

Configuring Cisco ACE for Load Balancing Cisco Identity Service Engine (ISE)

Craig Hyps

Principal Technical Marketing Engineer, Cisco Systems

Sample ACE Configuration

Sample ACE Configuration...

Health Probes and Real Servers

- Define TCP or HTTP/S probe to verify web services active on configured HTTPS ports.

Guest/Sponsor SSL Settings

Admin Portal Settings
HTTP Port: 80
HTTPS Port: 443

Guest Portal Settings
HTTPS Port: 8443 (Valid Range 1 to 65535)

Sponsor Portal Settings
HTTPS Port: 8444 (Valid Range 1 to 65535)
 Default Sponsor Portal URL: sponsor.cts.local

My Devices Portal Settings
HTTPS Port: 8443 (Valid Range 1 to 65535)
 Default My Devices Portal URL: mydevices.cts.local

- Define RADIUS probe to verify AAA services
- Define real servers = Policy Service node real IP address for RADIUS / Web

```
probe tcp 8443-PROBE
port 8443
interval 30
passdetect interval 90
connection term forced
open 1
```

Simple example;
HTTP/S probe
recommended

```
probe radius PSN-PROBE
port 1812
interval 10
passdetect interval 90
credentials radprobe cisco123 secret cisco123
nas ip address 10.1.99.2
```

```
probe icmp ping
interval 15
passdetect interval 60
```

Sample ping probe

```
rserver host ise-psn-1
ip address 10.1.99.5
inservice

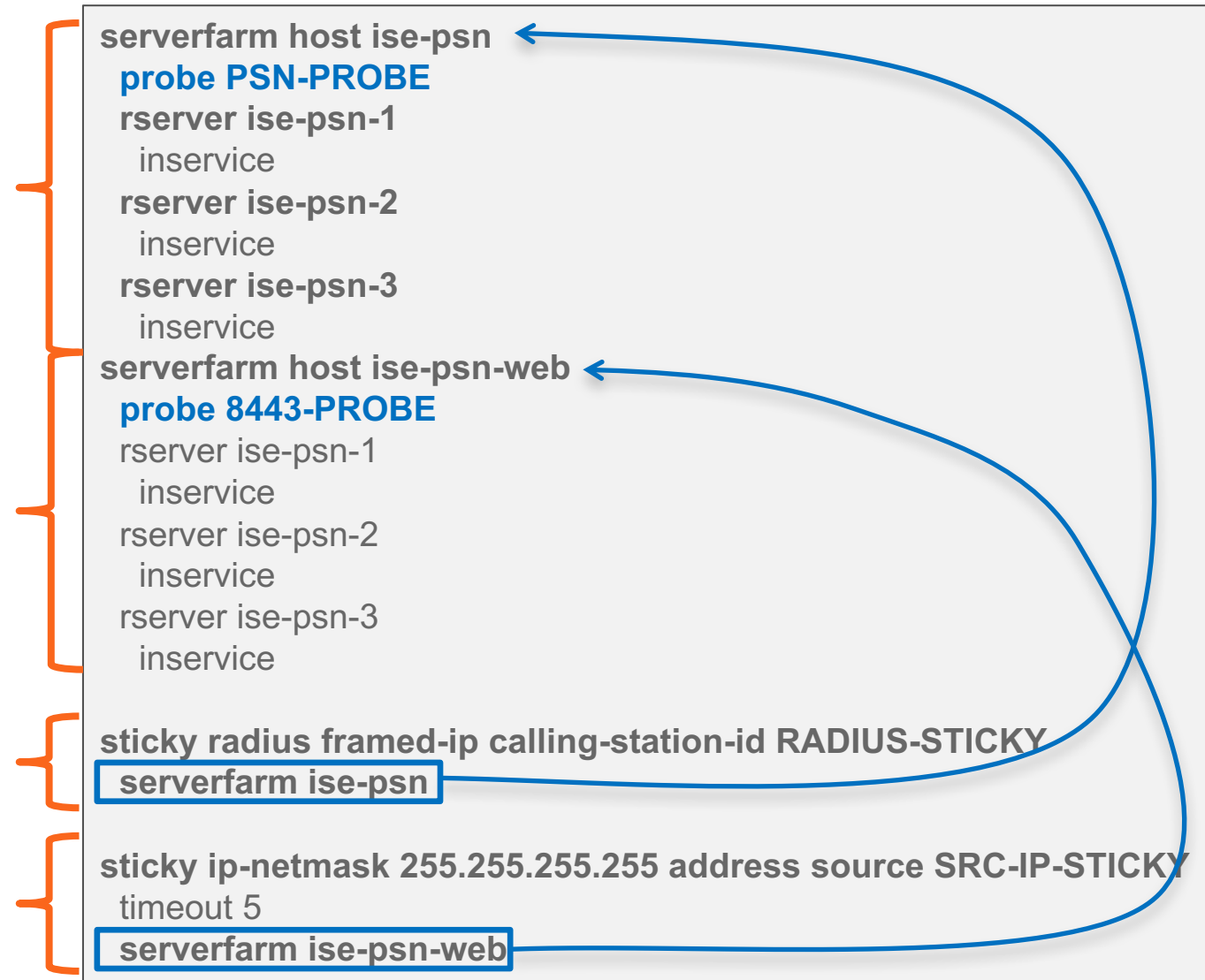
rserver host ise-psn-2
ip address 10.1.99.6
inservice

rserver host ise-psn-3
ip address 10.1.99.7
inservice
```

