Compare ISE Posture Redirection Flow to ISE Posture Redirectionless Flow

Contents

Introduction

This document describes posture redirectionless flow (from ISE v2.2 onward) compared to posture redirection flow supported by earlier ISE versions.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Posture flow on ISE
- Configuration of posture components on ISE
- **Adaptive Security Appliance** (ASA) configuration for posture over **Virtual Private Networks** (VPN)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ISE version 2.2
- Cisco ASAv with software 9.6 (2)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document describes a new functionality introduced in Identity Service Engine (ISE) 2.2 that allows ISE to support a posture flow without any kind of redirection support on either a **Network Access Device** (NAD) or ISE.

Posture is a core component of Cisco ISE. Posture as a component can be represented by three main elements:

1. ISE as a policy configuration distribution and decision point.
   From the administrator perspective on ISE, you configure **posture policies** (what exact conditions must be met to mark a device as corporate compliant), **client provisioning policies** (what agent software must be installed on what kind of devices), and **authorization policies** (what kind of permissions must be assigned to, depends upon their posture status).
2. A network access device as a policy enforcement point.
   On the NAD side, actual authorization restrictions are applied at the time of user authentication. ISE as a policy point provides authorization parameters like **Downloaded ACL (dACL)/VLAN/Redirect-URL/Redirect Access Control List (ACL)**. Traditionally, in order for posture to happen, NADs are required to support redirection (to instruct user or agent software which ISE node must be contacted) and **Change of Authorization** (CoA) to reauthenticate the user after the posture status of the endpoint is determined.
3. Agent software as a point of data collection and interaction with the end user.
   Cisco ISE uses three types of agent software: **AnyConnect ISE Posture Module**, **NAC Agent**, and **Web Agent**. Agent receives information about posture requirements from the ISE and provides a report to the ISE about the status of the requirements.

Note: This document is based on Anyconnect ISE Posture Module which is the only one that supports posture fully without redirection.

In the pre-ISE 2.2 flow posture, NADs are not only used to authenticate users and restrict access, but also to provide information to agent software about a specific ISE node that must be contacted. As part of the redirection process, the information about the ISE node is returned to the agent software.

Historically, redirection support (either on the NAD or ISE side) was an essential requirement for posture implementation. In ISE 2.2 requirement to support redirection is eliminated for both the initial client provisioning and posture process.

Client provisioning without redirection - In ISE 2.2 you can access the **Client Provisioning Portal** (CPP) directly via the portal **Fully Qualified Domain Name** (FQDN). This is similar to the way you access **Sponsor Portal** or **MyDevice Portal**.

Posture process without redirection - During agent installation from the CPP portal information about ISE servers is saved on the client side which makes direct communication possible.

Posture Flow Pre ISE 2.2

This image shows a step-by-step explanation of the **Anyconnect ISE Posture Module** flow prior to ISE 2.2:

