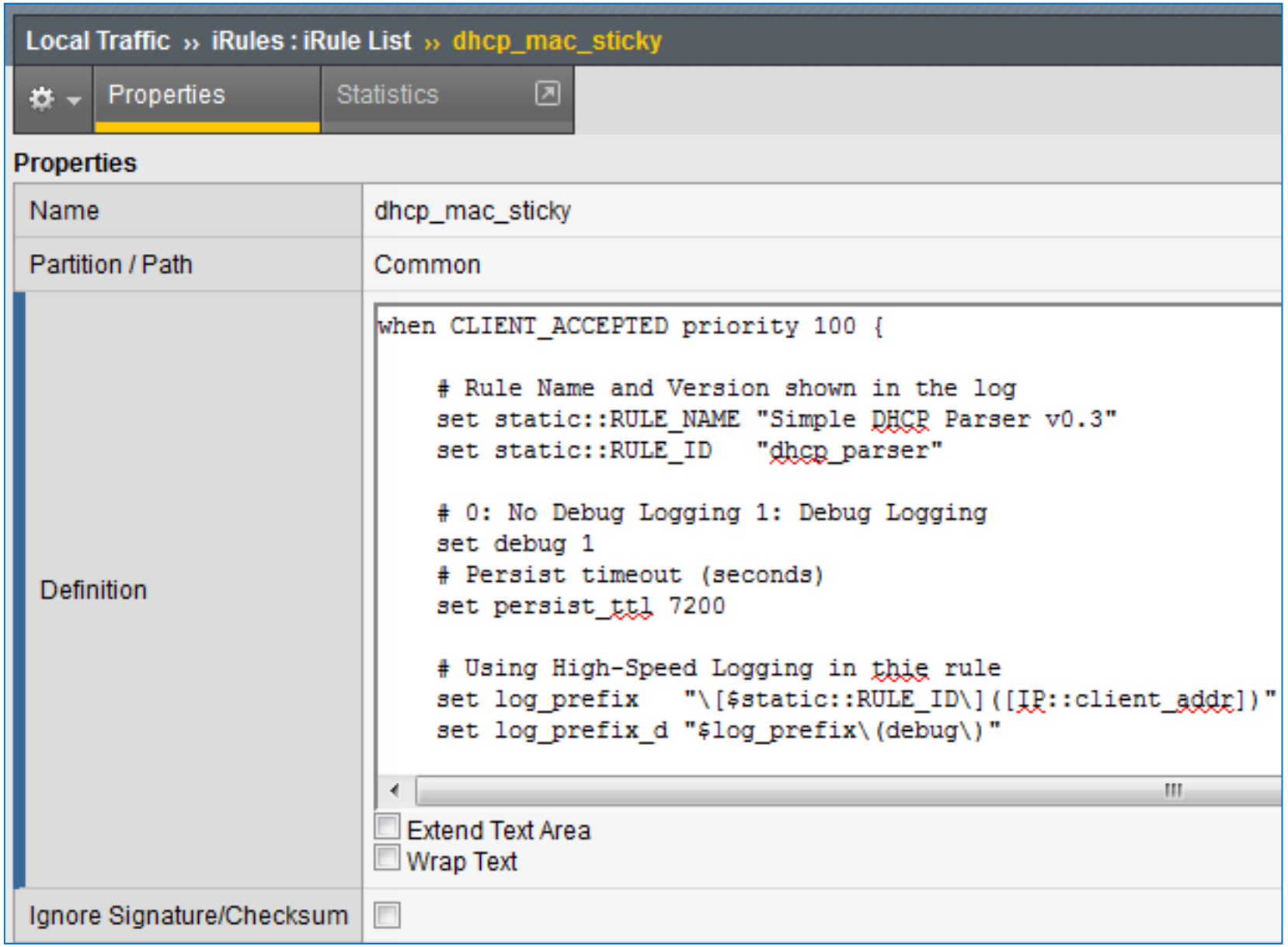
iRule for DHCP Persistence – Sample Debug Output

```
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 iRule for DHCP Profiling Persistence

Local Traffic > iRules > iRule List

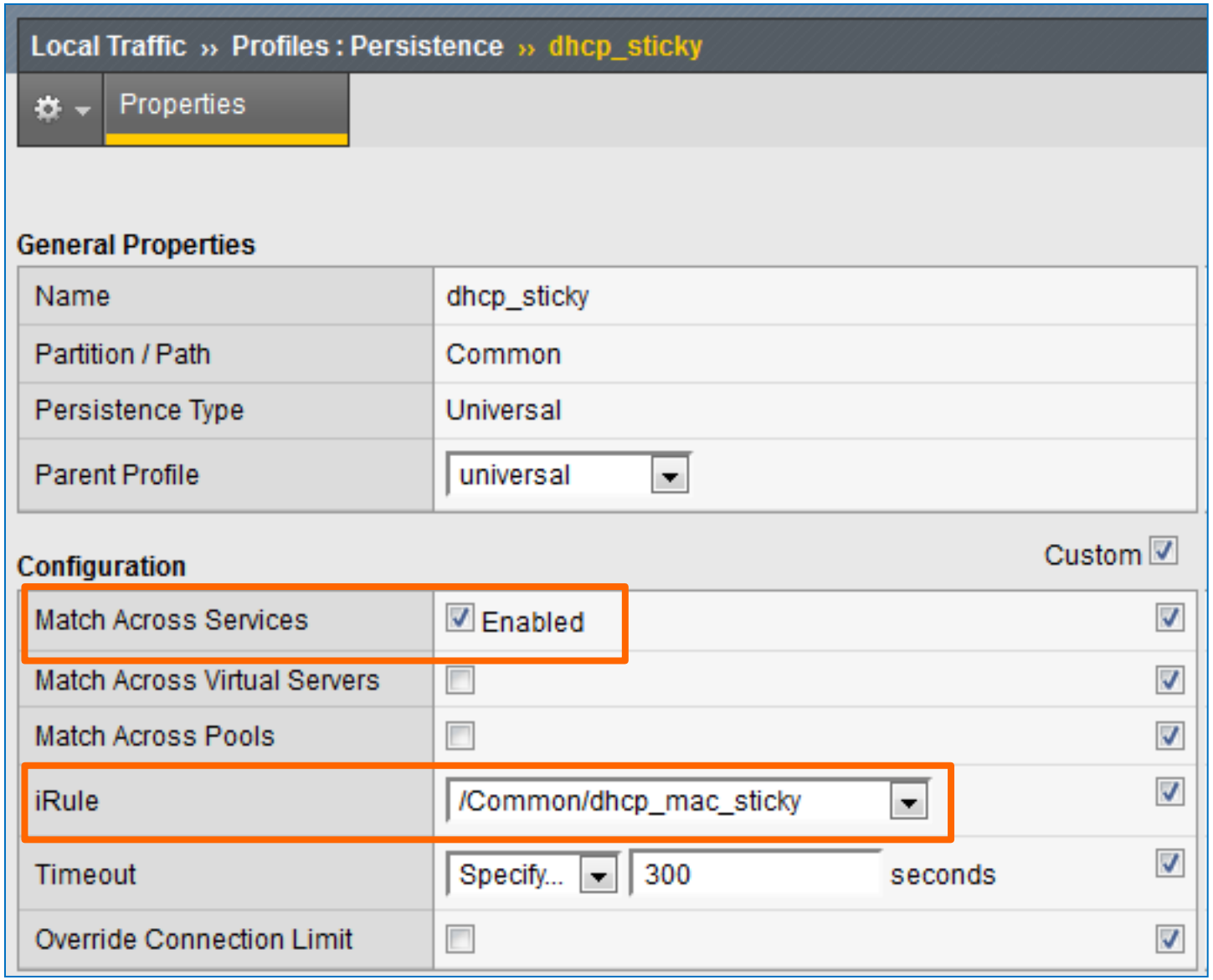
- Alternative to basic Source Address-based persistence
- Sample iRule based on client MAC address parsed from DHCP Request packets
- Allows DHCP for given endpoint to persist to same PSN serving RADIUS for same endpoint
- Recommend copy and paste working iRule into text area.



Optional: Configure Persistence Profile for Profiling

Local Traffic > Profiles > Persistence

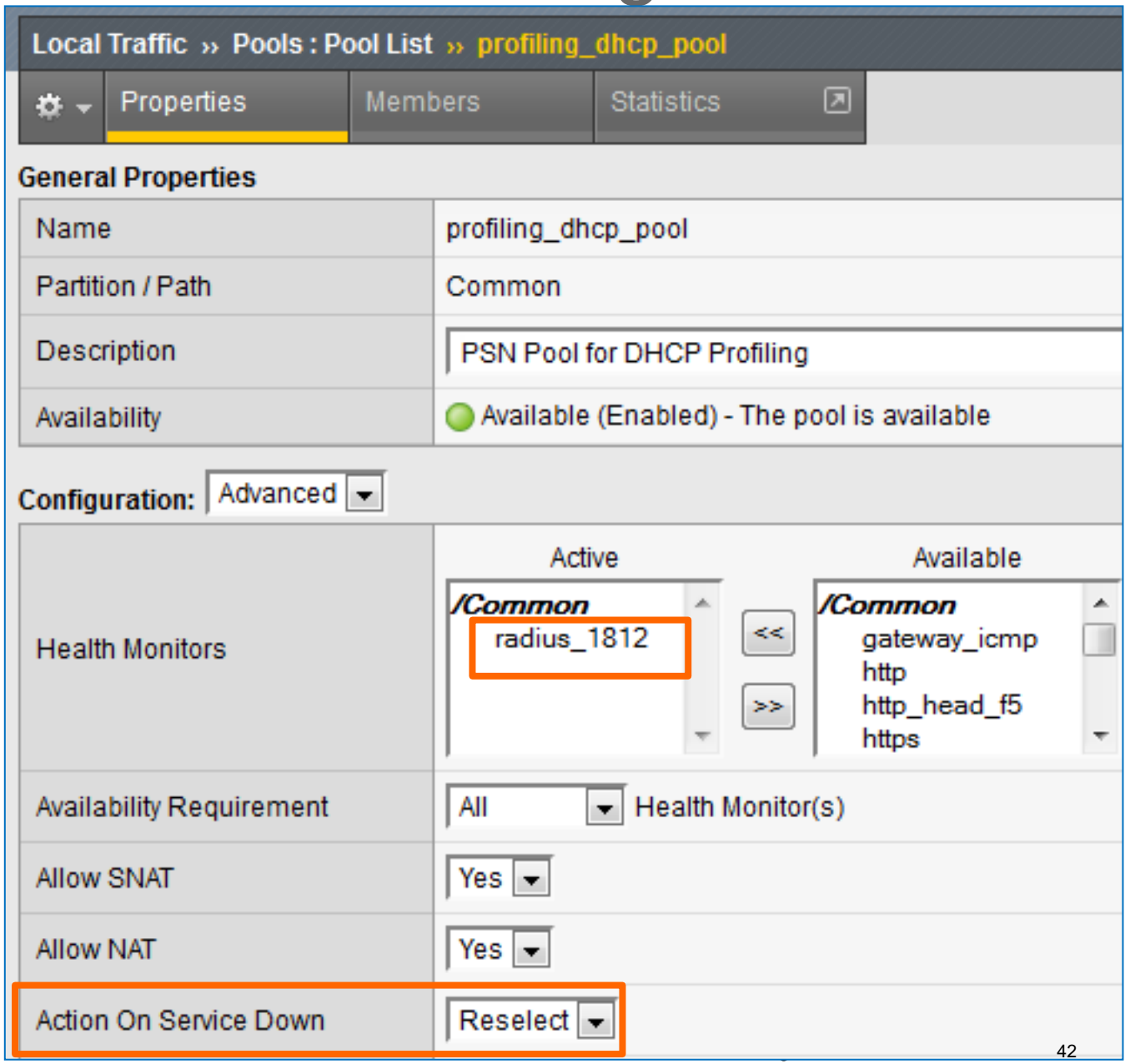
- Enable **Match Across Services**
- If different Virtual Server IP addresses used for DHCP Profiling and RADIUS, then enable Match Across Virtual Servers. (Recommend use same IP address)
- Specify DHCP Persistence iRule
- iRule persistence timer overrides profile setting.



