
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Mastering ISE Posture: Ensuring Compliance and Tackling Common Challenges

Identity Services Engine (ISE)

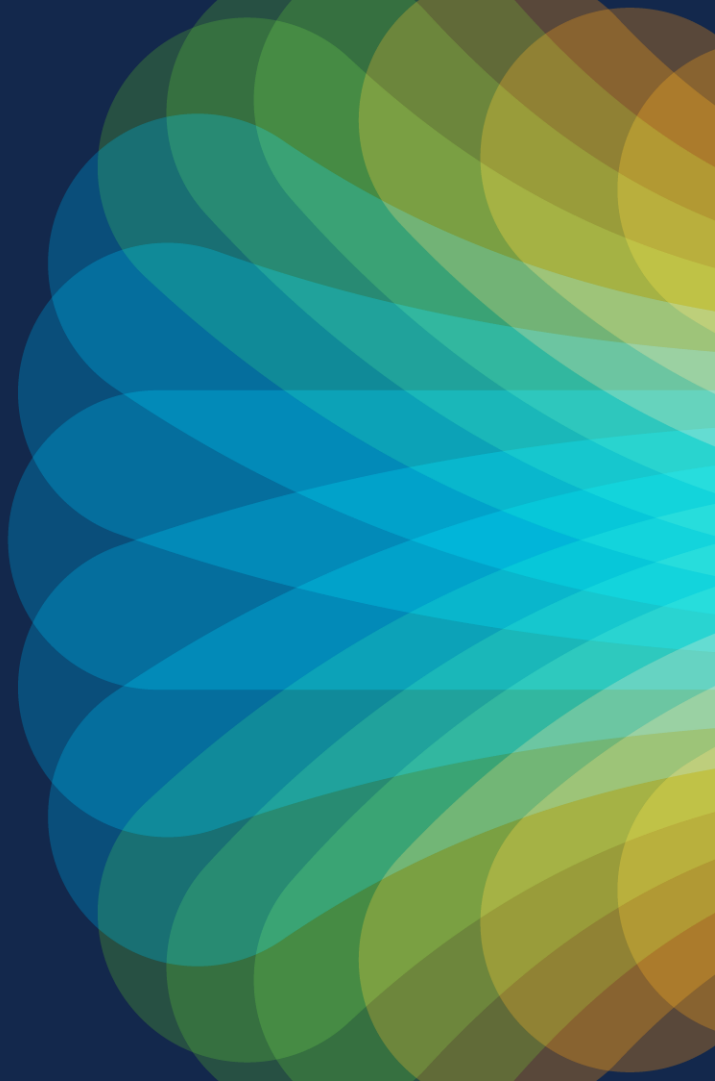
Michael Zilligen – Technical Consulting Engineer

TACSEC-2005

Agenda

- Introduction
- Posture Workflow Review
- Troubleshooting “No Policy Server Detected”
- Troubleshooting “Posture Pending state” on ISE
- Q&A

Posture Workflow Review



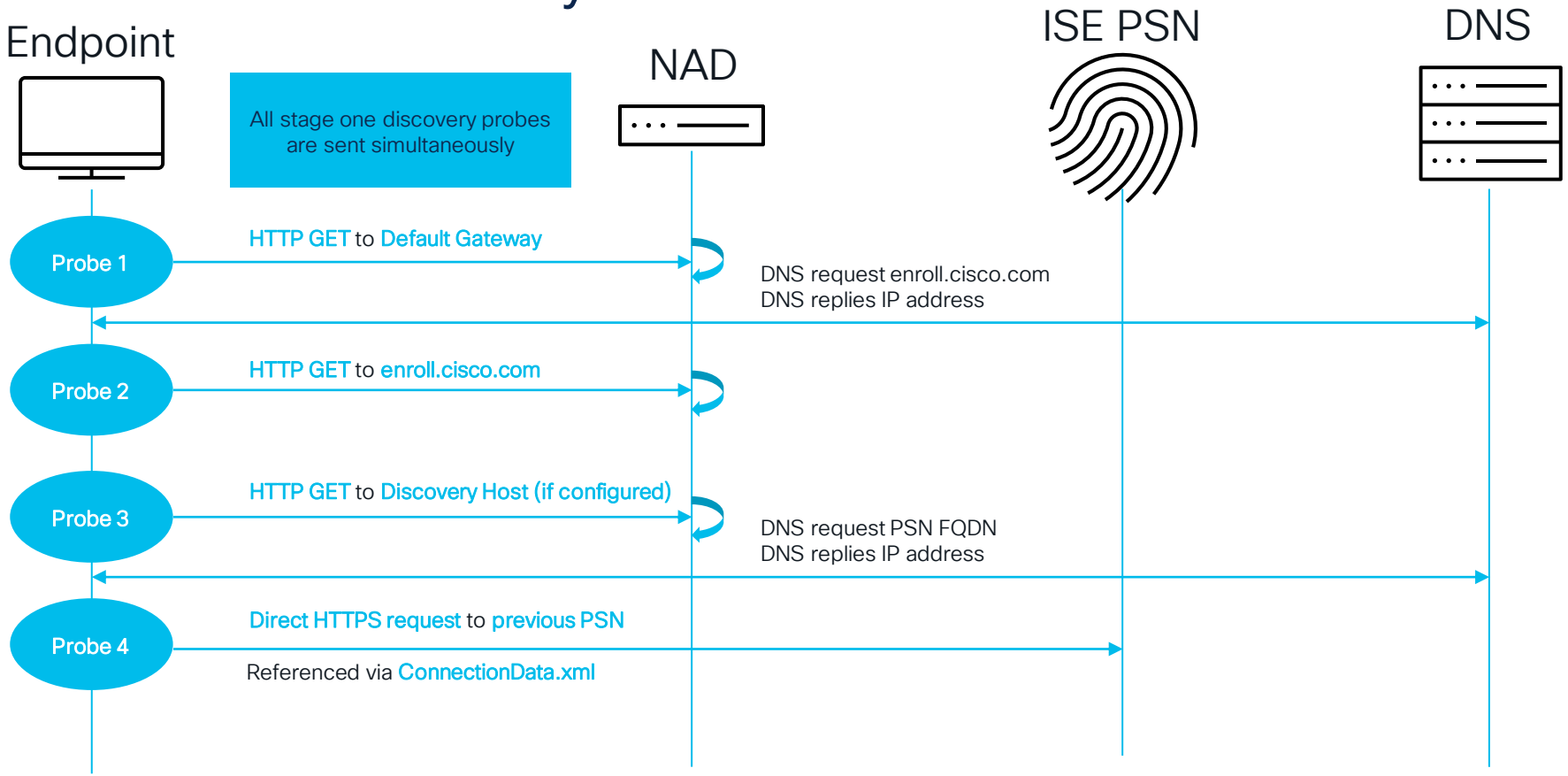
Redirect

- Uses stage one HTTP probes to discover ISE
- Endpoints do not need ISEPostureCFG.xml predeployed
- Discovery host probe configured on the ISE posture profile
- Users will be redirected to the CPP

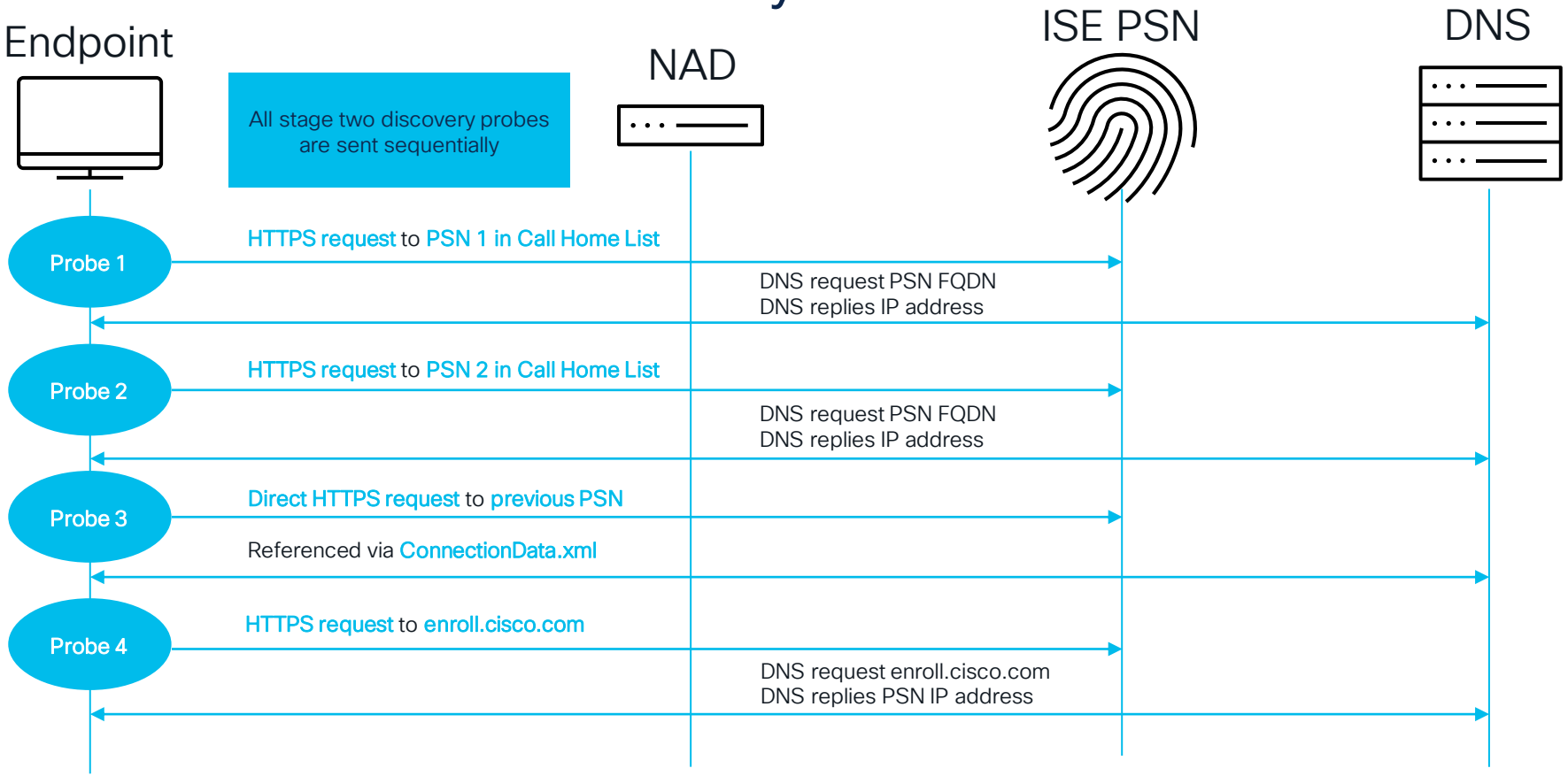
Redirectionless

- Uses stage two HTTPS probes to discover ISE
- Endpoints need to have ISEPostureCFG.xml predeployed or access to CPP FQDN
- Probes configured in call-home list on the ISE posture profile