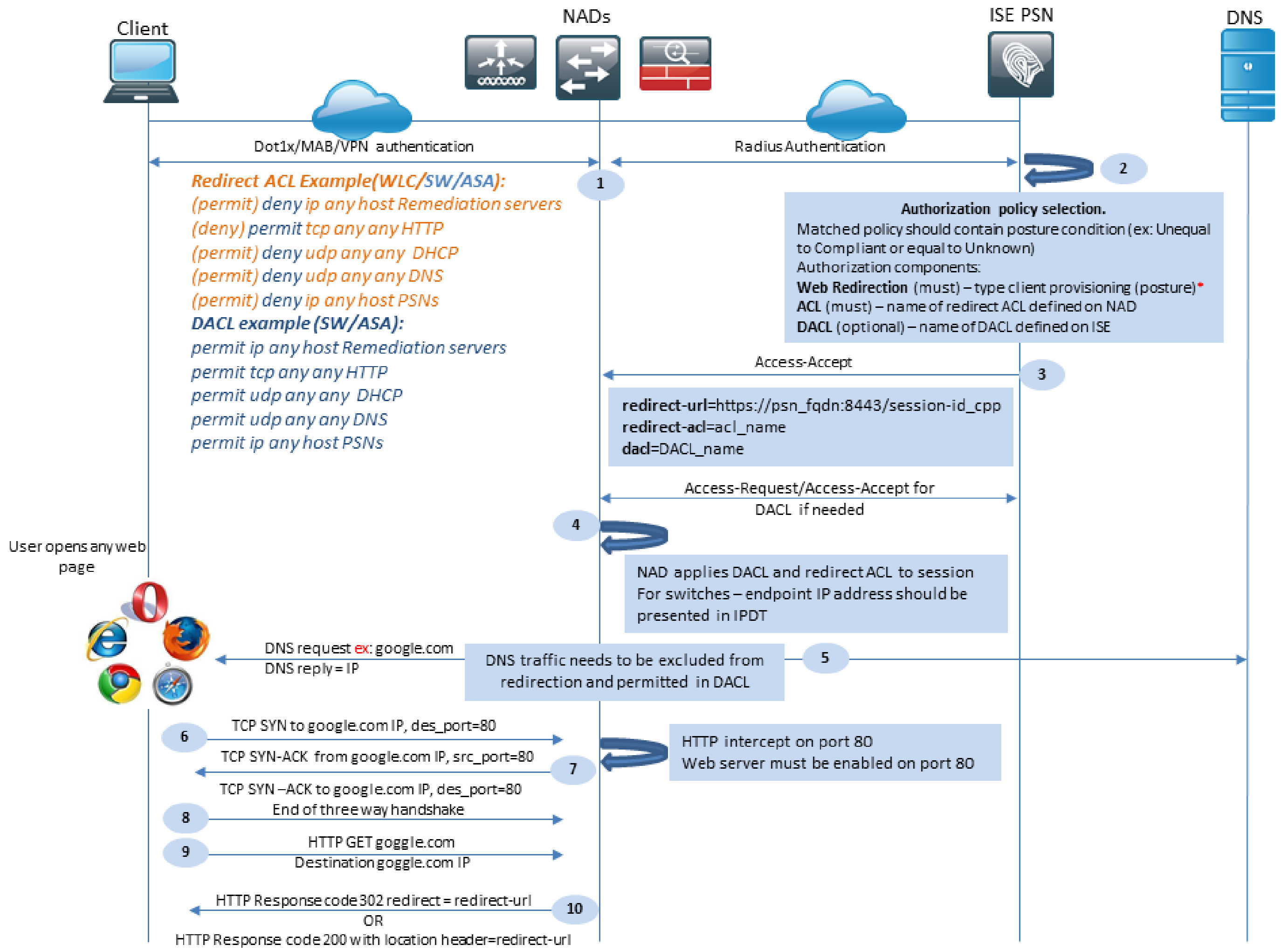

Client
NADs
ISE PSN
DNS
Dot1x/MAB/VPN authentication
Radius Authentication
1
2
Redirect ACL Example(WLC/SW/ASA):
(permit) deny ip any host Remediation servers
(deny) permit tcp any any HTTP
(permit) deny udp any any DHCP
(permit) deny udp any any DNS
(permit) deny ip any host PSNs
DACL example (SW/ASA):
permit ip any host Remediation servers
permit tcp any any HTTP
permit udp any any DHCP
permit udp any any DNS
permit ip any host PSNs
Authorization policy selection.
Matched policy should contain posture condition (ex: Unequal to Compliant or equal to Unknown)
Authorization components:
Web Redirection (must) – type client provisioning (posture)*
ACL (must) – name of redirect ACL defined on NAD
DACL (optional) – name of DACL defined on ISE
Access-Accept
3
redirect-url=https://psn_fqdn:8443/session-id_cpp
redirect-acl=acl_name
dacl=DACL_name
Access-Request/Access-Accept for DACL if needed
4
NAD applies DACL and redirect ACL to session
For switches – endpoint IP address should be presented in IPDT
User opens any web page
DNS request ex: google.com
DNS reply = IP
DNS traffic needs to be excluded from redirection and permitted in DACL
5
6
TCP SYN to google.com IP, des_port=80
TCP SYN-ACK from google.com IP, src_port=80
7
HTTP intercept on port 80
Web server must be enabled on port 80
TCP SYN –ACK to google.com IP, des_port=80
End of three way handshake
8
HTTP GET goggle.com
Destination goggle.com IP
9
HTTP Response code 302 redirect = redirect-url
OR
HTTP Response code 200 with location header=redirect-url
10