Configure Server Pool for DHCP Profiling

Local Traffic > Pools > Pool List

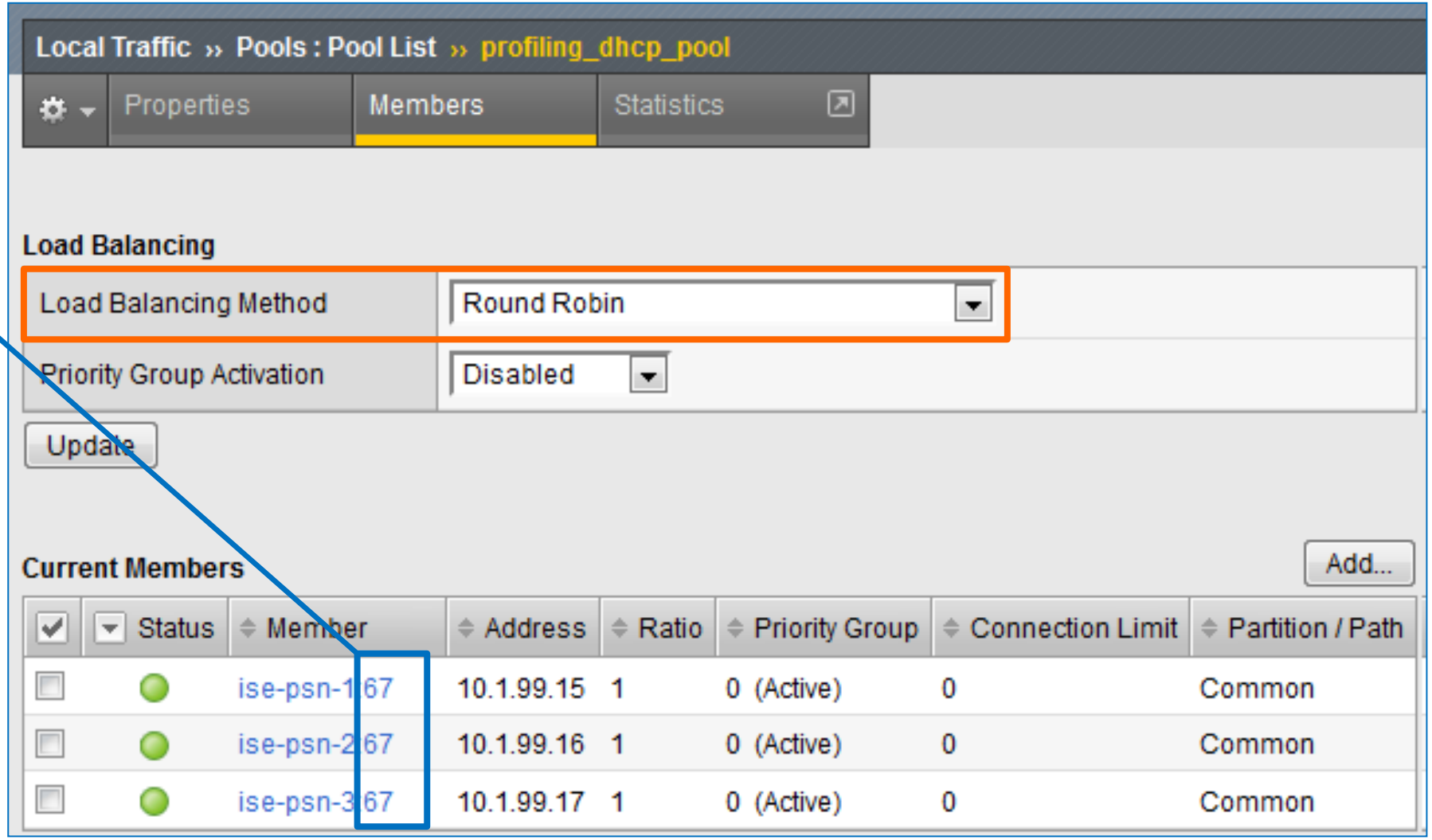
- Health Monitor = RADIUS Monitor
  - If PSN not configured for User Services (RADIUS auth), then can use default **gateway_icmp** monitor.
- Action on Service Down = Reselect
  - Ensures existing connections are moved to an alternate server.



Configure Member Nodes in DHCP Profiling Pool

Local Traffic > Pools > Members

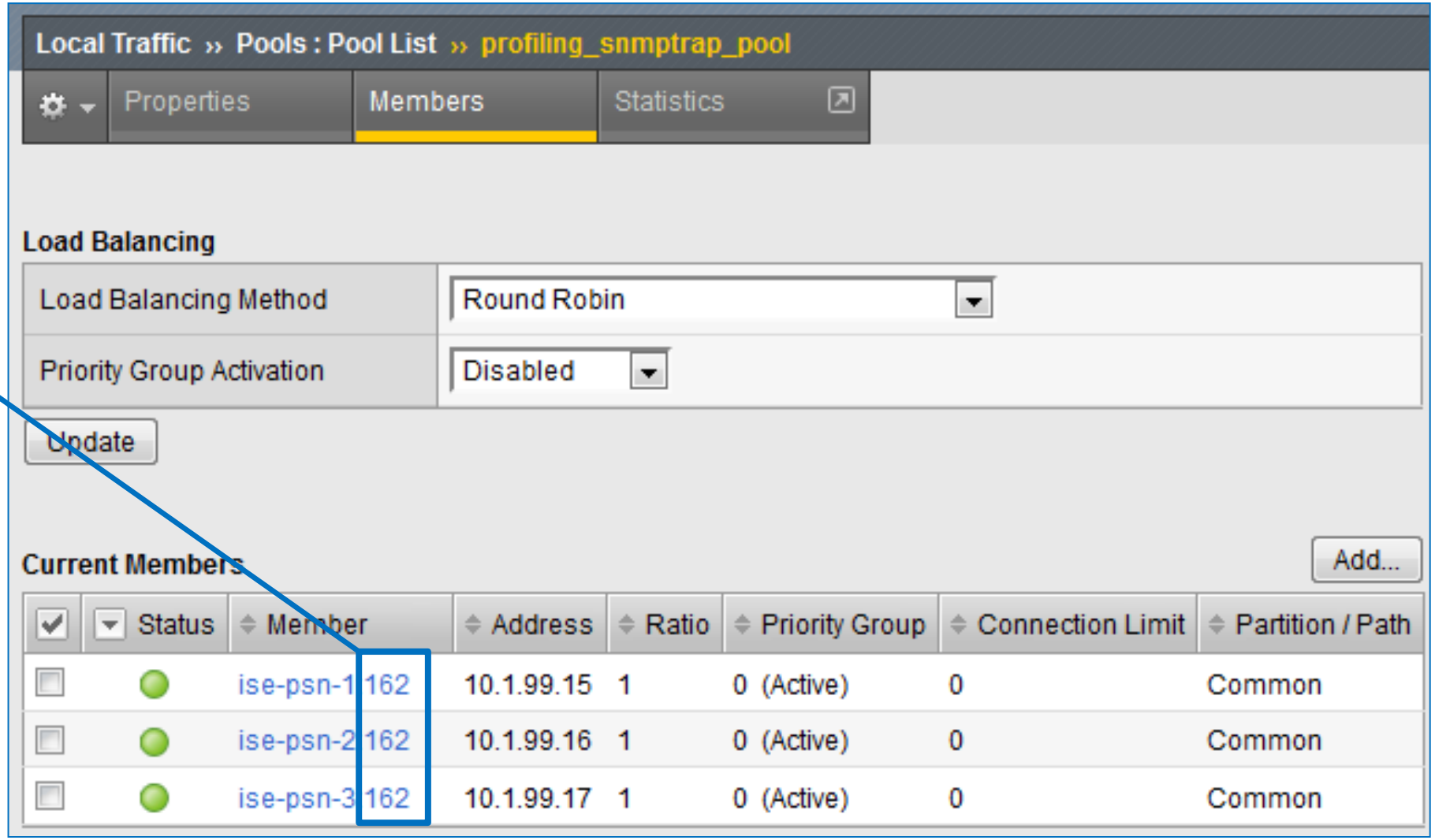
- Load Balancing Method = Round Robin
- Server Port = 67 (DHCP Server)



Configure Server Pool for SNMP Trap Profiling

Local Traffic > Pools

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

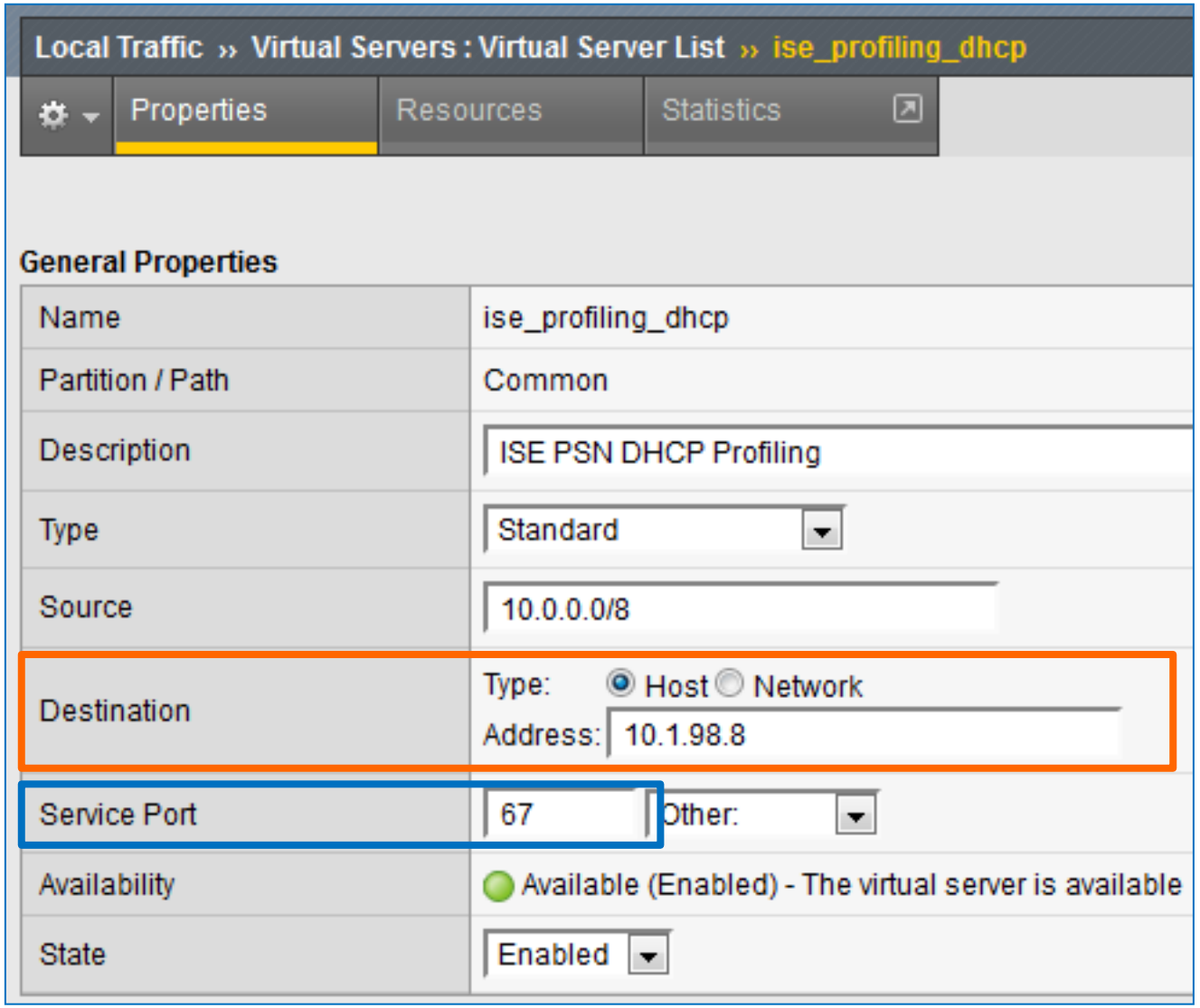


Configure Virtual Server for DHCP Profiling (Properties)

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.