Redirect Discovery Probes



Redirectionless Discovery Probes



Redirect Flow Example – Logs Example

- 2023/04/27 09:15:44 [Information] aciseagent Function: SwiftHttpRunner::startNoMntStageDiscovery Thread Id: 0xBEC File: swifthttprunner.cpp Line: 766 Level: debug MSG_NS_INTERFACE_CHANGE, Starting HTTP Discovery
- 2023/04/27 09:15:44 [Information] aciseagent Function: HttpConnection::MakeRequest Thread Id: 0x1398 File: httpconnection.cpp Line: 542 Level: debug Redirected url https://ise32.test.com:8443/portal/gateway?sessionId=0e24f33c0002b000644a9fa9&portal=df7fd7aa-d311-4a6c-b6e5-306acd2ebcef&action=cpp&token=f8e99e100042fcdbe5f5beffdf1d60fc
- 2023/04/27 09:15:44 [Information] aciseagent Function: Target::probeDiscoveryUrl Thread Id: 0x1398 File: target.cpp Line: 261 Level: debug GET request to URL (http://enroll.cisco.com/auth/discovery), returned status 0 <Operation Success.>
- 2023/04/27 09:15:45 [Information] aciseagent Function: SwiftManager::sendUIStatus Thread Id: 0xBEC File: swiftmanager.cpp Line: 186 Level: debug MSG_SU_STEP_STATUS, {Status:3,Compliant:3,RemStatus:11337728,Phase:0,StepNumber:-1,Progress:2,Attention:0,Cancellable:0,Restartable:0,ErrorMessage:0,Description1:"Downloading ISE Posture Profile - 100%",Description2:""}.

Redirect Flow Example - Logs Example

- 2023/04/27 09:15:45 [Information] aciseagent Function: SwiftManager::sendUIStatus Thread Id: 0xBEC File: swiftmanager.cpp Line: 186 Level: debug MSG_SU_STEP_STATUS, {Status:3,Compliant:3,RemStatus:11337728,Phase:0,StepNumber:-1,Progress:6,Attention:0,Cancellable:0,Restartable:0,ErrorMessage:0,Description1:"Performing any required updates...",Description2:""}.
- 2023/04/27 09:15:51 [Information] aciseagent Function: SMNav::logTransition Thread Id: 0xBEC File: smnav.cpp Line: 167 Level: info New State = PM_SND_POSTURE_RESP, New Event = EV_SND_POSTURE_RPT
- 2023/04/27 09:15:56 [Information] aciseagent Function: Authenticator::sendUIStatus Thread Id: 0xBEC File: authenticator.cpp Line: 1905 Level: debug MSG_SU_STEP_STATUS, {Status:4,Compliant:2,RemStatus:2,Phase:0,StepNumber:-1,Progress:-1,Attention:1,Cancellable:0,Restartable:0,ErrorMessage:0,Description1:"Compliant.",Description2:"Network access allowed."}.

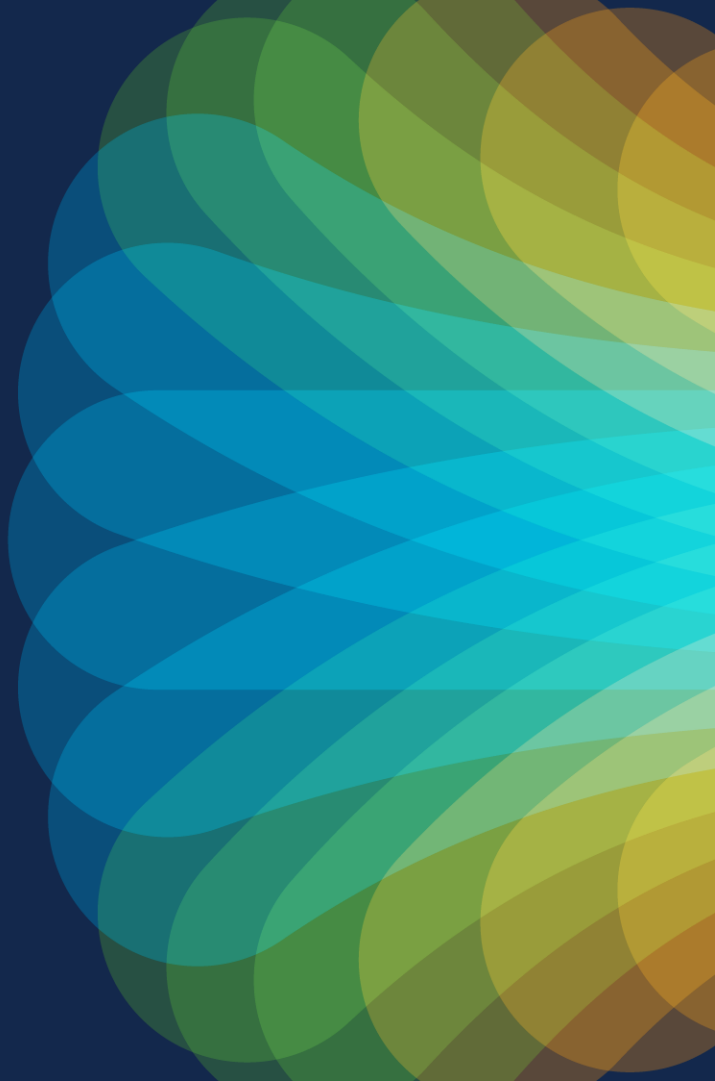
Redirectionless Flow Example - Logs Example

- 2023/05/02 15:55:57 [Information] aciseagent Function: SwiftHttpRunner::probeNextMntTarget Thread Id: 0x10B4 File: swifthttprunner.cpp Line: 1652 Level: debug Probing Mnt stage Ng-Discovery target ise32.test.com with path /auth/ng-discovery.
- 2023/05/02 15:55:57 [Information] aciseagent Function: HttpConnection::MakeRequest Thread Id: 0x1448 File: httpconnection.cpp Line: 330 Level: debug Url=https://ise32.test.com:8443/auth/ng-discovery
- 2023/05/02 15:55:58 [Information] aciseagent Function: Target::fetchPostureStatus Thread Id: 0x1448 File: target.cpp Line: 451 Level: debug POST request to URL (https://ise32.test.com:8443/auth/ng-discovery), returned status 0 <Operation Success.>, stage 2
- 2023/05/02 15:55:58 [Information] aciseagent Function: SwiftManager::sendUIStatus Thread Id: 0x10B4 File: swiftmanager.cpp Line: 186 Level: debug MSG_SU_STEP_STATUS, {Status:3,Compliant:3,RemStatus:4131024,Phase:0,StepNumber:-1,Progress:2,Attention:0,Cancellable:0,Restartable:0,ErrorMessage:0,Description1:"Downloading ISE Posture Profile - 100%",Description2:""}

Redirectionless Flow Example - Logs Example

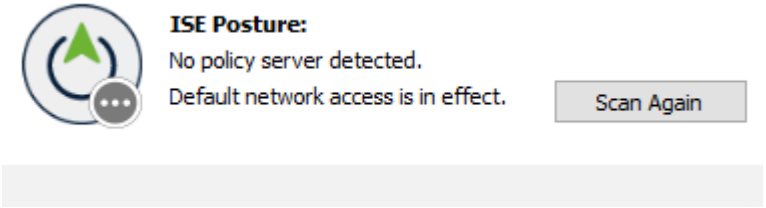
- 2023/05/02 15:55:58 [Information] aciseagent Function: SwiftManager::sendUIStatus Thread Id: 0x10B4 File: swiftmanager.cpp Line: 186 Level: debug MSG_SU_STEP_STATUS, {Status:3,Compliant:3,RemStatus:4131024,Phase:0,StepNumber:-1,Progress:6,Attention:0,Cancellable:0,Restartable:0,ErrorMessage:0,Description1:"Performing any required updates...",Description2:""}.
- 2023/05/02 15:55:58 [Information] aciseagent Function: SMNav::logTransition Thread Id: 0x10B4 File: smnav.cpp Line: 220 Level: info New State = PM_SND_POSTURE_RESP, New Event = EV_SND_POSTURE_RPT
- 2023/05/02 15:55:58 [Information] aciseagent Function: Authenticator::sendUIStatus Thread Id: 0x10B4 File: authenticator.cpp Line: 1905 Level: debug MSG_SU_STEP_STATUS, {Status:4,Compliant:2,RemStatus:1,Phase:0,StepNumber:-1,Progress:-1,Attention:1,Cancellable:0,Restartable:0,ErrorMessage:0,Description1:"Compliant.",Description2:"Network access allowed."}.