Figure 1-1

Step 1. Authentication is the first step of the flow, it can be dot1x, MAB, or VPN.

Step 2. ISE needs to choose an authentication and authorization policy for the user. In the posture scenario, chosen authorization policy must contain a reference to the posture status, which initially must be either unknown or not applicable. To cover both these cases, conditions with posture status unequal compliance can be used.

The chosen authorization profile must contain information about redirection:

- Web Redirection- For the posture case, the web redirection type must be specified as client provisioning (posture).
- ACL- This section needs to contain the ACL name which is configured on the NAD side. This ACL is used to instruct NAD which traffic must bypass the redirection and which must be actually redirected.
- DACL- It can be used together with redirect access-list but consider that different platforms process DACL and Redirect ACLs in a different order.

For example, ASA always processes DACL before it redirects ACL. At the same time, some switch platforms process it in the same way as ASA, and other switch platforms process Redirect ACL first and then check DACL/Interface ACL if traffic must be dropped or allowed.

Note: After you enable the web redirection option in the authorization profile, the target portal for redirection must be chosen.

Step 3. ISE returns Access-Accept with authorization attributes. Redirect URL in authorization attributes is automatically generated by ISE. It contains these components:

- FQDN of ISE node on which authentication happened. In some cases, dynamic FQDN can be overwritten by Authorization profile configuration (Static IP/Hostname/FQDN) in the Web Redirection section.

If the static value is used it must point to the same ISE node where authentication was processed.

In the case of Load Balancer (LB), this FQDN can point to LB VIP but only in case when LB is configured to tie together Radius and SSL connections.

- Port- The port value is obtained from the target portal configuration.
- Session ID- This value is taken by ISE from the Cisco AV pair audit session ID presented in Access-Request. The value itself is dynamically generated by NAD.
- Portal ID- Identifier of a target portal on the ISE side.

Step 4. NAD applies an authorization policy to the session. Additionally, if DACL is configured, its content is requested before authorization policies are applied.

Important considerations:

- All NADs- Device must have locally configured ACL with the same name as the one received in Access-Accept as redirect-acl.
- Switches- The IP address of the client must be presented in the output of `show authentication session interface details` command to successfully apply redirection and ACLs. The client IP address is learned by IP Device Tracking Feature (IPDT).

Step 5. The client sends a DNS request for the FQDN which is entered into the web browser. At this stage, DNS traffic must bypass redirection and the correct IP address must be returned by the DNS server.

Step 6. The client sends TCP SYN to the IP address which is received in the DNS reply. The Source IP address in the packet is the client IP and the Destination IP address is the IP of the requested resource. The destination port equals 80, except for cases when a direct HTTP proxy is configured in the client web browser.

Step 7.NAD intercepts client requests and prepares SYN-ACK packets with a source IP equal to the requested resource IP, destination IP equal to the client IP, and source port equal to 80.

Important considerations:

- NADs must have an HTTP server running on the port on which the client sends requests. By default, it is port 80.
- If the client uses a direct HTTP proxy web server, the HTTP server must run on the proxy port on NAS. This scenario is outside of the scope of this document.

- In the cases when NAD does not have a local IP address in the client, subnet SYN-ACK is sent with NAD routing table (over management interface usually).