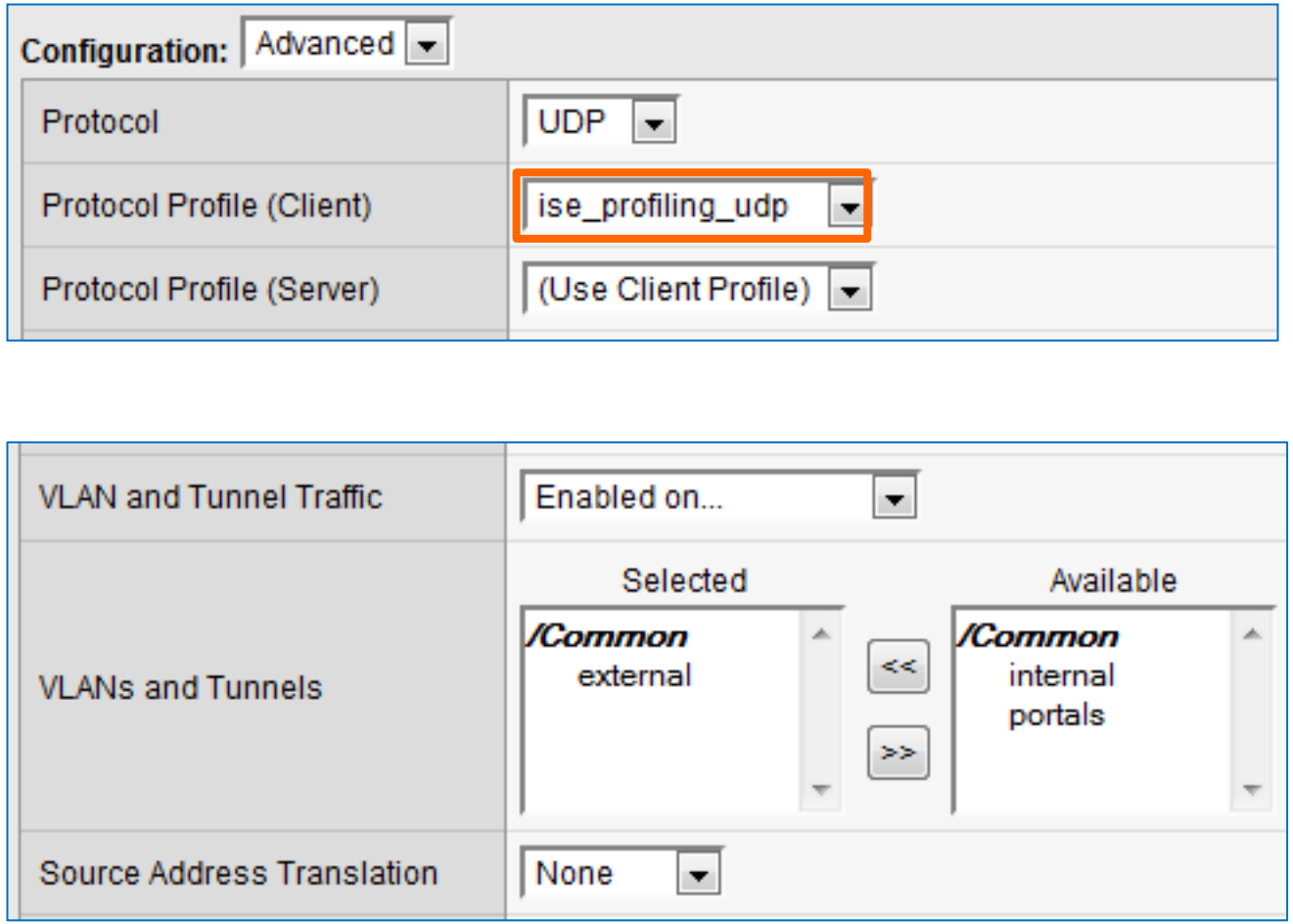
  Be sure to configure DHCP Relays/ IP Helpers to point to this IP address
- Service Port = 67



Configure Virtual Server for DHCP Profiling (Advanced)

Local Traffic > Virtual Servers

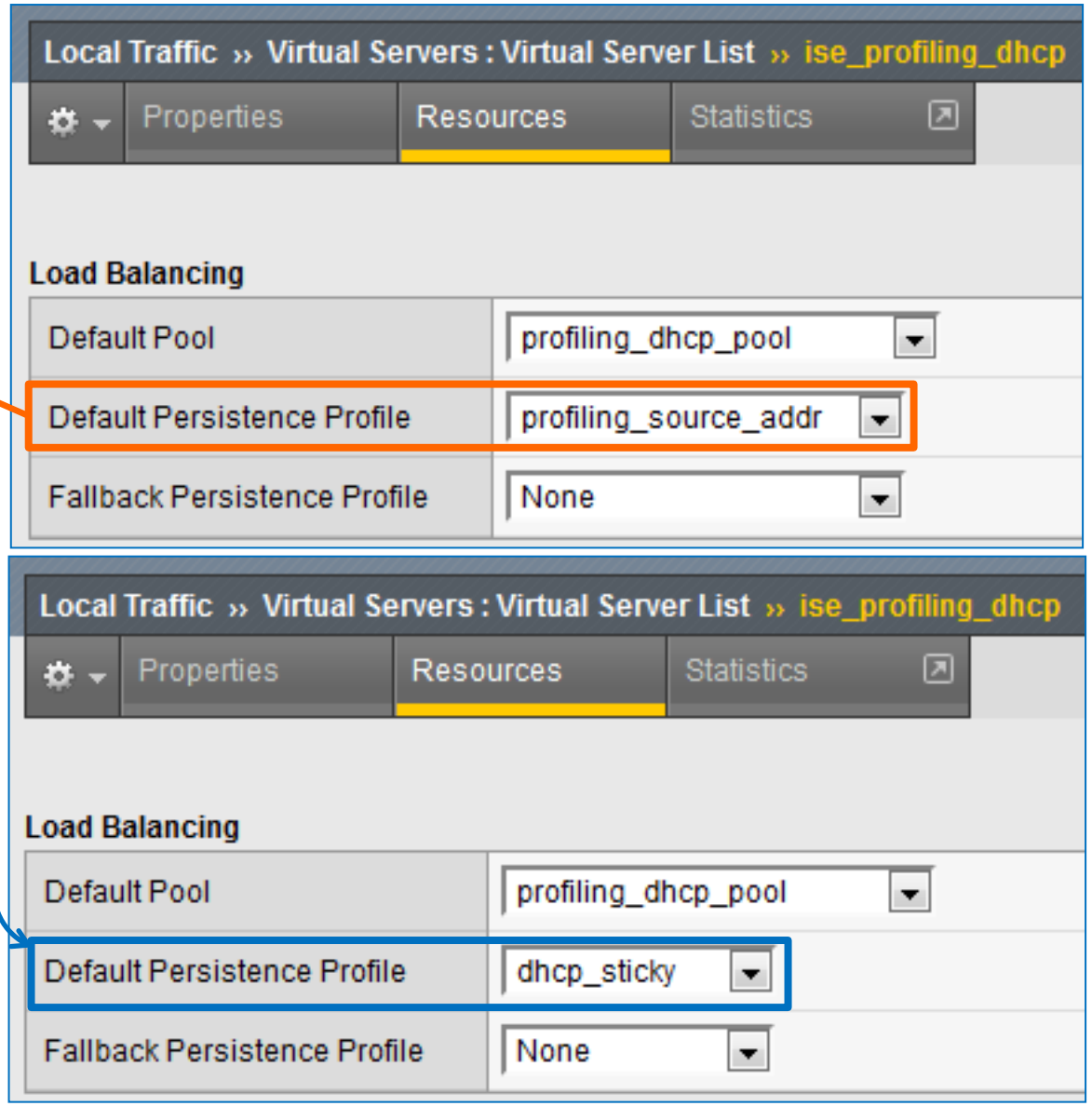
- Protocol = UDP
- Protocol Profile = udp or custom UDP profile
- Optional: Limit traffic to specific VLAN(s)



Configure Virtual Server for DHCP Profiling (Resources)

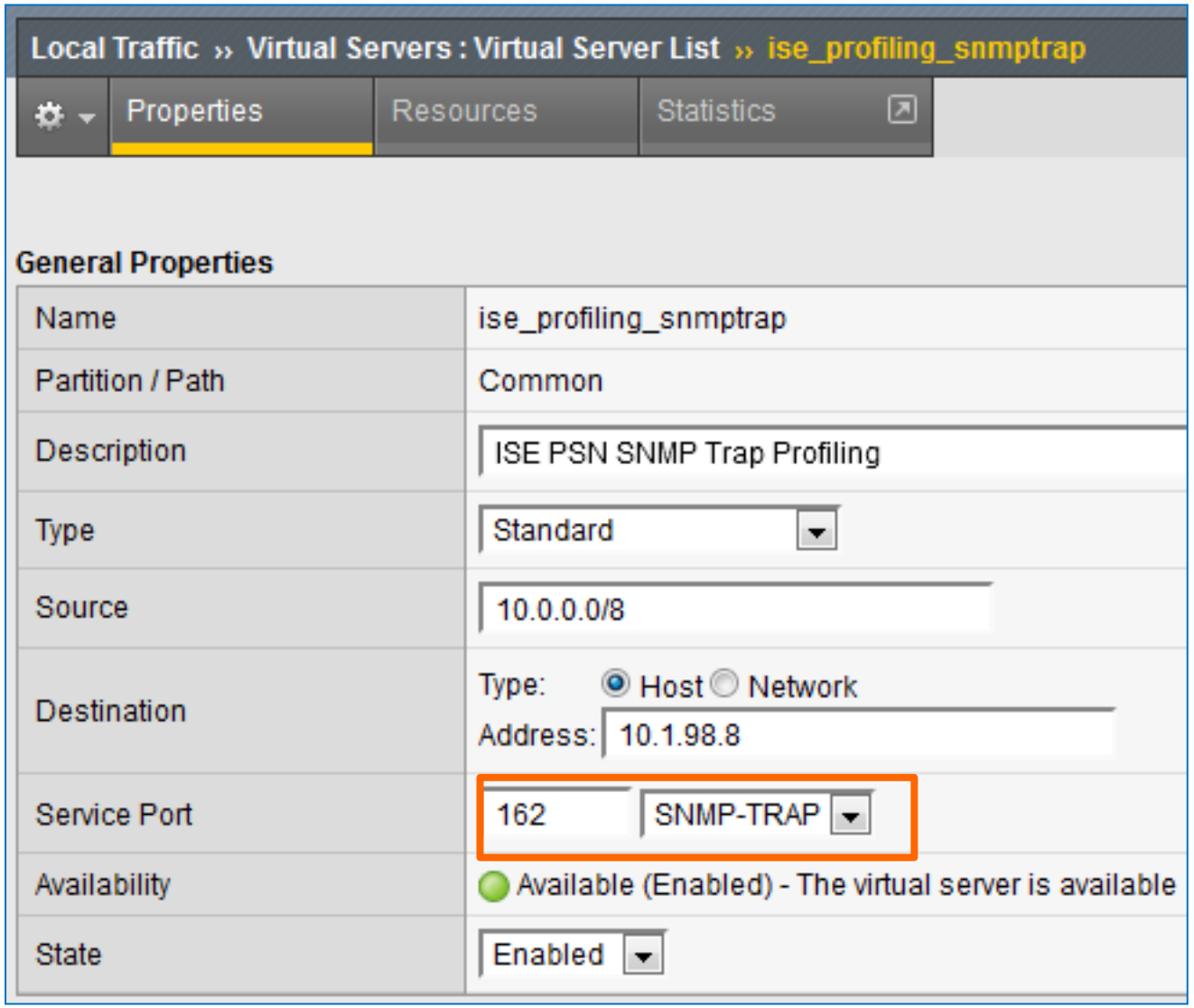
Local Traffic > Virtual Servers > Resources

- 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.