Troubleshooting No Policy Server Detected



No Policy Server Detected and Why It Happens

- The Posture Module was unable to discover a PSN to start posture
  - Redirect-ACL is not correct or ISEPostureCFG.xml in a redirectionless environment
  - Port 8443 not open (this is the default CPP port and is customizable)
  - DNS resolution issues



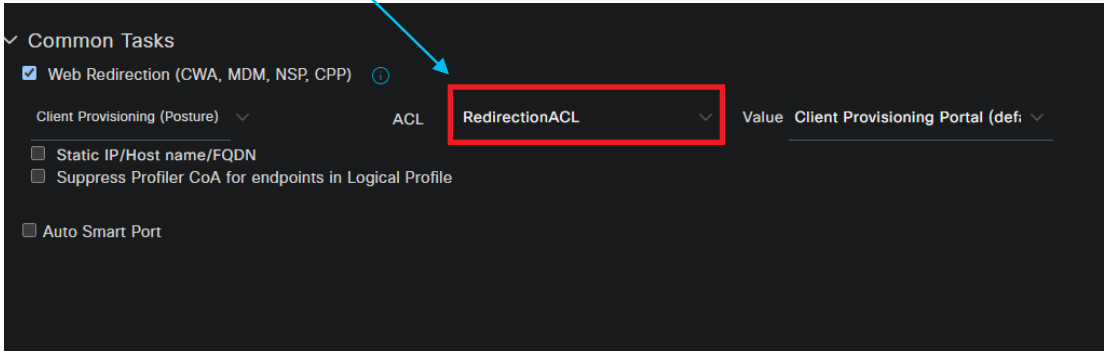
Troubleshooting – Redirect Issues Checklist

- Verify Redirect-ACL Configuration on the NAD
- If an endpoint tries to access 72.163.1.80, are they redirected?
- Verify http-server is enabled on the NAD/sh run | include http
- Verify http discovery probes are sent by endpoint

Troubleshooting – Redirect Issues

- Verify the Redirection ACL's name on the NAD matches what is configured on the ISE Authorization Profile

```
asa# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list RedirectionACL  6 elements; name hash: 0x7ea19faf
access-list RedirectionACL line 1 extended deny udp any any eq domain (hitcnt=32847) 0xd3732145
access-list RedirectionACL line 2 extended deny icmp any any (hitcnt=1494) 0x63581429
access-list RedirectionACL line 3 extended deny udp any any eq bootps (hitcnt=0) 0xfd9b2e98
access-list RedirectionACL line 4 extended deny udp any any eq bootpc (hitcnt=0) 0x05ab0b88
access-list RedirectionACL line 5 extended permit tcp any any eq www (hitcnt=1249) 0x77ca97b9
access-list RedirectionACL line 6 extended deny ip any host 14.36.243.51 (hitcnt=704) 0xcfcb7769
asa#
```



Troubleshooting – Redirect Issues

- Verify the Redirection ACL's configuration
- Redirection should be triggered only for HTTP traffic
- Discovery Host should not be a PSN IP address; it should be any address the endpoint can resolve that will trigger redirection

Example ASA Configuration:

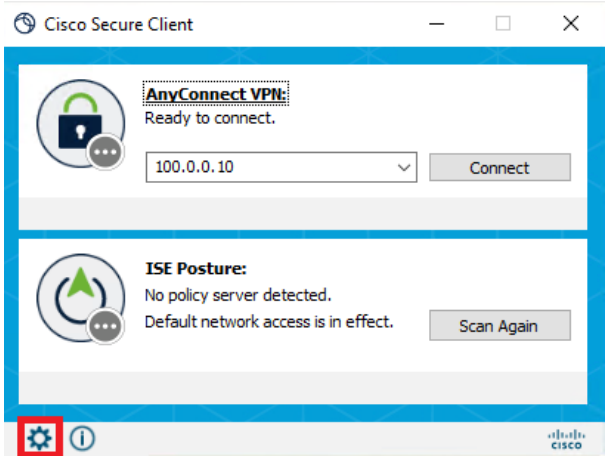
```
access-list RedirectionACL extended deny ip any host <PSN_IP>
access-list RedirectionACL extended deny udp any any eq domain
access-list RedirectionACL extended deny udp any any eq bootps
access-list RedirectionACL extended deny udp any any eq bootpc
access-list RedirectionACL extended permit tcp any any eq www
```

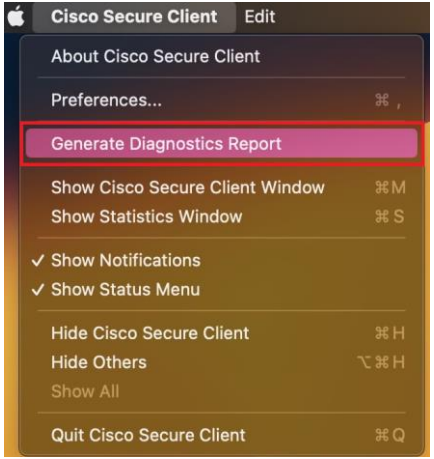
Example Switch Configuration:
Note: AireOS controllers will be configured the exact opposite

```
Extended IP access list RedirectionACL
deny ip any host <PSN_IP>
deny udp any any eq domain
deny udp any any eq bootps
deny udp any any eq bootpc
permit tcp any any eq www
```

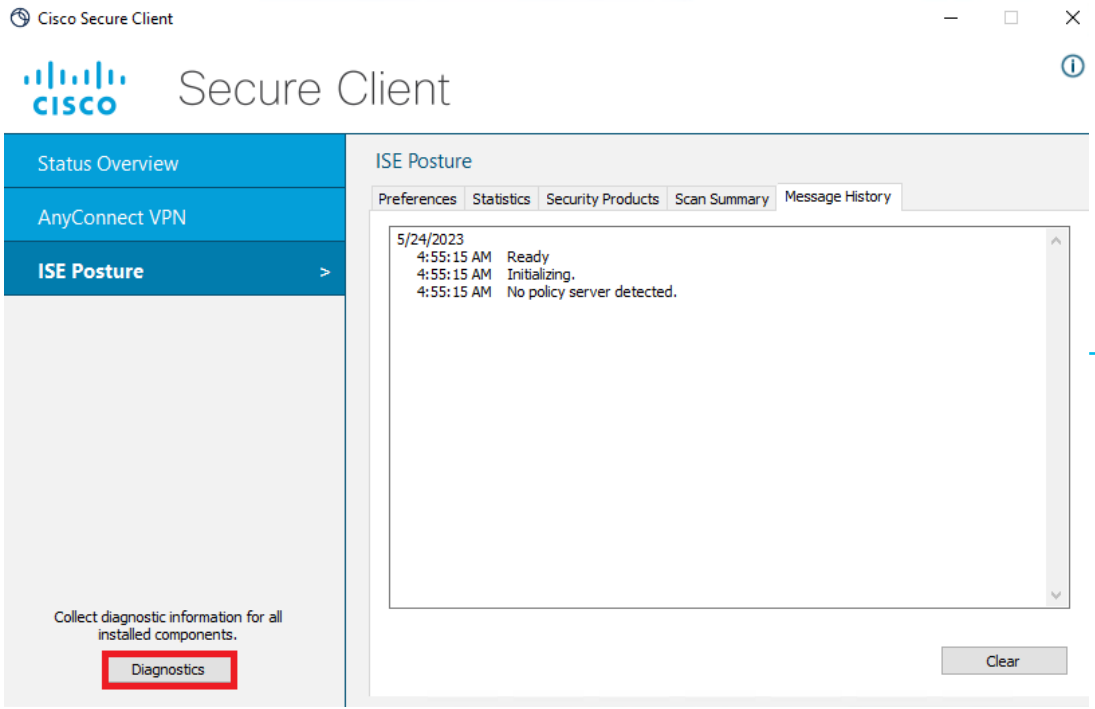
Troubleshooting – No Policy Server Detected

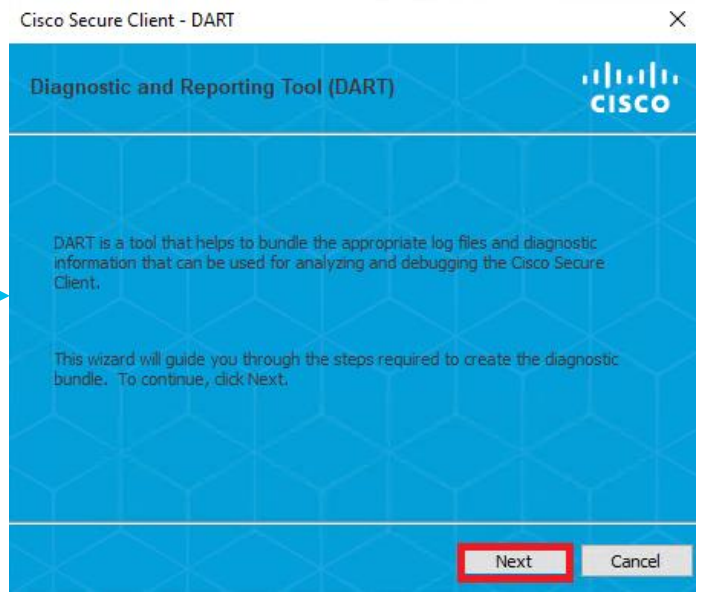
- Using a Diagnostics and Reporting Tool bundle or "DART" we can determine what is happening during the posture process
- Bulk of log analysis will be in "AnyConnect_ISEPosture.txt" located in the "ISE Posture -> Logs" folder (system.log on MAC)
- AnyConnectVPN.txt is useful for certificate issues or failed to launch downloader issues when performing posture over VPN