Sample ACE Configuration...

Server Farms and Sticky

- Define server farm for RADIUS services using RADIUS health probe
- Optionally define separate server farm for client HTTPS requests sent to LB VIP address (different health probe)
- RADIUS sticky based on Framed-IP-Address and Calling-Station-ID to ensure Auth and Acctng for same client stay with same PSN
- Simple Source IP sticky used for client web requests sent directly to LB VIP.



Sample ACE Configuration...

Class Maps to Define Matching VIP Traffic

- Profiling Services: Load balance DHCP (IP Helper) requests forwarded from client gateways (UDP/67)

- Note: To LB SNMP traps or NetFlow, add UDP/162 or UDP/9996, respectively to list of ports. Example:

class-map **match-any** PROFILER-CLASS

```
2 match virtual-address 10.1.98.10 udp eq 67
3 match virtual-address 10.1.98.10 udp eq 162
4 match virtual-address 10.1.98.10 udp eq 9996
```

- Configure VIP for HTTP/S ports used for direct access to PSN web services (Guest LWA, Sponsor, and MyDevices portals)

- Configure VIP for RADIUS Auth/Acctng

```
class-map match-all DHCP-CLASS
2 match virtual-address 10.1.98.10 udp eq 67

class-map match-any HTTPS-CLASS
2 match virtual-address 10.1.98.10 tcp eq http
3 match virtual-address 10.1.98.10 tcp eq https
4 match virtual-address 10.1.98.10 tcp eq 8443
5 match virtual-address 10.1.98.10 tcp eq 8444

class-map match-all RAD-L4-CLASS
2 match virtual-address 10.1.98.10 udp range 1812 1813
```

HTTP (tcp/80) allows redirect to secure HTTPS port.

Specific ports will depend on ISE configuration for web portal ports.

Sample ACE Configuration...

Policy Maps

- Map LB policies for RADIUS, DHCP (Profiling), and Web services to specific sticky server farms.

- Define general service policy to be applied to ACE client-side interface.

Maps VIPs to individual LB policies which point to sticky server farms.