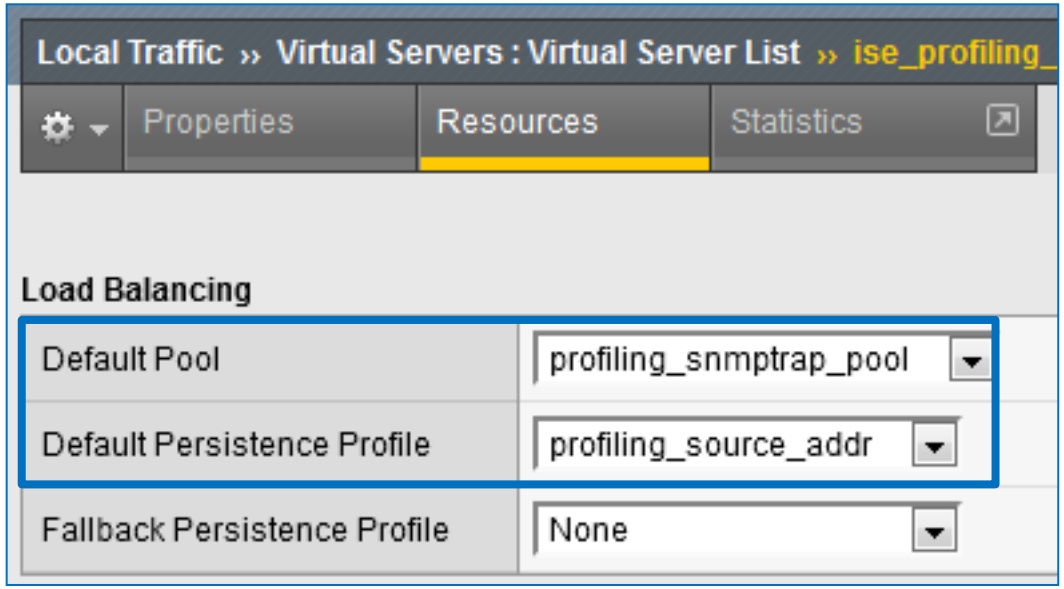
Configure Virtual Server for SNMP Trap Profiling

Local Traffic > Virtual Servers



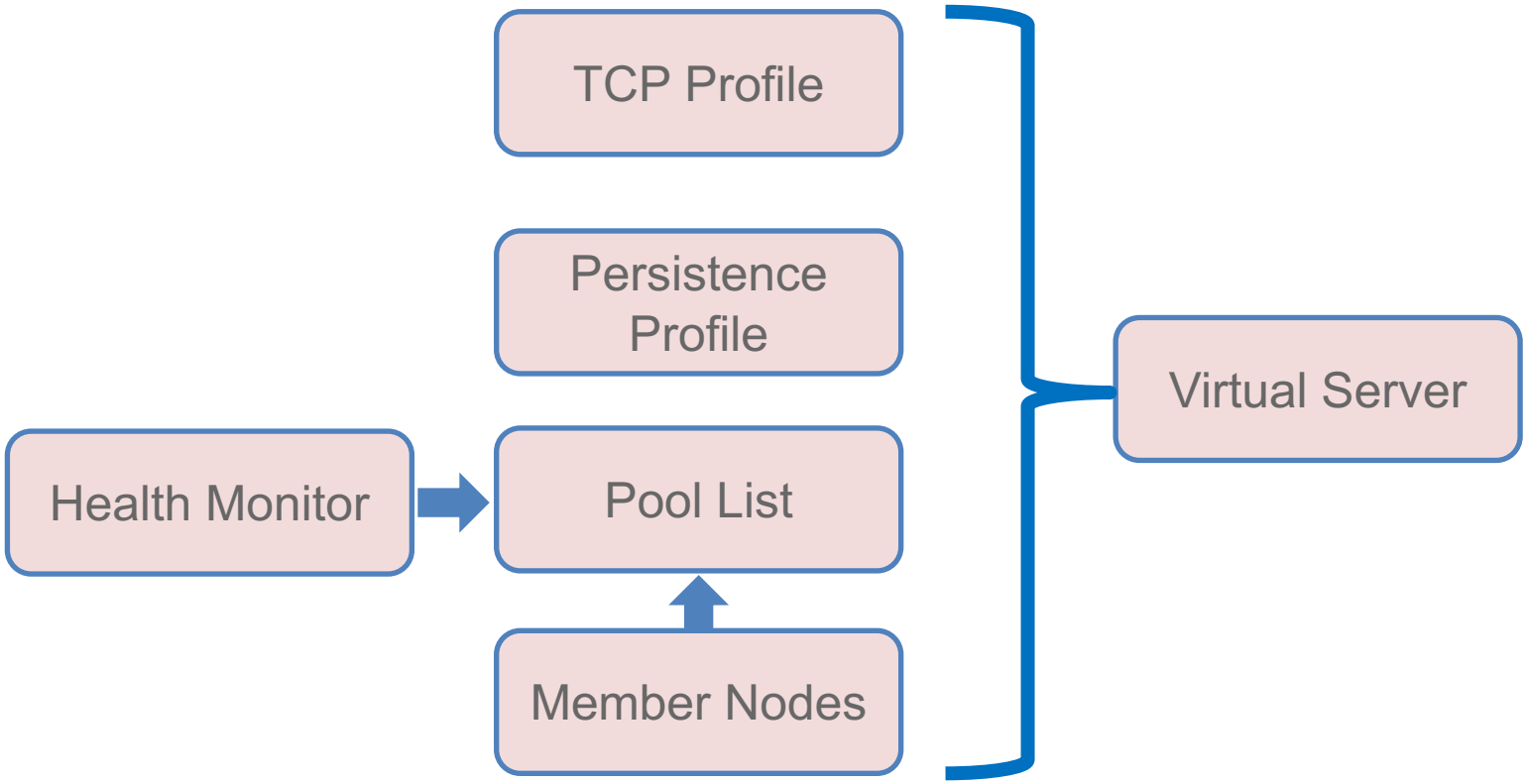
- Same settings as DHCP Profiling Virtual Server but different service port and pool.

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



Load Balancing ISE Web Services

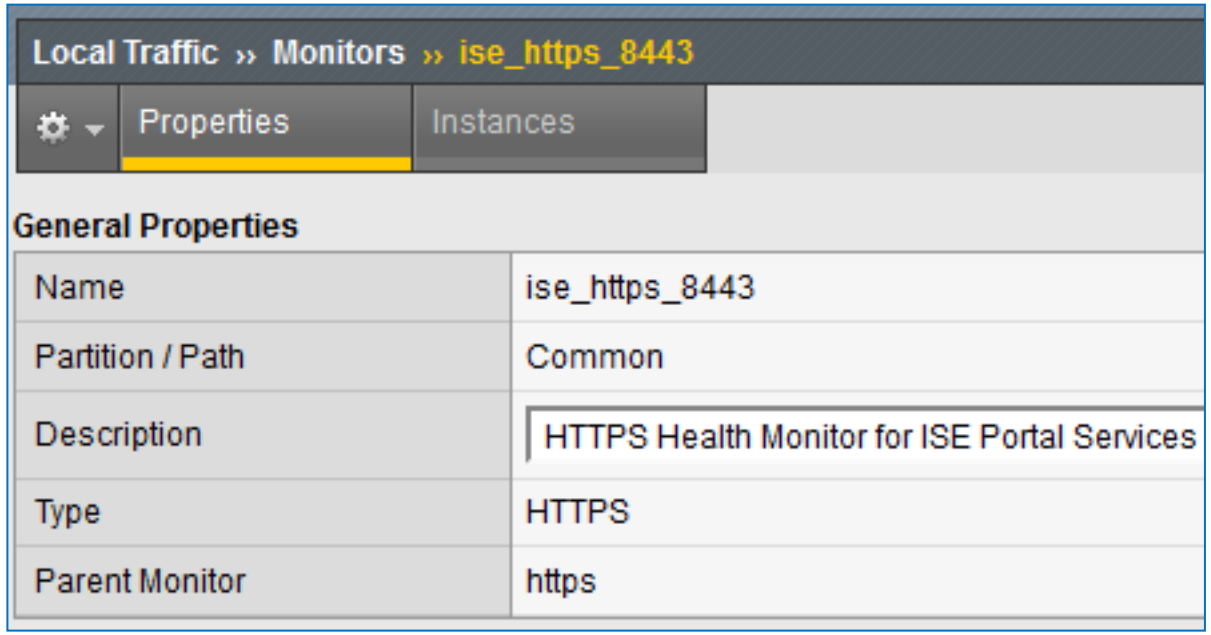
F5 LTM Configuration Components for HTTP/S LB

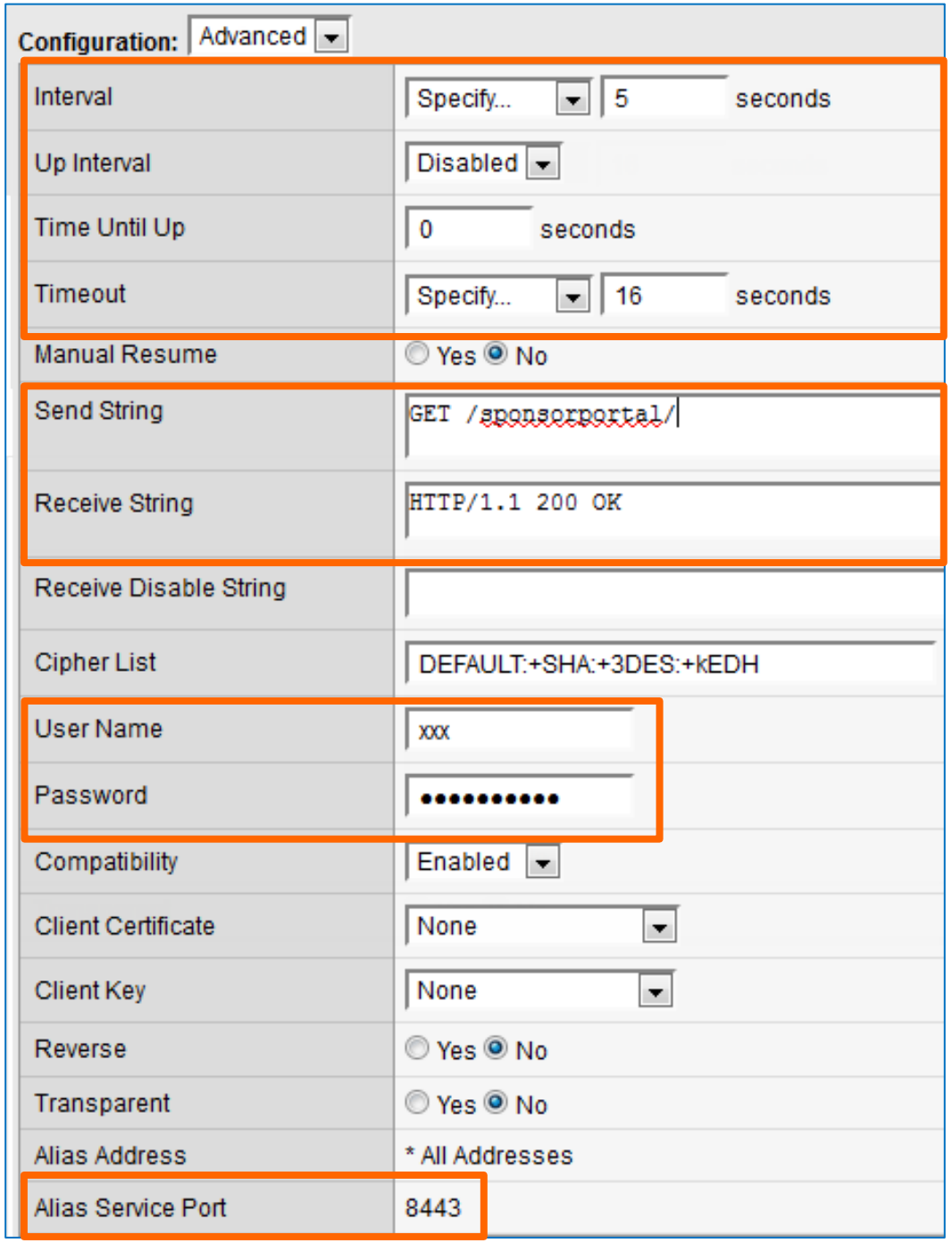


Configure HTTPS Health Monitor

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





HTTPS Health Monitor Examples