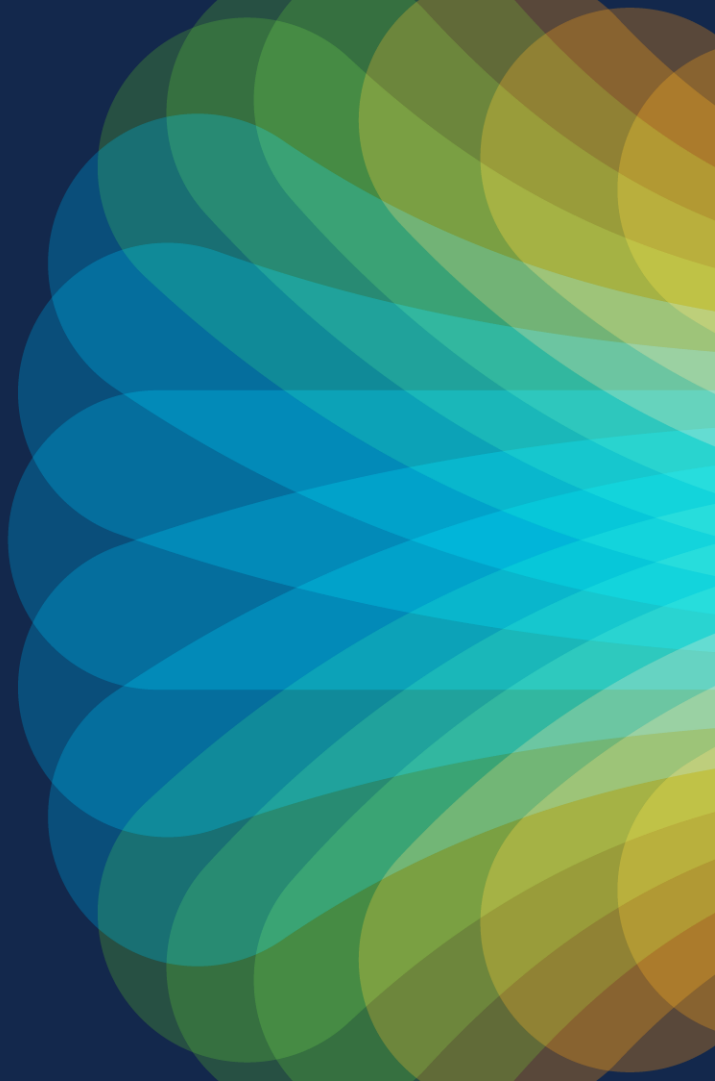


Generate a DART Bundle

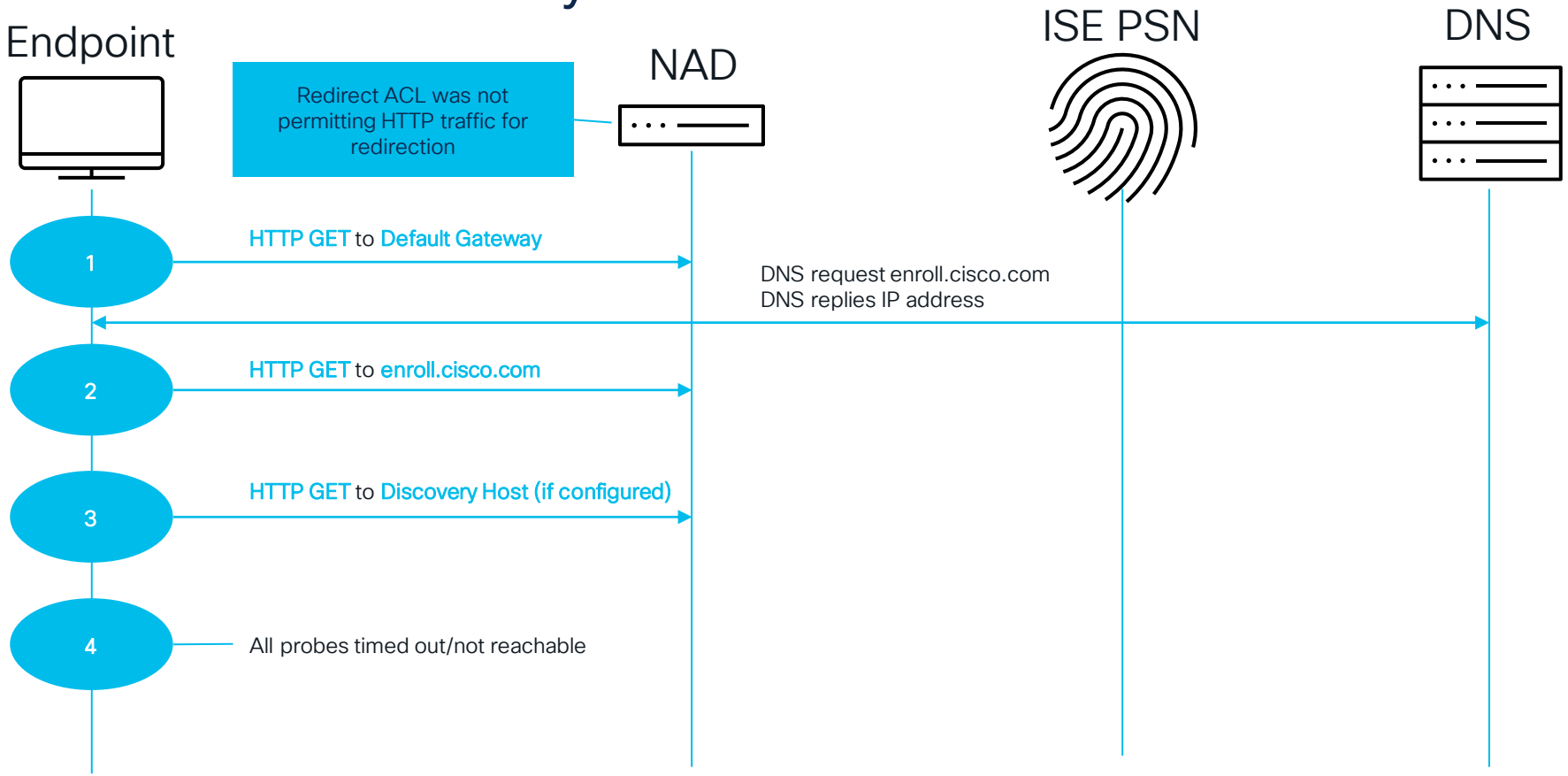




Scenario 1
Redirect ACL Misconfiguration



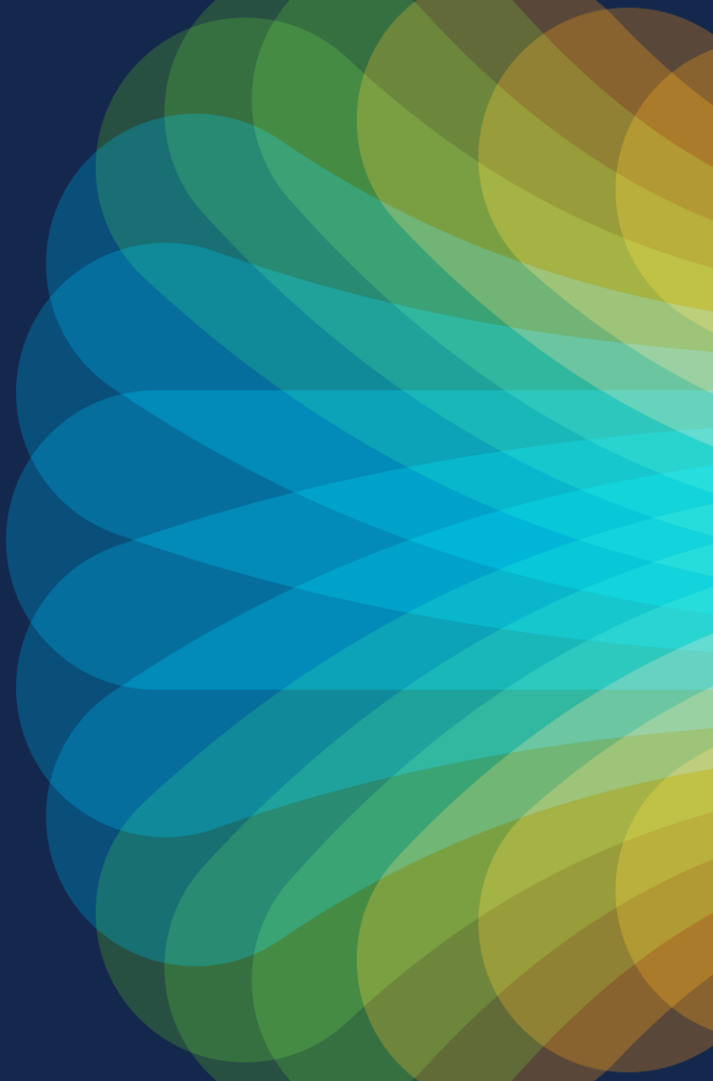
Redirect Discovery Probes



Troubleshooting – Redirect Issues

- Check“AnyConnect_ISEPosture.txt” from the DART bundle
- 2023/04/27 07:55:24 [Information] aciseagent Function: SwiftHttpRunner::startNoMntStageDiscovery Thread Id: 0x1404 File: swifthttprunner.cpp Line: 766 Level: debug MSG_NS_INTERFACE_CHANGE, Starting HTTP Discovery
- 2023/04/27 07:55:24 [Information] aciseagent Function: HttpConnection::MakeRequest Thread Id: 0x638 File: httpconnection.cpp Line: 330 Level: debug Url=http://14.36.1.1/auth/discovery
- 2023/04/27 07:55:24 [Information] aciseagent Function: HttpConnection::MakeRequest Thread Id: 0x1B38 File: httpconnection.cpp Line: 330 Level: debug Url=http://enroll.cisco.com/auth/discovery
- 2023/04/27 07:55:24 [Information] aciseagent Function: Target::Probe Thread Id: 0x1B38 File: target.cpp Line: 212 Level: debug Status of Redirection target enroll.cisco.com is 6 <Not Reachable.>
- 2023/04/27 07:55:24 [Information] aciseagent Function: Target::Probe Thread Id: 0x638 File: target.cpp Line: 212 Level: debug Status of Redirection target 14.36.1.1 is 6 <Not Reachable.>