Allows VIP to be pinged by clients

```
policy-map type loadbalance radius first-match RAD-L7-POLICY
class class-default
  sticky-serverfarm RADIUS-STICKY

policy-map type loadbalance generic first-match WEB-L4-POLICY
class class-default
  sticky-serverfarm SRC-IP-STICKY

policy-map type loadbalance generic first-match DHCP-L4-POLICY
class class-default
  sticky-serverfarm SRC-IP-STICKY

policy-map multi-match RAD-L4-POLICY
class RAD-L4-CLASS
  loadbalance vip inservice
  loadbalance policy RAD-L7-POLICY
  loadbalance vip icmp-reply
class HTTPS-CLASS
  loadbalance vip inservice
  loadbalance policy WEB-L4-POLICY
  loadbalance vip icmp-reply
class DHCP-CLASS
  loadbalance vip inservice
  loadbalance policy DHCP-L4-POLICY
  loadbalance vip icmp-reply
class class-default
```

Sample ACE Configuration...

Interfaces and Service Policies

- Optional ACL to define traffic permitted to/from each interface
- Client-facing interface—includes general service policy for LB services
- Server-facing interface
- Default route pointing to upstream L3 switch.

```
access-list ALL line 1 extended permit ip any any
```

```
interface vlan 98
```

```
description ACE
```

```
ip address 10.1.98.2 255.255.255.0
```

```
access-group input ALL
```

```
service-policy input RAD-L4-POLICY
```

```
no shutdown
```

```
interface vlan 99
```

```
description CLUSTER
```

```
ip address 10.1.99.1 255.255.255.0
```

```
alias 10.1.99.2 255.255.255.0
```

```
mac-sticky enable
```

```
no icmp-guard
```

```
access-group input ALL
```

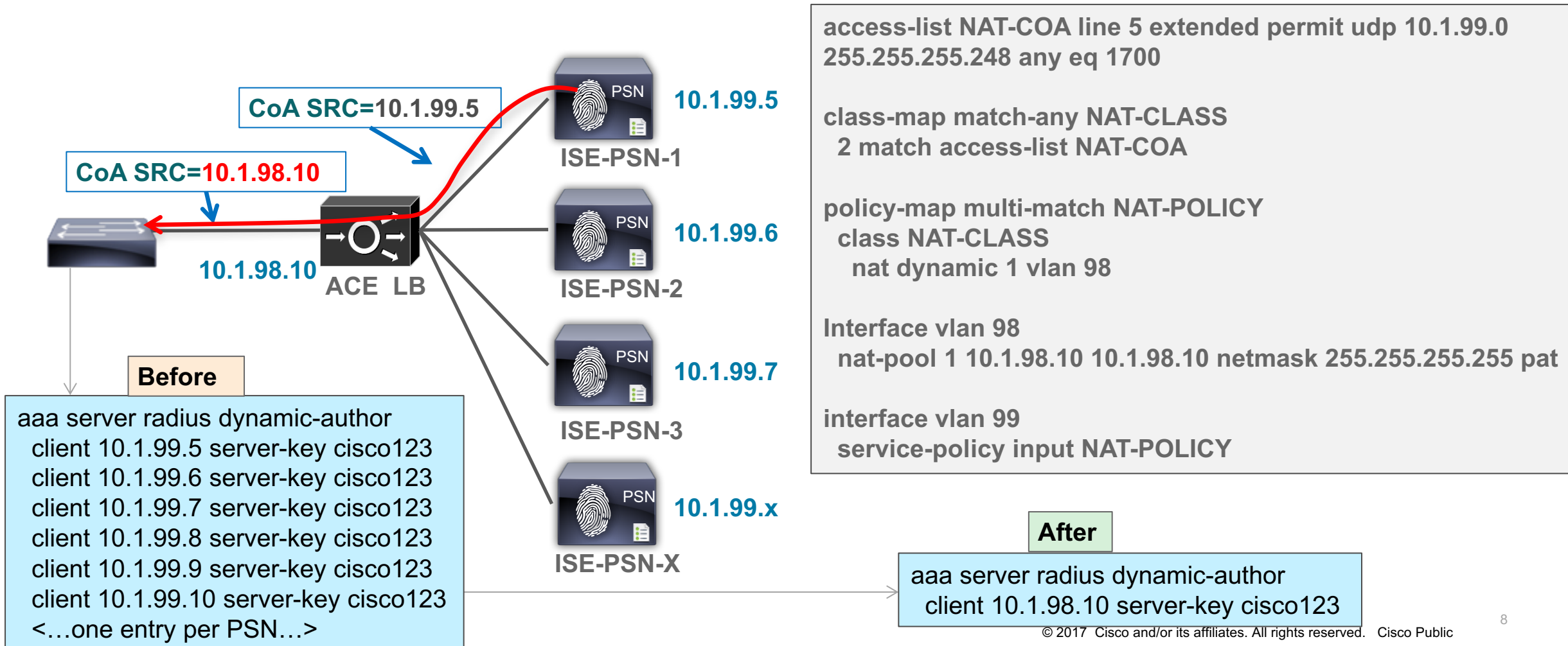
```
no shutdown
```

```
ip route 10.1.0.0 255.255.0.0 10.1.98.1
```