Local Traffic > Monitors

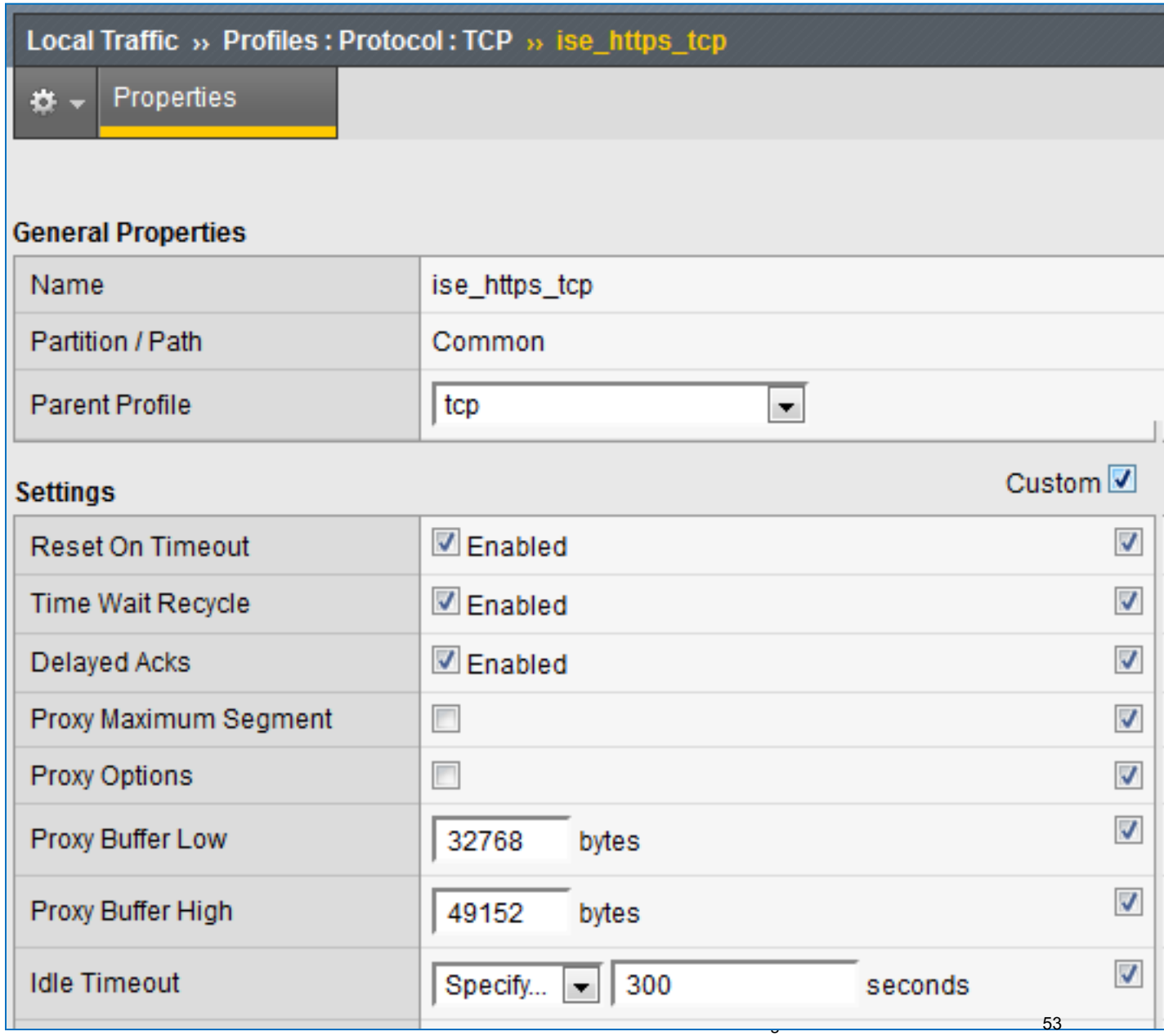
- ISE 1.2 Example
  - Send String: GET /sponsorportal/
  - Receive String: HTTP/1.1 200 OK

- 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



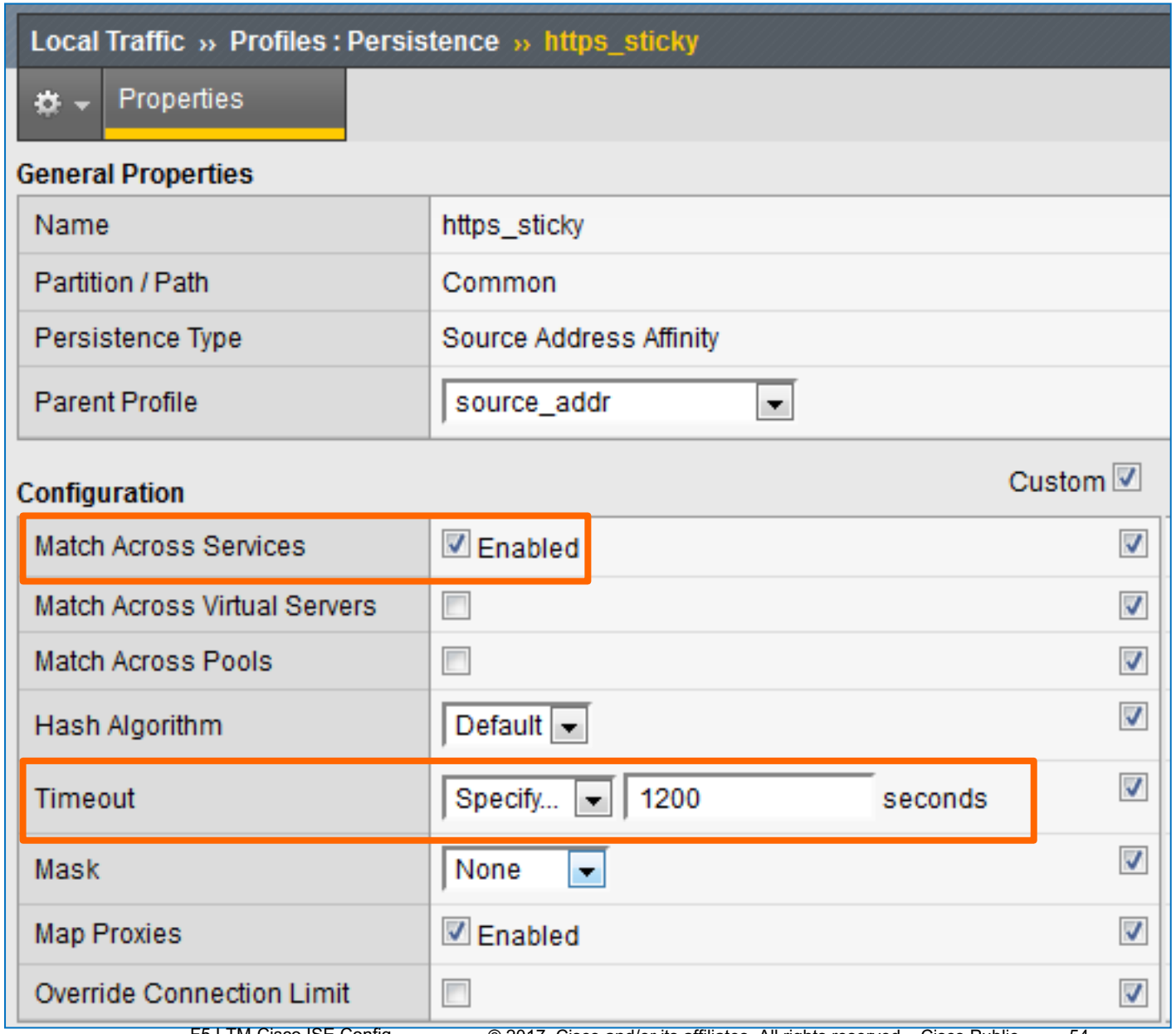
Configure Persistence Profile for HTTPS

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

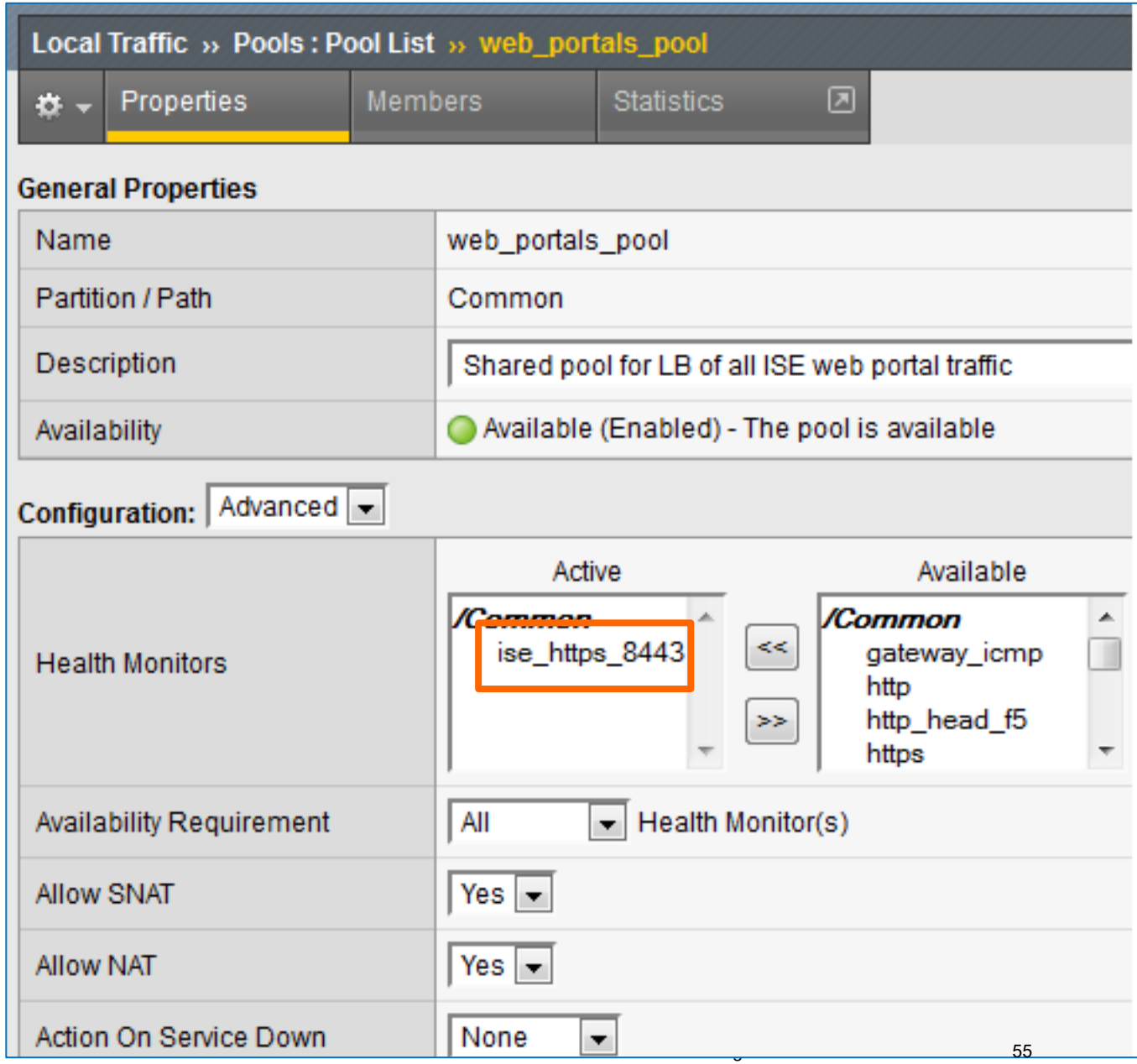
  Value of 1200 seconds = 20 minutes (default Sponsor Portal idle timeout setting in ISE)



Configure Server Pool for Web Services

Local Traffic > Pools > Pool List

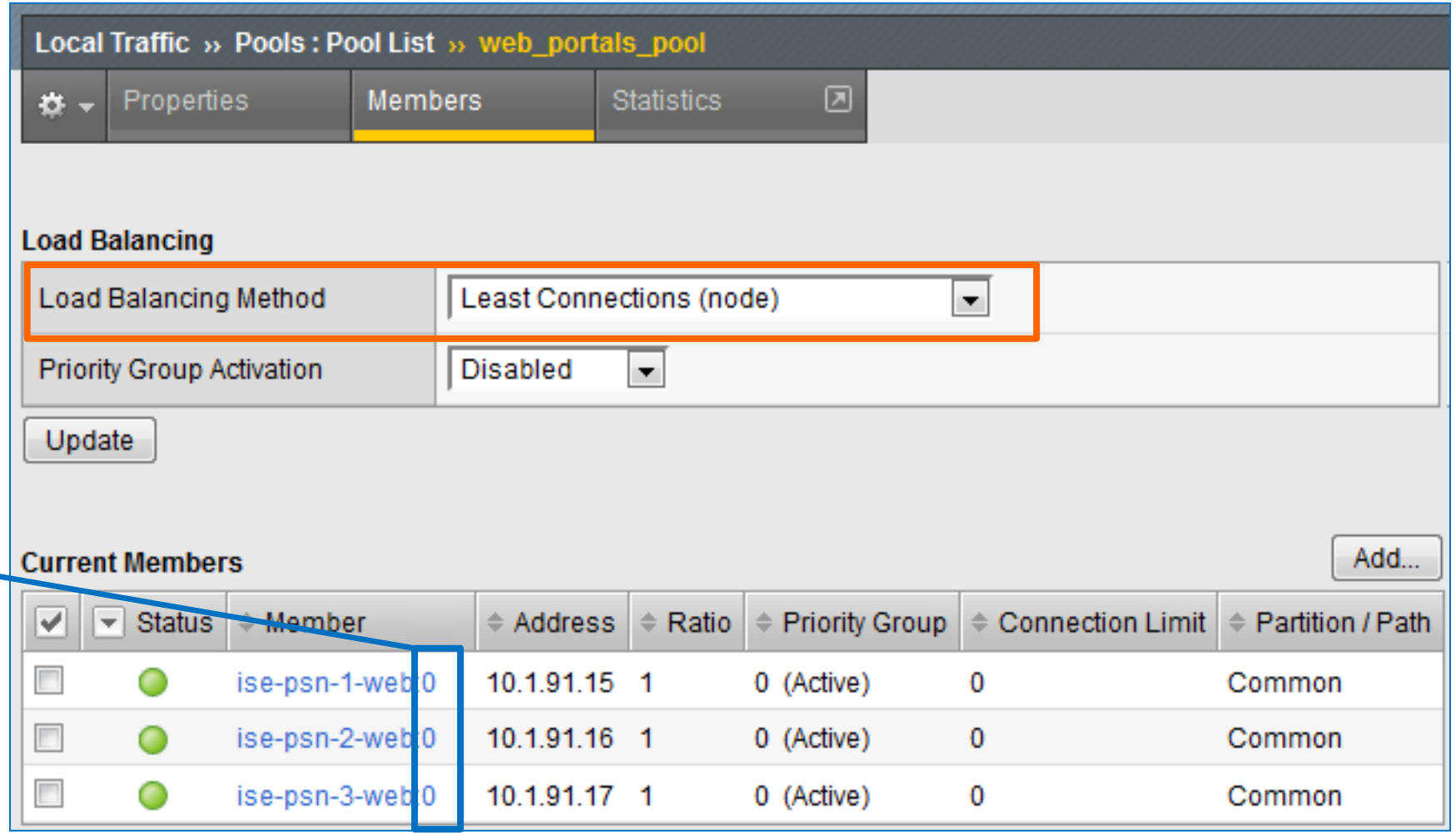