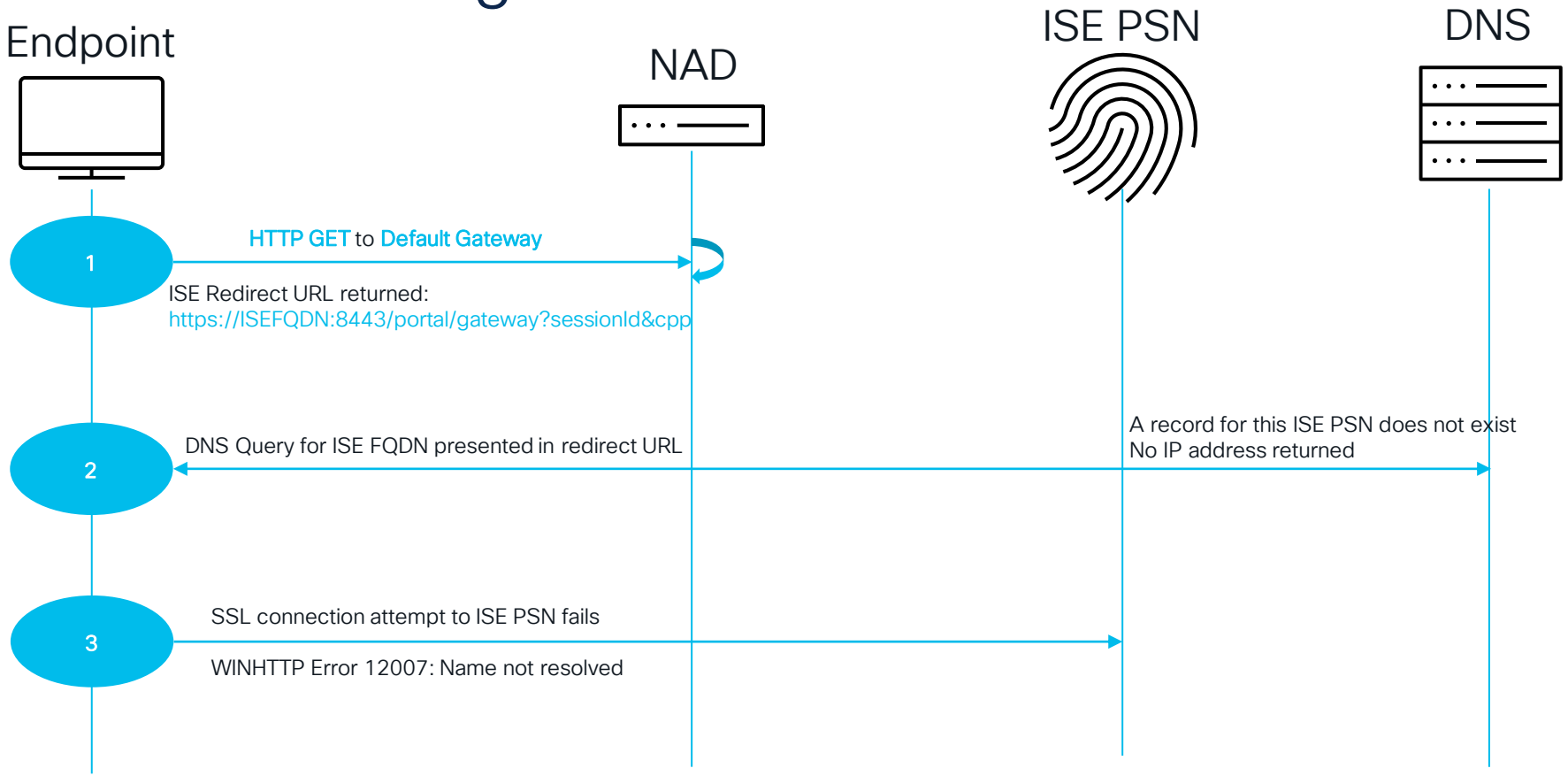
Scenario 2
DNS Issues



Troubleshooting – DNS Issues

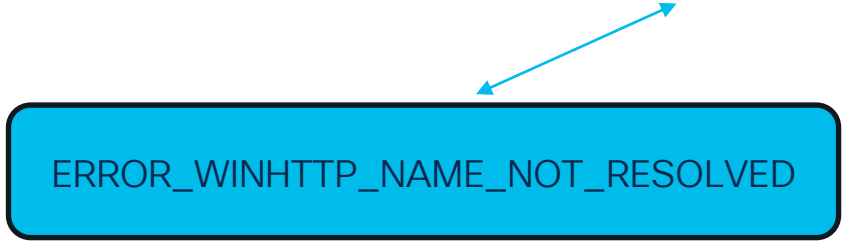
- Verify we're not redirecting DNS traffic on the NAD
- Ensure we're allowing DNS traffic on ISE through the DACL being pushed
- Confirm forward/reverse lookup is successful and A/PTR records exist for ISE on the DNS server

Troubleshooting – DNS Issues

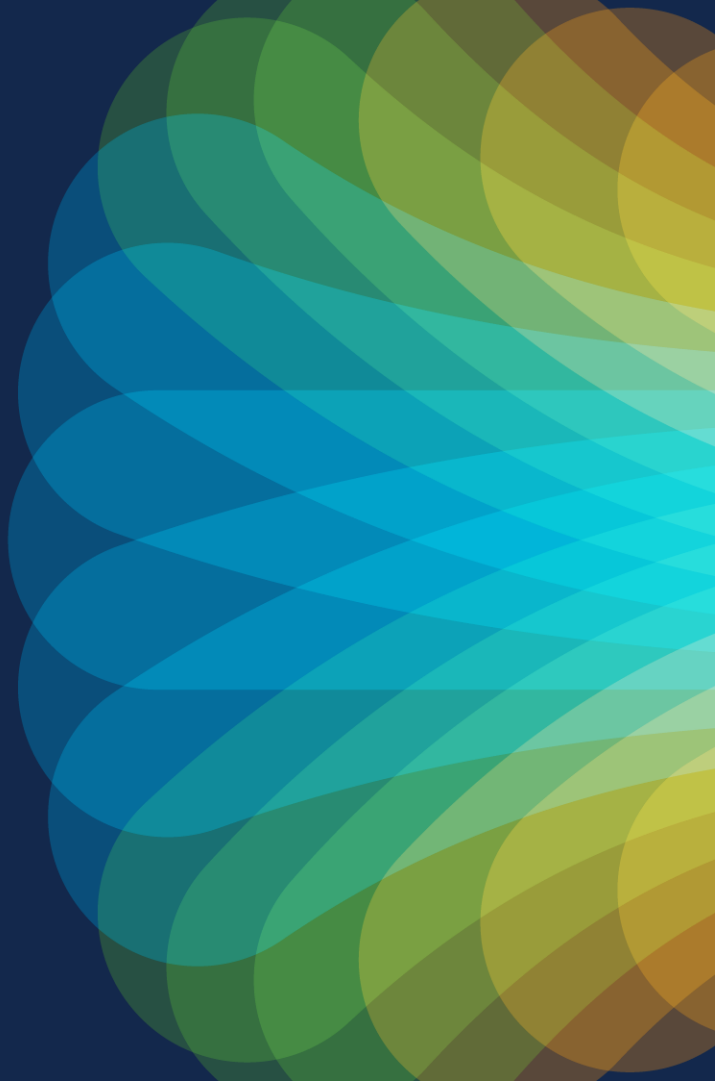


Troubleshooting – DNS Issues

- Check “AnyConnect_ISEPosture.txt” from the DART bundle
- 2023/04/26 06:01:55 [Information] aciseagent Function: SwiftHttpRunner::startNoMntStageDiscovery Thread Id: 0xD70 File: swifthttprunner.cpp Line: 766 Level: debug MSG_NS_INTERFACE_CHANGE, Starting HTTP Discovery
- 2023/04/26 06:01:56 [Information] aciseagent Function: HttpConnection::MakeRequest Thread Id: 0x16C4 File: httpconnection.cpp Line: 542 Level: debug Redirected url https://ise32.test.com:8443/portal/gateway?sessionId=0e24f33c00026000644920bd&portal=df7fd7aa-d311-4a6c-b6e5-306acd2ebcef&action=cpp&token=ec2e4e9458f97596e7b2c9d6e708f88a
- 2023/04/26 06:01:56 [Information] aciseagent Function: hs_transport_winhttp_get Thread Id: 0x16C4 File: hs_transport_winhttp.c Line: 4829 Level: debug unable to send request: 12007



Scenario 3
Probes not being tunneled



Troubleshooting – Probes Not Being Tunneled

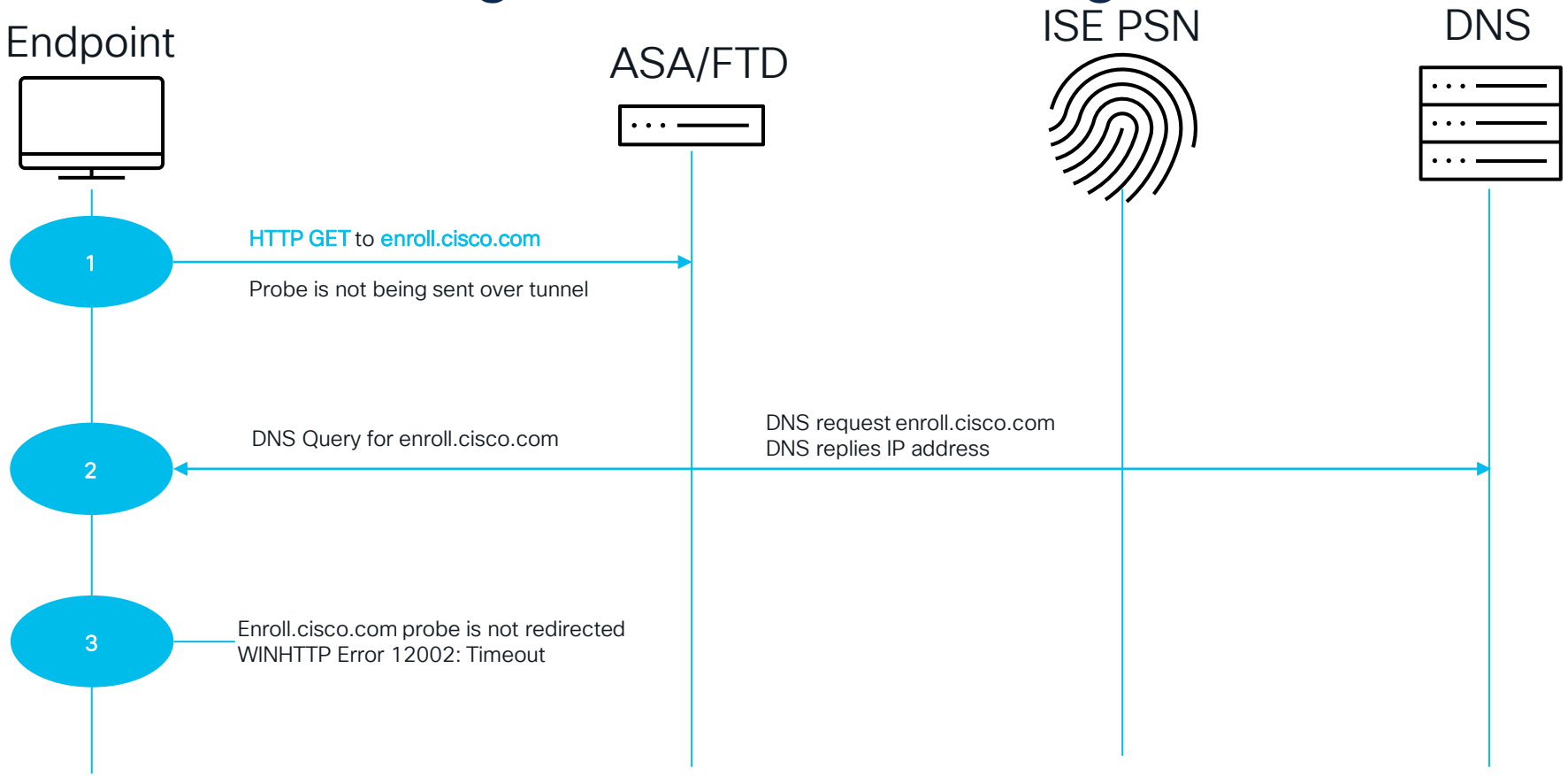
- In split-tunnel configurations, we should permit enroll.cisco.com/discovery host probes in the tunnel
- Default gateway probe will not be sent on MAC OS devices