Sample ACE Configuration...

Allow NAT of PSN CoA Requests

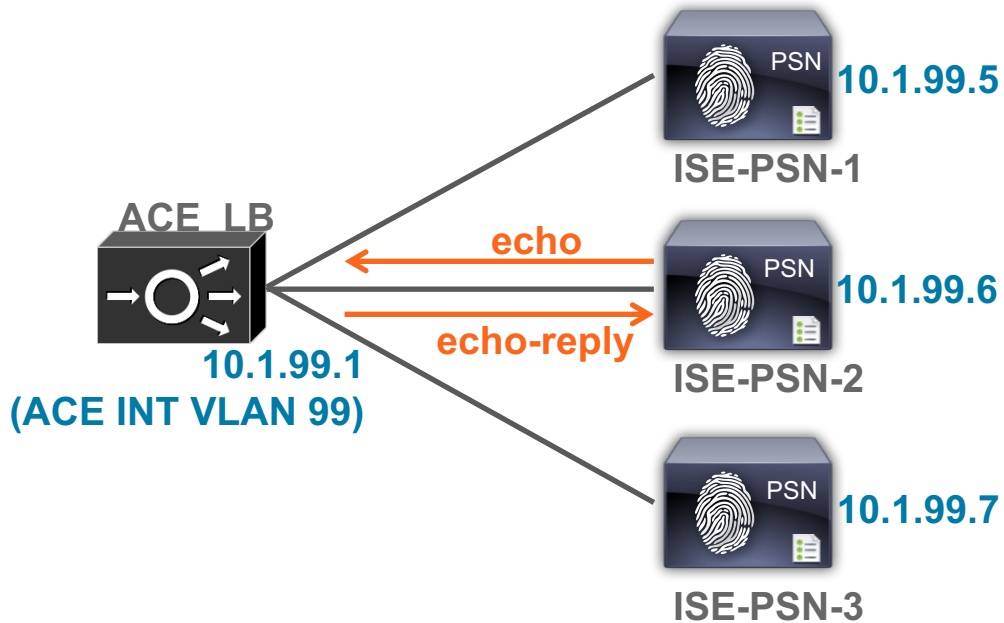
- Match traffic from PSNs to UDP/1700 (RADIUS CoA) and translate to PSN cluster VIP.



Sample ACE Configuration...

Allow Ping for ISE PSNs / UDP Connection Timer

- Allow ISE nodes to ping default gateway. Otherwise, install fails!



- Optionally set UDP connection timeout to match switch RADIUS timeout; assign to RADIUS LB connections.

```
class-map type management match-any remote_access
  2 match protocol icmp any
```

```
policy-map type management first-match
  remote_mgmt_allow_policy
  class remote_access
    permit
```

```
interface vlan 99
  service-policy input remote_mgmt_allow_policy
```

```
parameter-map type connection UDP_CONN
  set timeout inactivity 30
```

```
policy-map multi-match RAD-L4-POLICY
  class RAD-L4-CLASS
    connection advanced-options UDP_CONN
```

Thank You