- Health Monitor = HTTPS Monitor
- Action on Service Down = None



Configure Member Nodes in Web Services Pool

Local Traffic > Pools > Pool List > Members

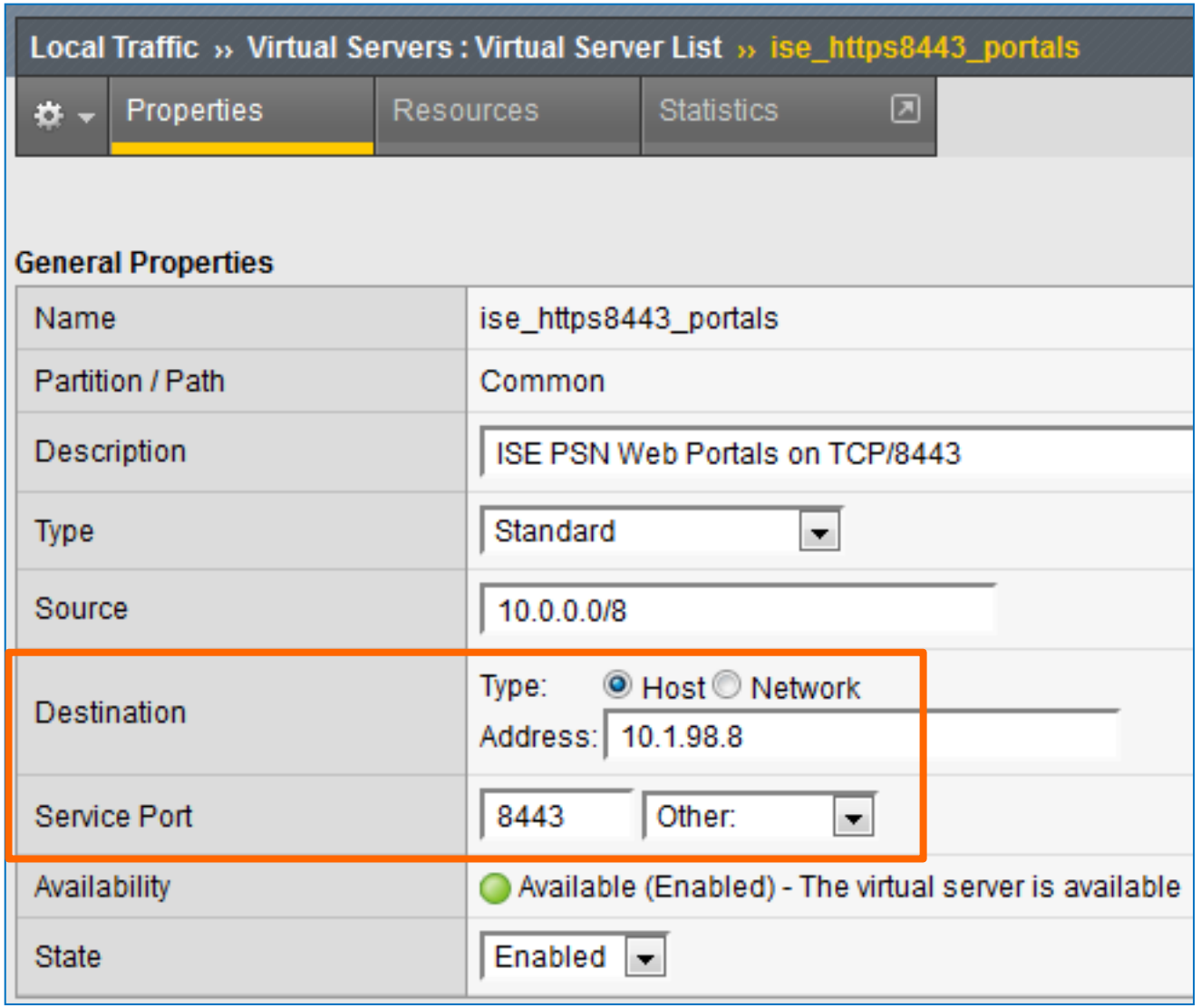
- Load Balancing Method options:
  - Least Connections (node)
  - Least Connections (member)
  - Fastest (application)
- Server Port = 0 (all ports)



Configure Virtual Server for Web Portals (Properties)

Local Traffic > Virtual Servers > Virtual Server List

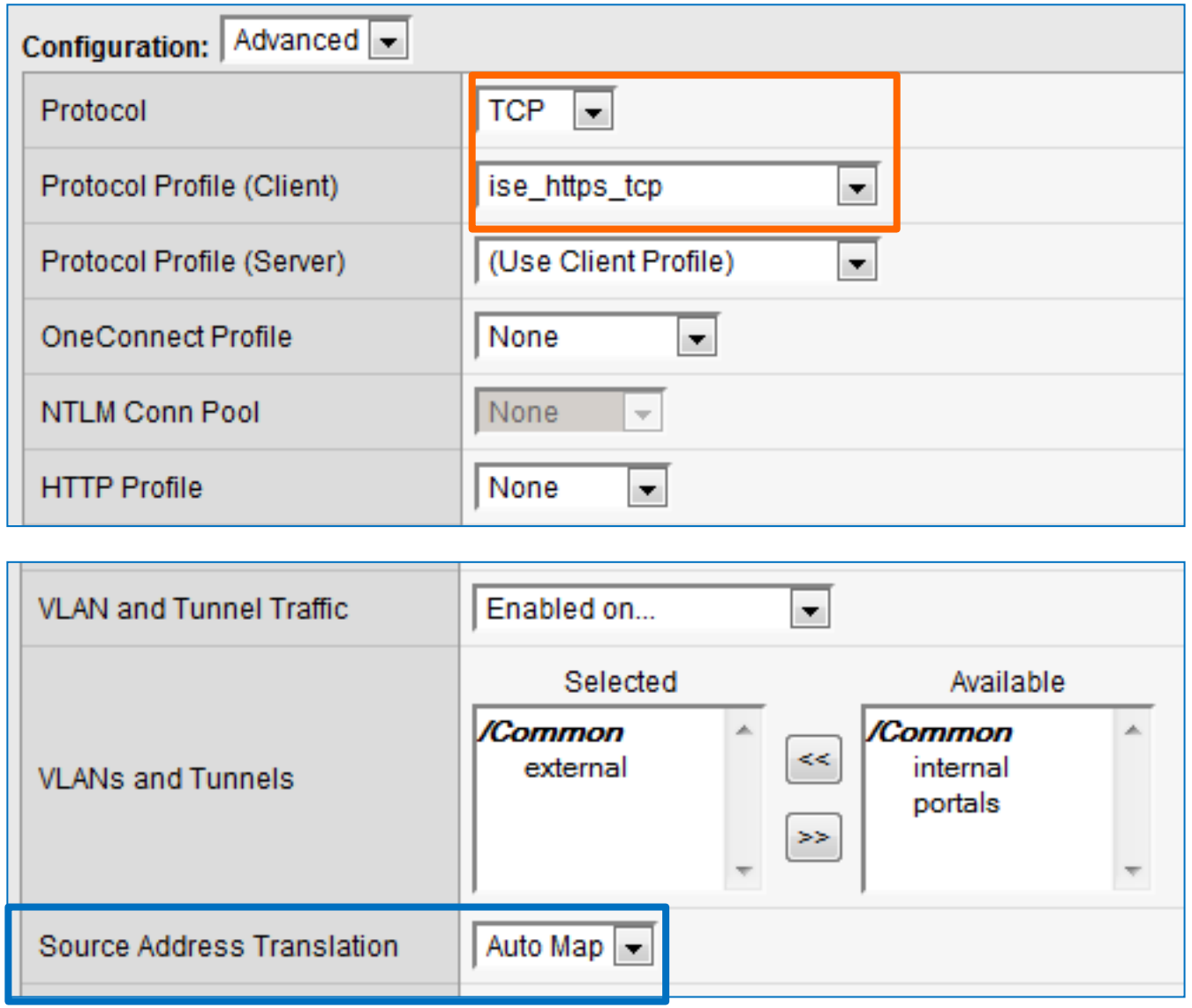
- Type = Standard
- Source = 0.0.0.0/0 (all hosts) or specific network address.