Example ASA Configuration:

access-list Split_Tunnel_ACL standard permit host 72.163.1.80
access-list Split_Tunnel_ACL standard permit host <discovery host>

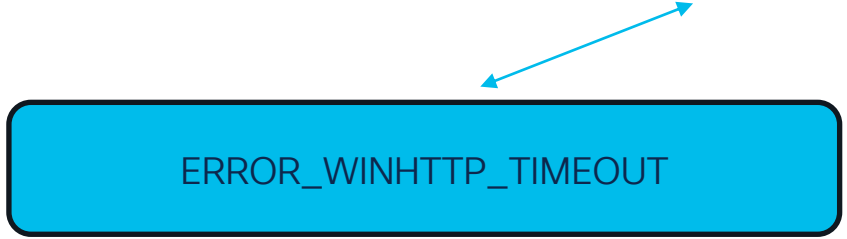
group-policy <name> attributes
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Split_Tunnel_ACL

Troubleshooting – Probes Not Being Tunneled

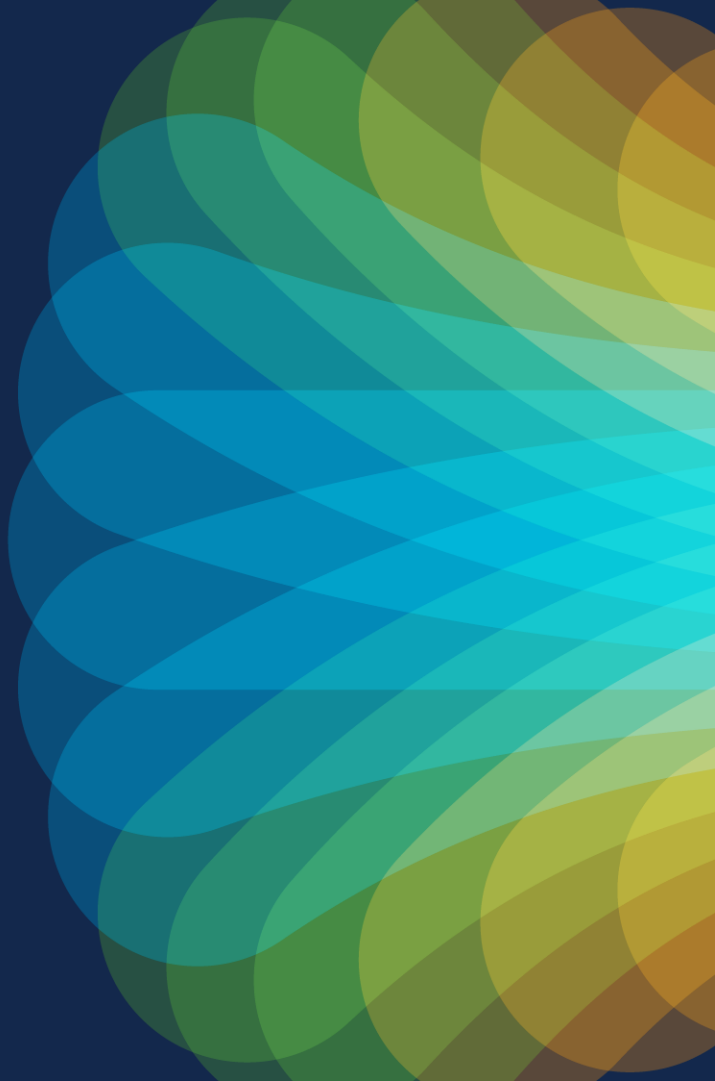


Troubleshooting – Probes Not Being Tunneled

- Check “AnyConnect_ISEPosture.txt” from the DART bundle
- 2023/05/03 12:27:42 [Information] aciseagent Function: SwiftHttpRunner::startNoMntStageDiscovery Thread Id: 0x1A94 File: swifthttprunner.cpp Line: 766 Level: debug MSG_NS_INTERFACE_CHANGE, Starting HTTP Discovery
- 2023/05/03 12:27:42 [Information] aciseagent Function: HttpConnection::MakeRequest Thread Id: 0x1C38 File: httpconnection.cpp Line: 330 Level: debug Url=http://enroll.cisco.com/auth/discovery
- 2023/05/03 12:27:42 [Information] aciseagent Function: Target::probeDiscoveryUrl Thread Id: 0x1CA8 File: target.cpp Line: 261 Level: debug GET request to URL (http://enroll.cisco.com/auth/discovery), returned status -1 <Operation Failed.>
- 2023/05/03 12:27:42 [Information] aciseagent Function: hs_transport_winhttp_get Thread Id: 0x1CA8 File: hs_transport_winhttp.c Line: 4829 Level: debug unable to send request: 12002



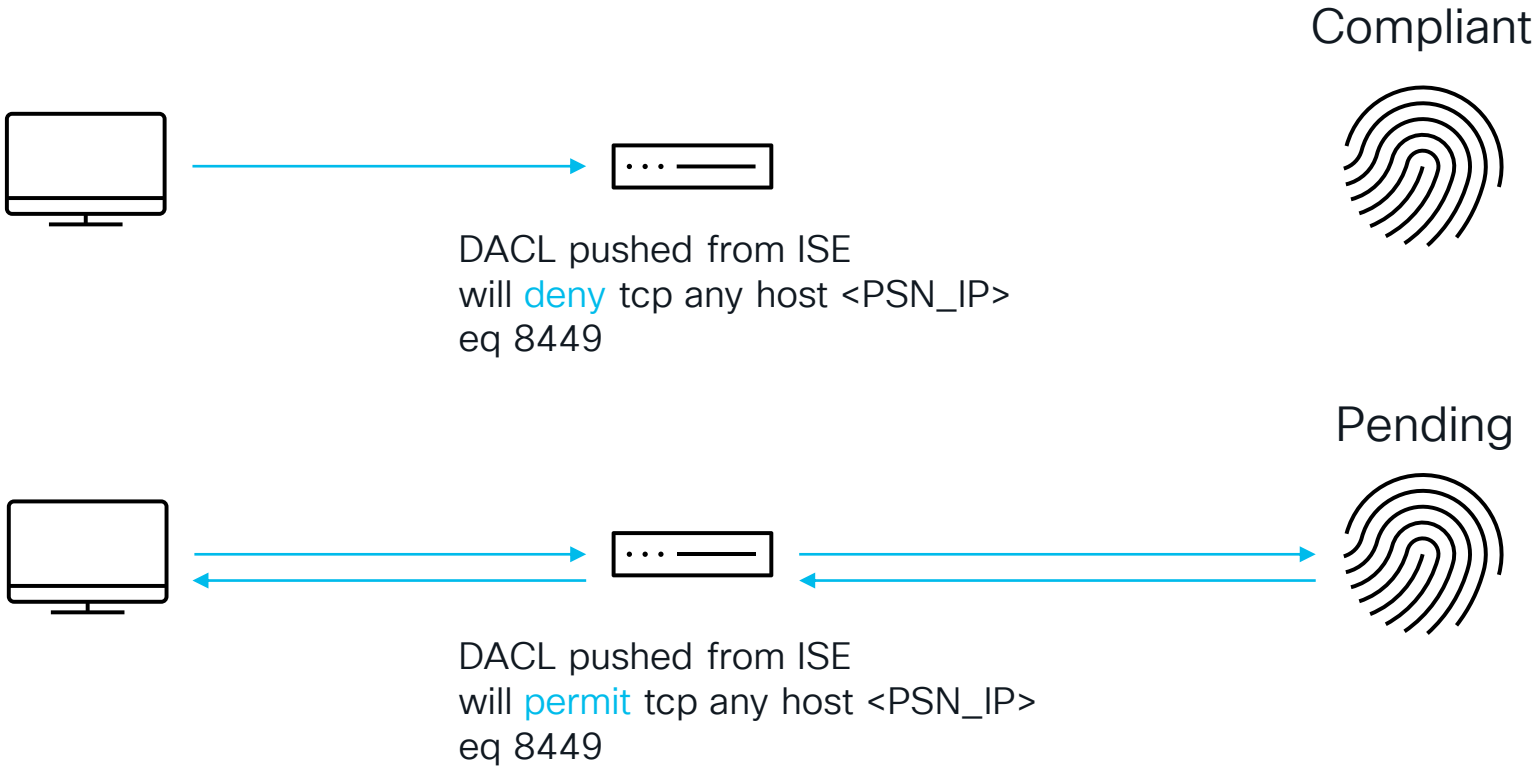
Troubleshooting Posture Pending State on ISE