- Destination = Web Portal Virtual IP
- Service Port = Web Portal Port configured in ISE (default 8443)



Configure Virtual Server for HTTPS Portals (Advanced)

Local Traffic > Virtual Servers

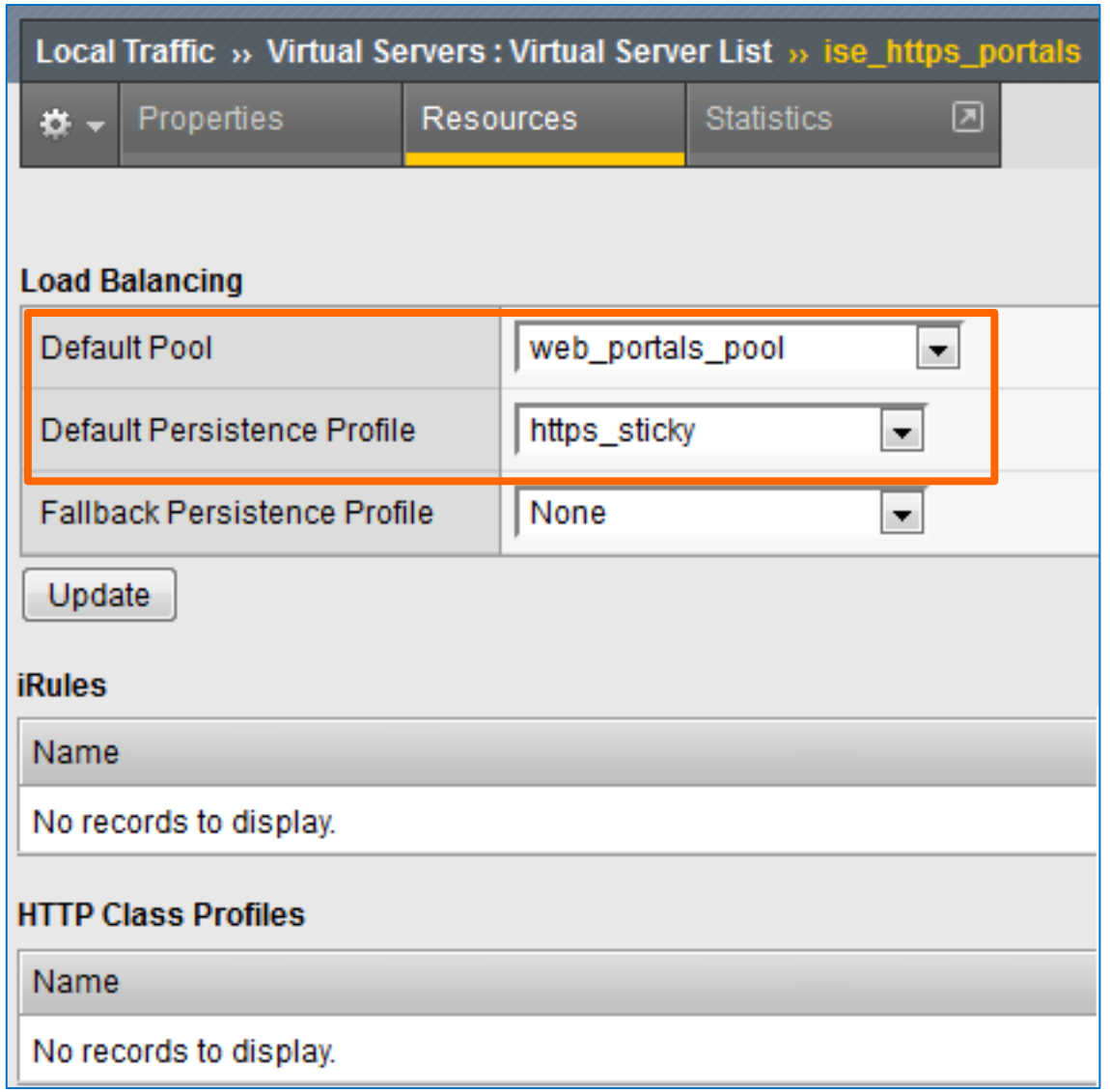
- Protocol = TCP
- Protocol Profile = tcp or custom TCP profile
- Optional: Limit traffic to specific VLAN(s)
- Source Address Translation (SNAT)
  - Single PSN interface: None
  - Dedicated PSN interface (ISE 1.2): Auto Map
  - Dedicated PSN interface (ISE 1.3): None or Auto Map



Configure Virtual Server HTTPS Portals (Resources)

Local Traffic > Virtual Servers > Virtual Server List > Resources

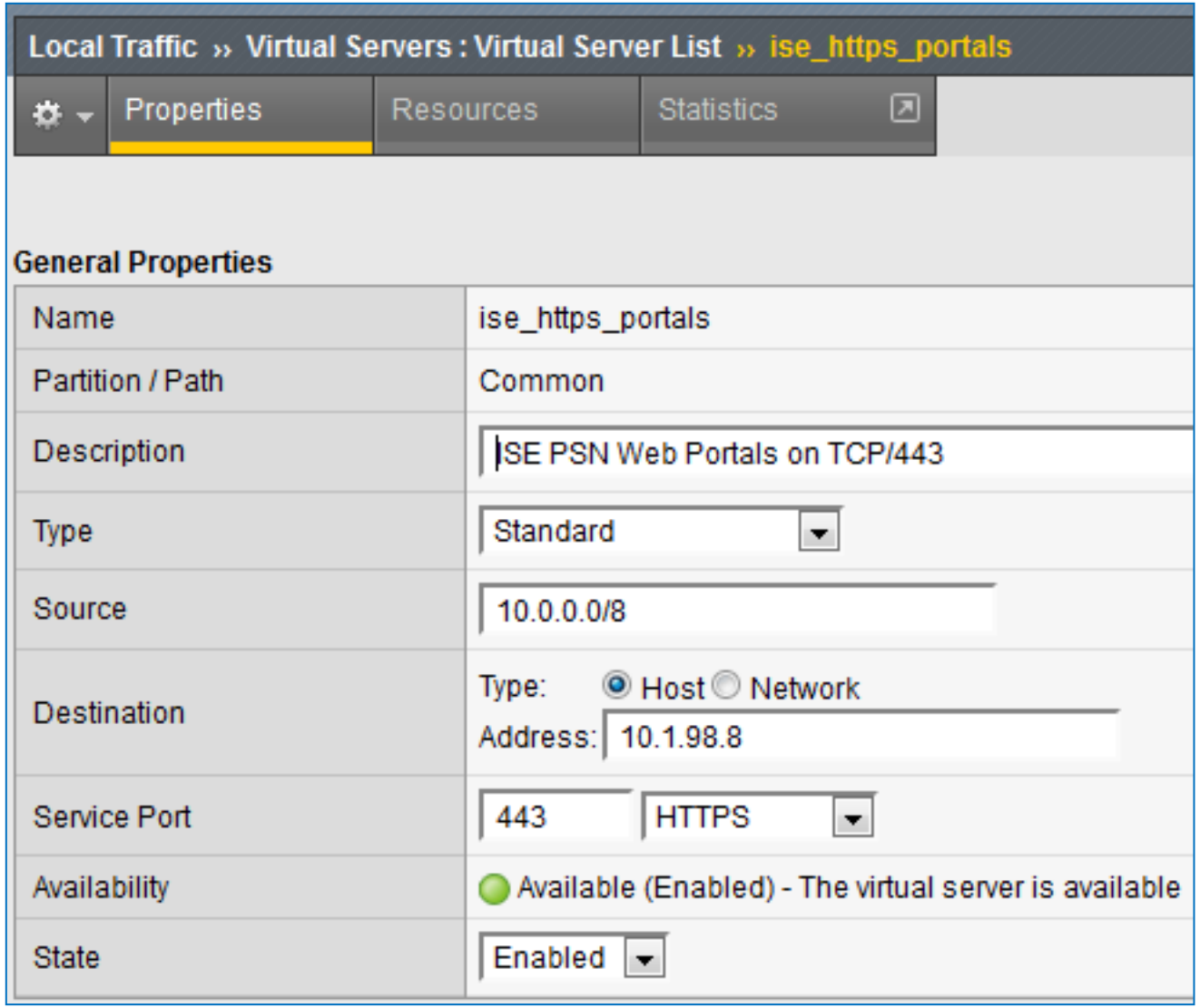
- Default Pool = Web Portals Pool
- Default Persistence Profile = HTTPS persistence profile
- Fallback Persistence Profile: Not required



Configure Virtual Server for Web Portals on TCP/443

Local Traffic > Virtual Servers > Virtual Server List

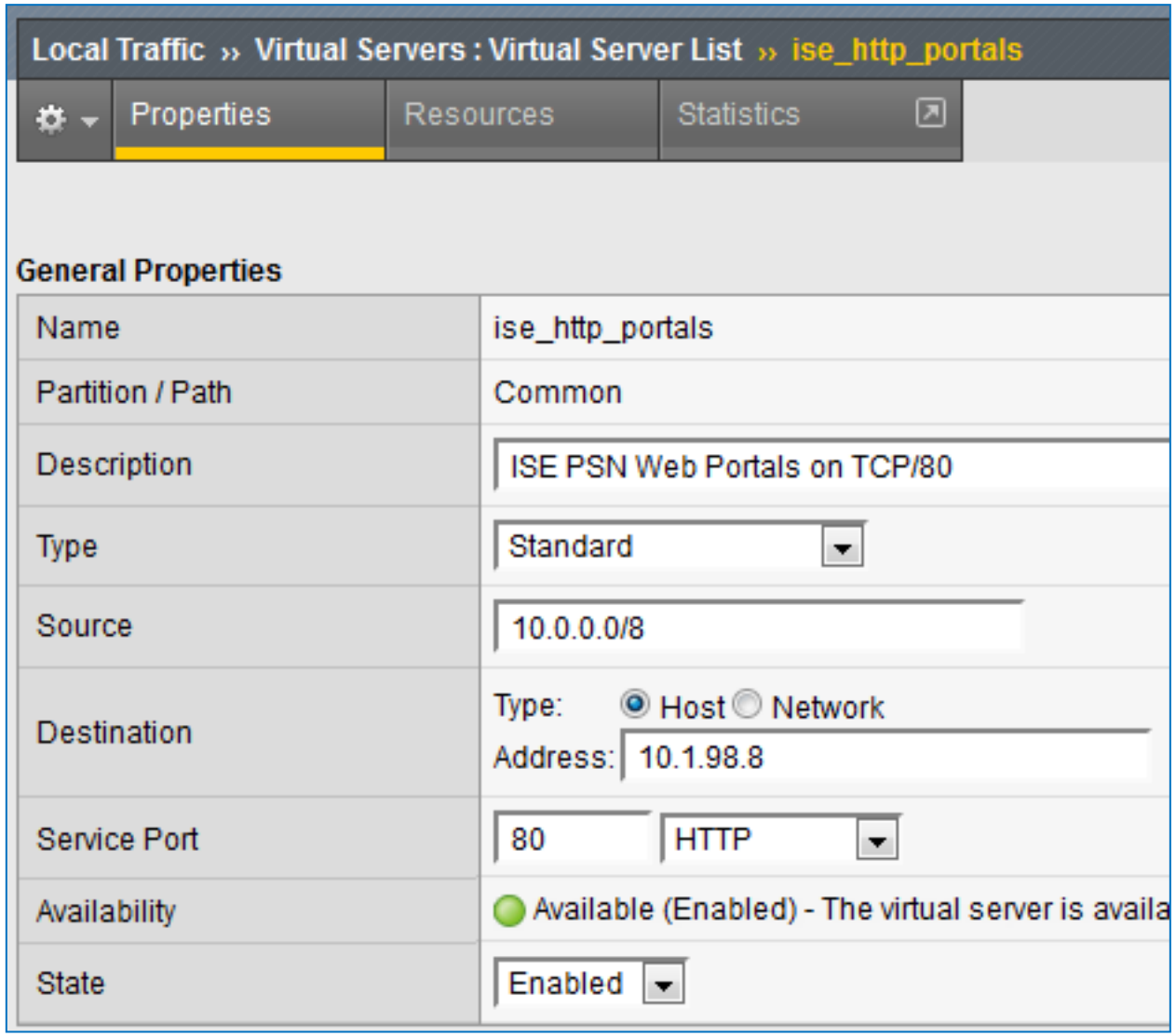
- Virtual Server used to forward web traffic sent to portal FQDN on default HTTPS port 443
- PSNs will automatically redirect traffic to FQDN to specific portal port / URL.
- Service Port = 443 (HTTPS) Default HTTPS port used in initial portal request by end user.
- All other Virtual Server settings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



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)

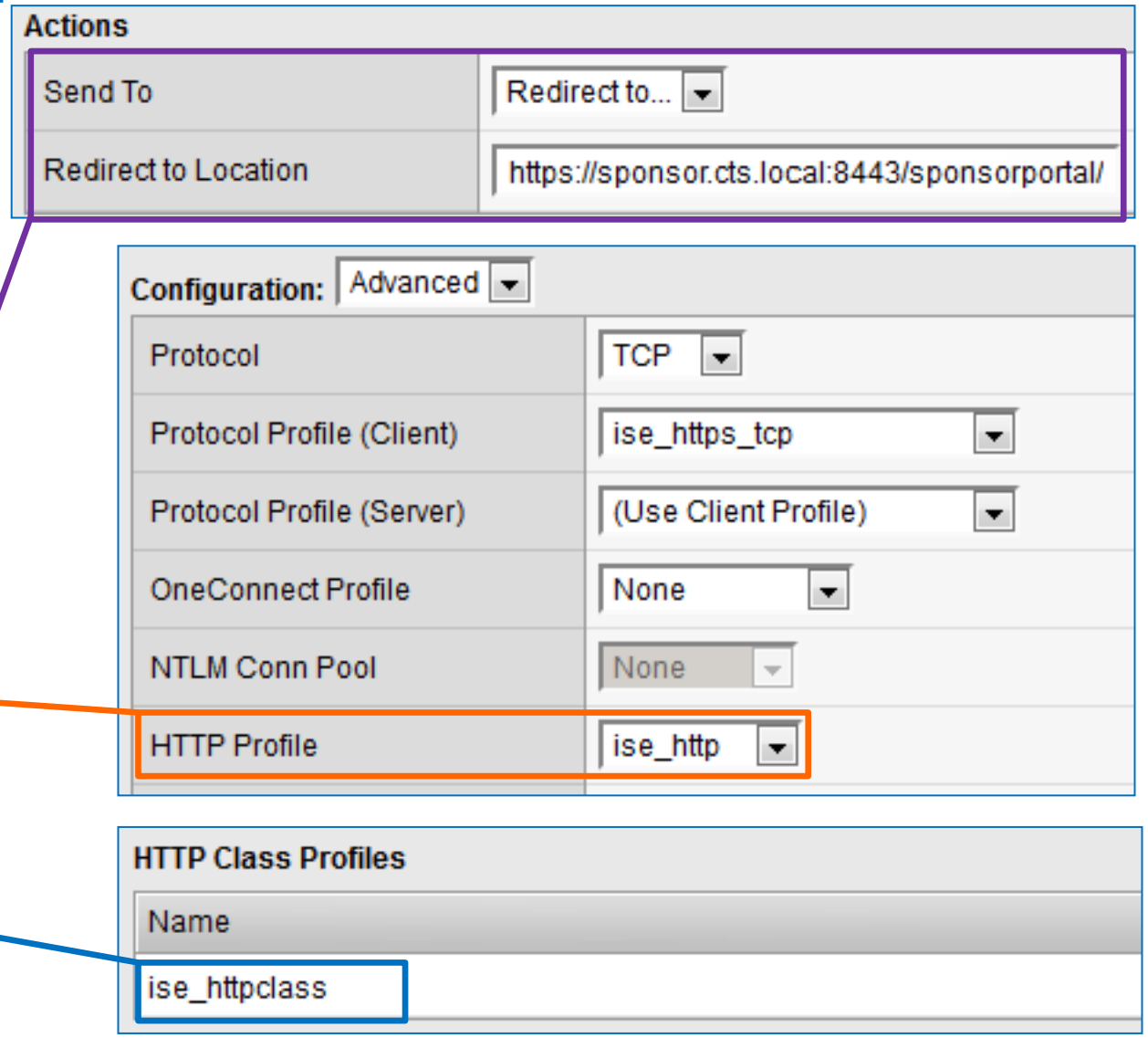


Configure Virtual Server for Web Portals on TCP/80

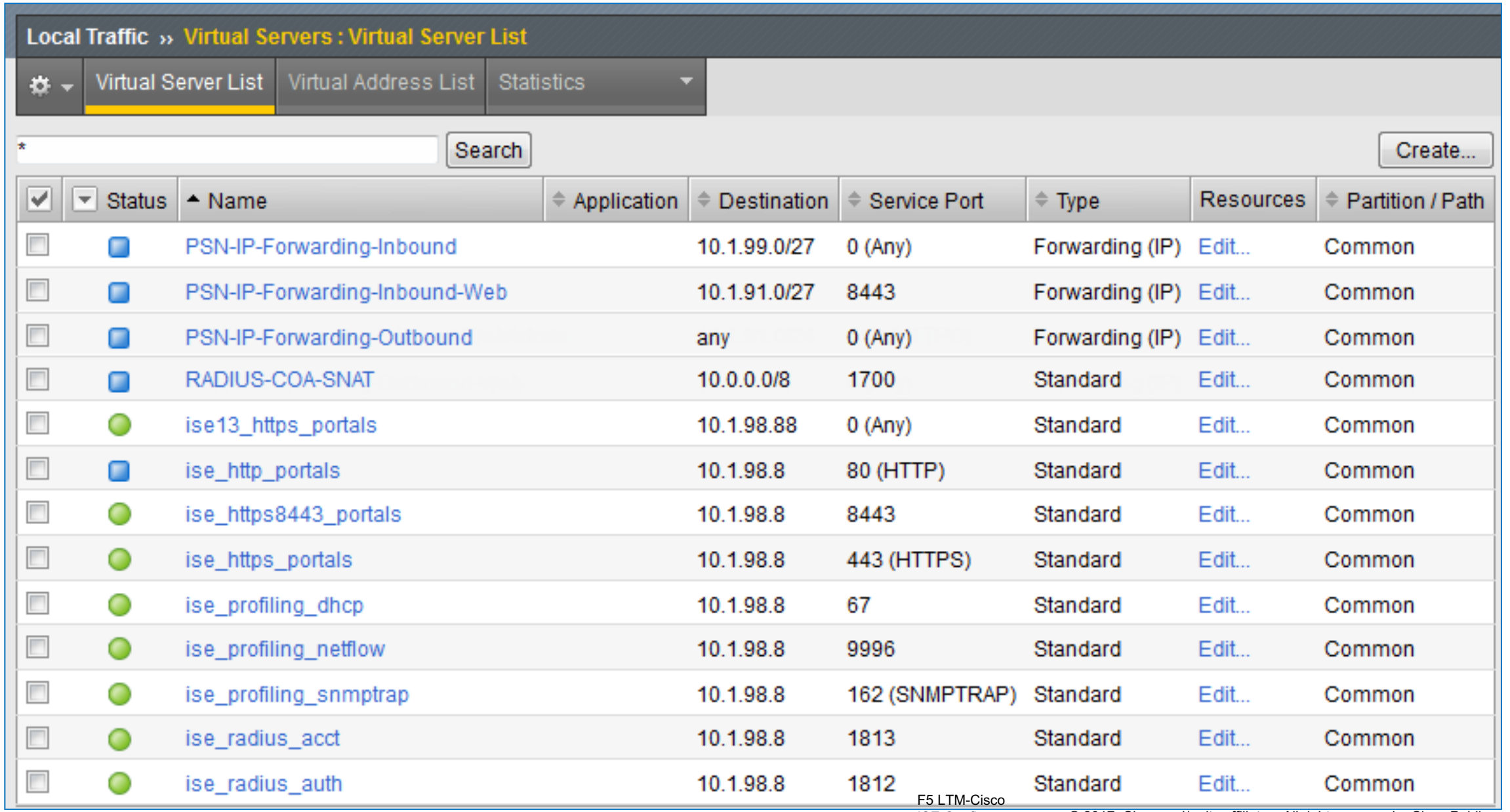
Optional HTTP -> HTTPS Redirect by F5 LTM

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.

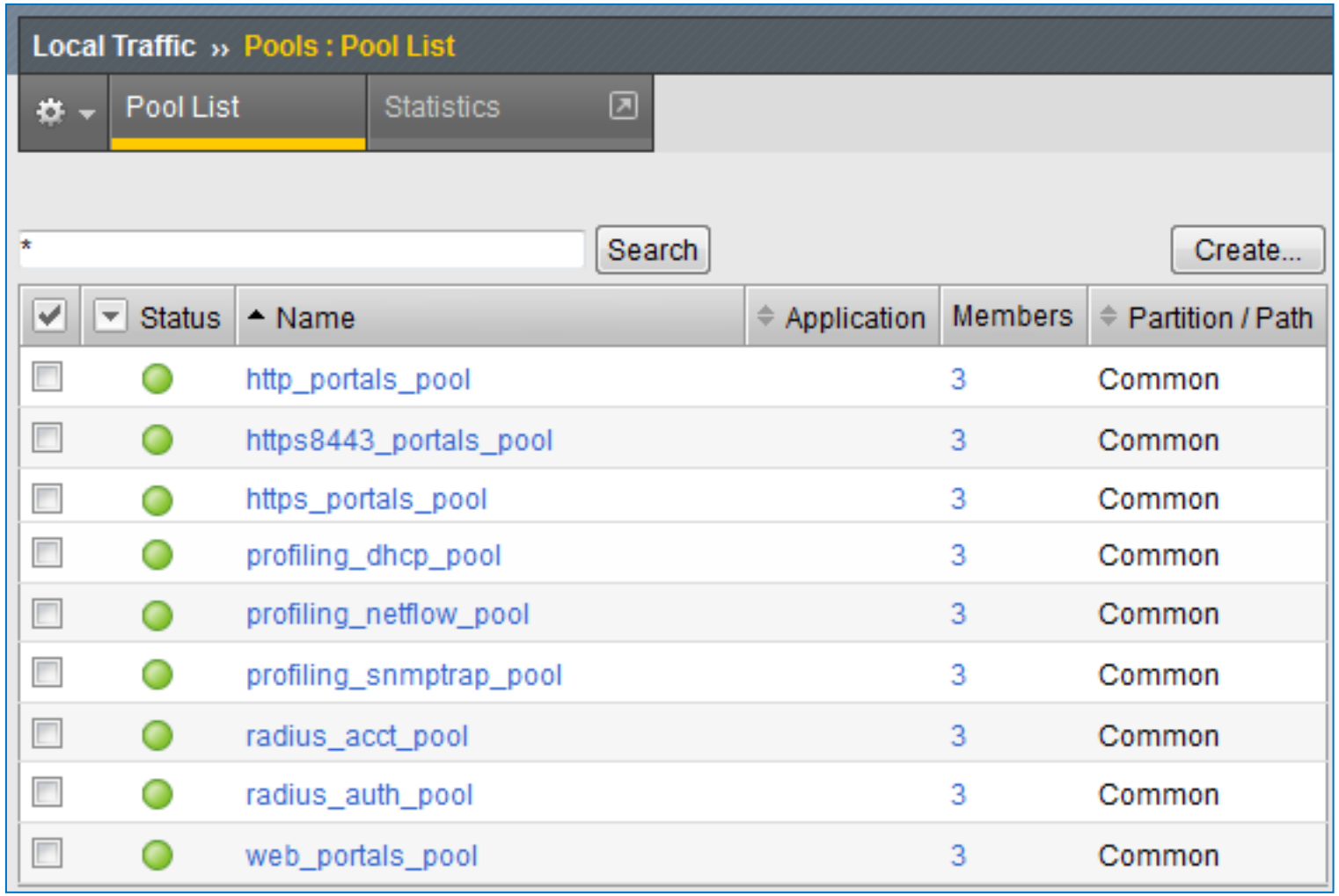


Virtual Server List



Status	Name	Application	Destination	Service Port	Type	Resources	Partition / Path
	PSN-IP-Forwarding-Inbound		10.1.99.0/27	0 (Any)	Forwarding (IP)	Edit...	Common
	PSN-IP-Forwarding-Inbound-Web		10.1.91.0/27	8443	Forwarding (IP)	Edit...	Common
	PSN-IP-Forwarding-Outbound		any	0 (Any)	Forwarding (IP)	Edit...	Common
	RADIUS-COA-SNAT		10.0.0.0/8	1700	Standard	Edit...	Common
	ise13_https_portals		10.1.98.88	0 (Any)	Standard	Edit...	Common
	ise_http_portals		10.1.98.8	80 (HTTP)	Standard	Edit...	Common
	ise_https8443_portals		10.1.98.8	8443	Standard	Edit...	Common
	ise_https_portals		10.1.98.8	443 (HTTPS)	Standard	Edit...	Common
	ise_profiling_dhcp		10.1.98.8	67	Standard	Edit...	Common
	ise_profiling_netflow		10.1.98.8	9996	Standard	Edit...	Common
	ise_profiling_snmptrap		10.1.98.8	162 (SNMPTRAP)	Standard	Edit...	Common
	ise_radius_acct		10.1.98.8	1813	Standard	Edit...	Common
	ise_radius_auth		10.1.98.8	1812	Standard	Edit...	Common

Server Pool List



Thank You