Users With The Wrong Posture Status

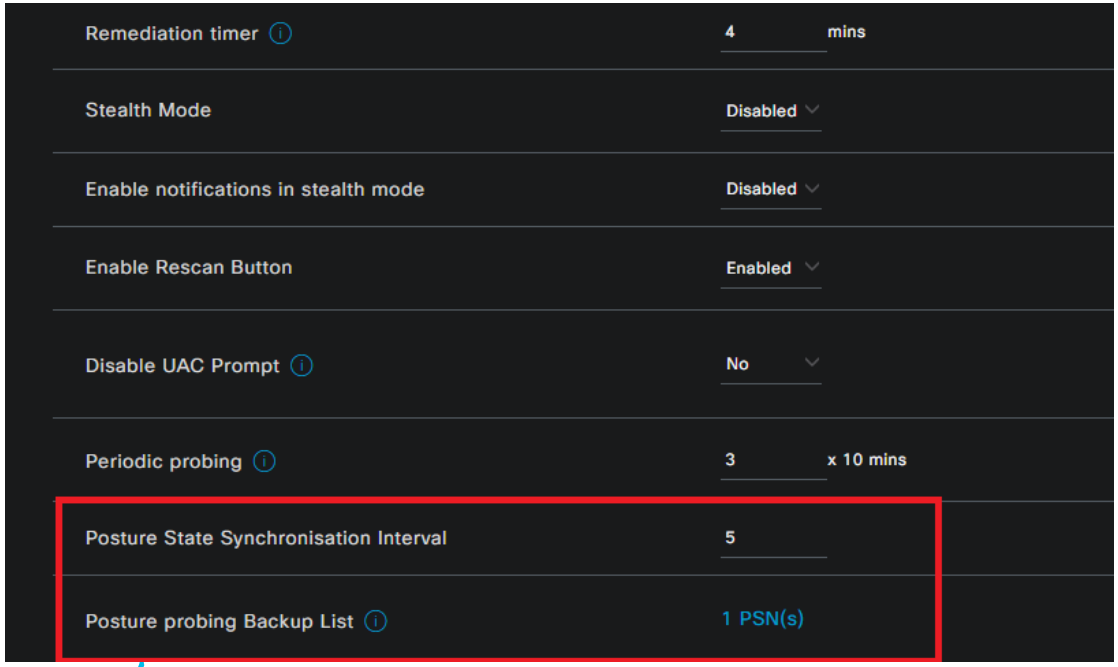
- Cisco ISE may move an endpoint to the “Pending” state because of a change in network configuration
- Endpoint is unable to detect this change and remains in the compliant state
- Posture State Synchronization resolves this by probing ISE for the correct posture status
- Posture State Synchronization port is 8449 by default. This is customizable on the CPP portal
- Probes will only fire off if the posture module is compliant
- Introduced in ISE 3.1+ and AC 4.10+

Posture State Synchronization



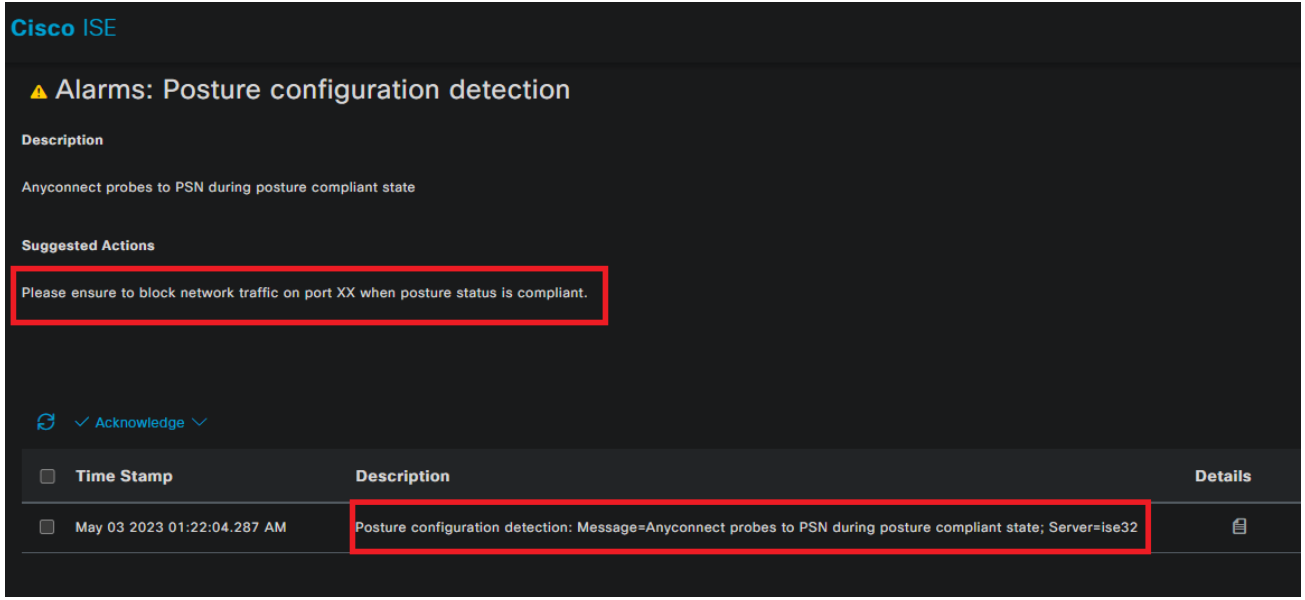
Posture State Synchronization

- Enabled under the Posture Profile settings (Work Centers -> Posture -> Client Provisioning -> Resources -> Posture Profile)
- Probing interval of 0 – 300 seconds



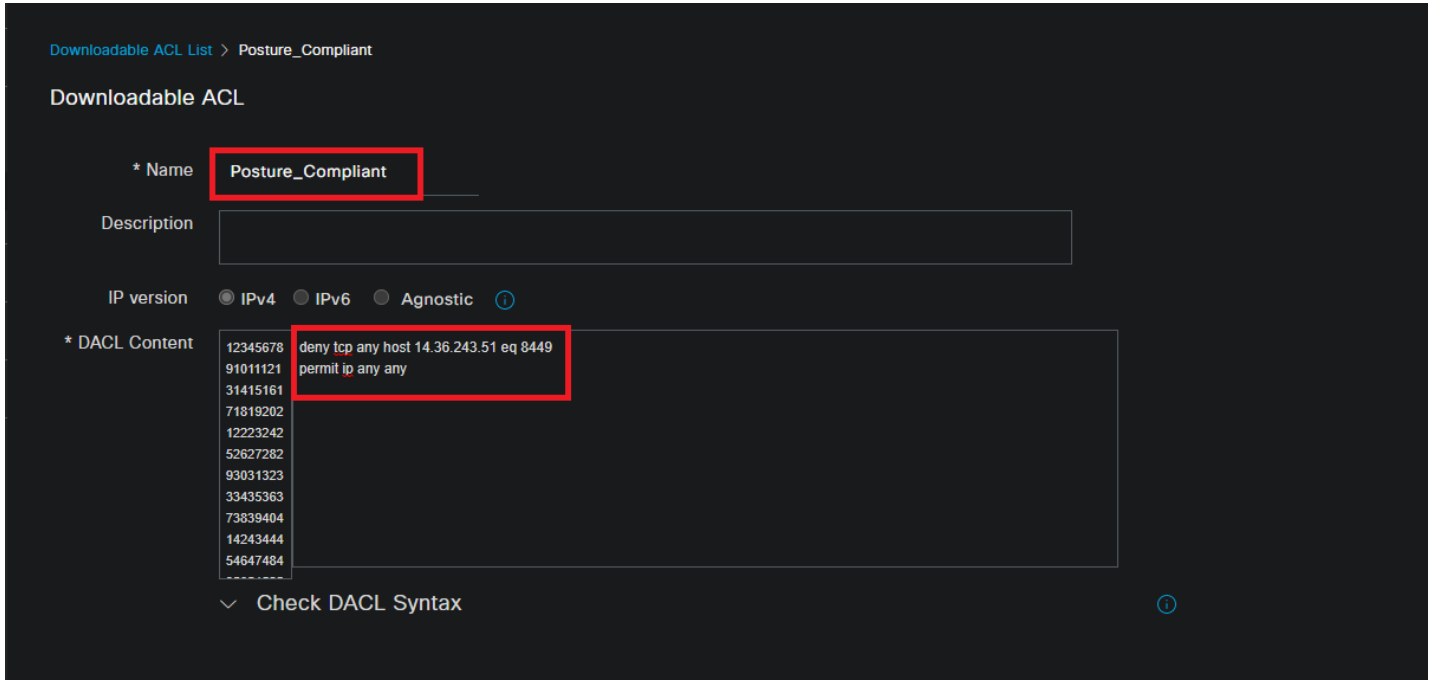
Posture State Synchronization

- Alarm received when compliant endpoints are probing ISE
- In some scenarios, this can cause “maximum resource limit reached” alarms on ISE

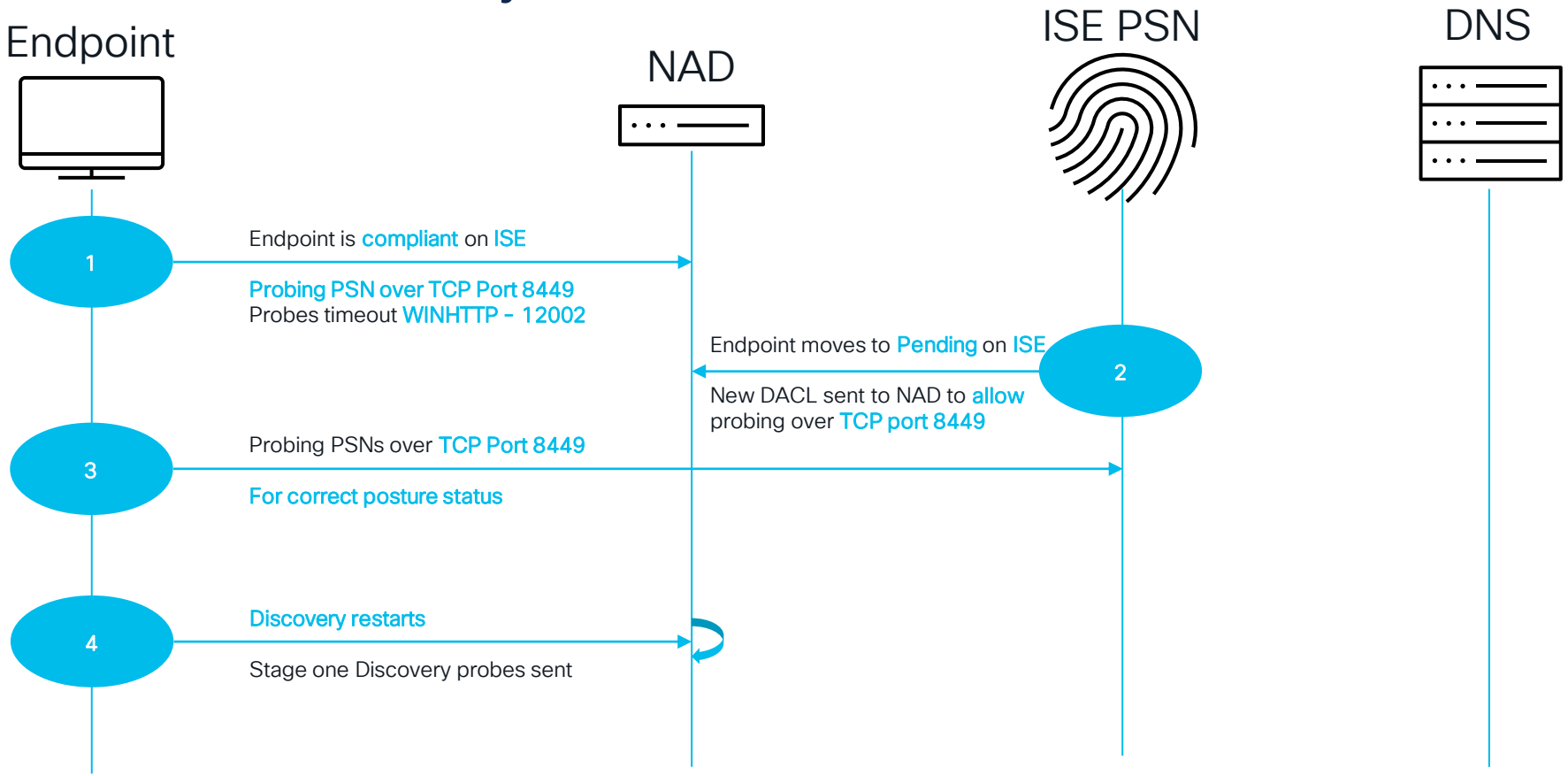


Posture State Synchronization

- Avoid issues by always ensuring traffic towards the posture state synchronization port is being denied



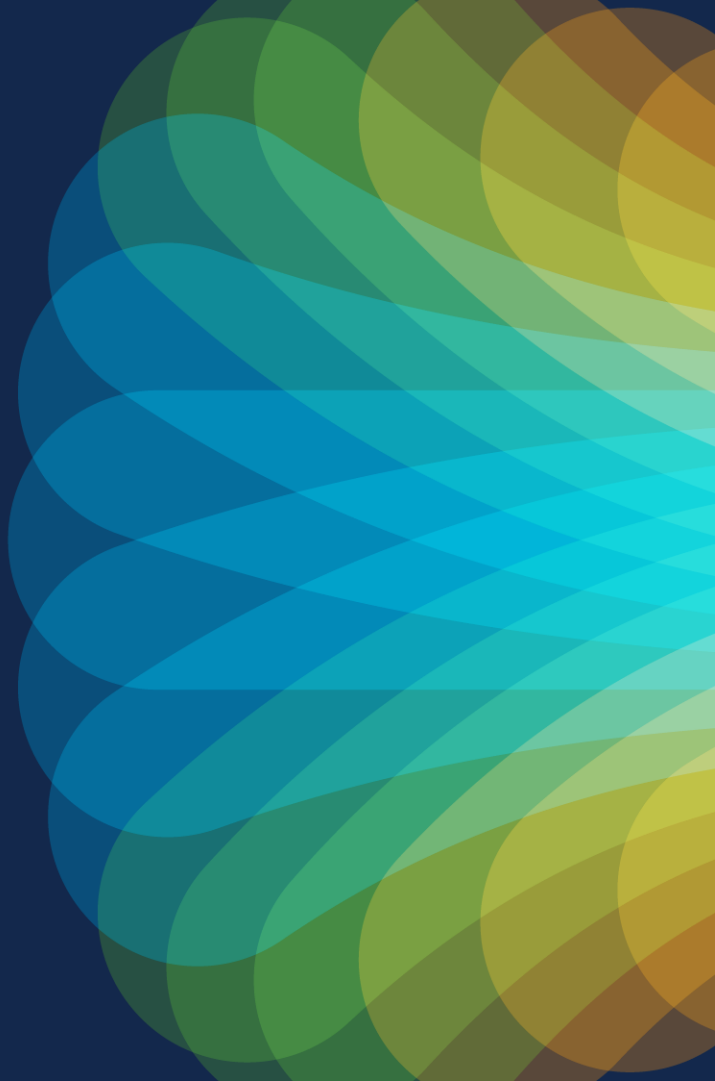
Posture State Synchronization



Posture State Synchronization – In The Logs

- Check“AnyConnect_ISEPosture.txt” from the DART bundle
- 2023/04/27 14:03:29 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0x204C File: periodic_probe.cpp Line: 67 Level: info MSG_SN_START_PERIODIC_PROBE received. Requesting periodic probe start
- 2023/04/27 14:03:31 [Information] aciseagent Function: hs_transport_winhttp_post Thread Id: 0x1C2C File: hs_transport_winhttp.c Line: 5815 Level: debug unable to send request: 12002
- 2023/04/27 14:03:31 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x1C2C File: periodic_probe.cpp Line: 394 Level: debug HTTP Probe failed/timed-out, Retrying...
- 2023/04/27 14:03:31 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x1C2C File: periodic_probe.cpp Line: 357 Level: debug Sending http session sync periodic probe to [ise32.test.com]
- 2023/04/27 14:05:05 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x1C2C File: periodic_probe.cpp Line: 379 Level: debug Different Session state on ISE = [ise32.test.com]. Restarting discovery

Q&A



Fill out your session surveys!

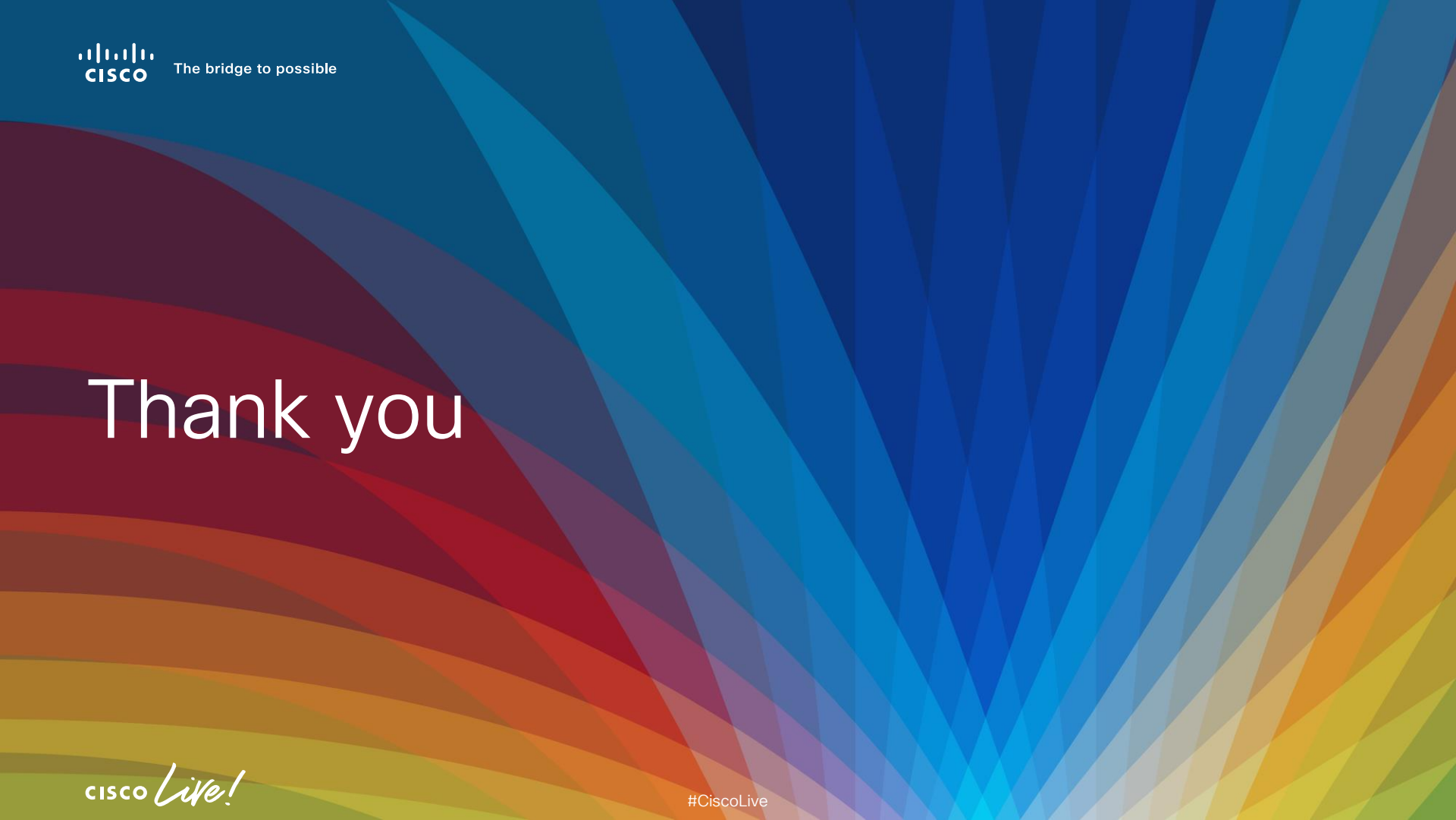
Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live-branded socks (while supplies last)!

Attendees will also earn 100 points in the Cisco Live Game for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand


The bridge to possible
Thank you
cisco Live!
#CiscoLive


cisco Live!
Let's go
#CiscoLive