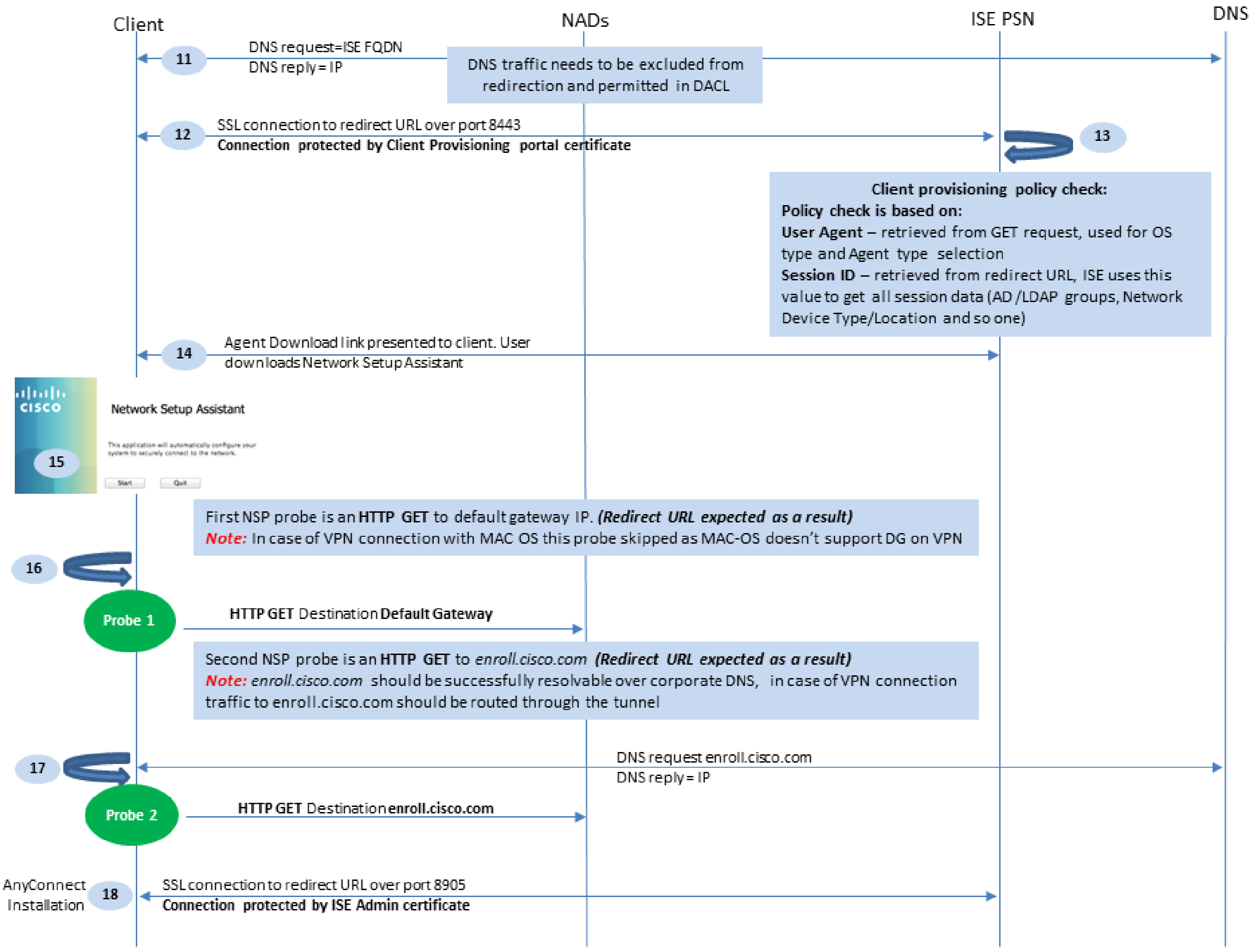
In this scenario, the packet is routed over L3 infrastructure and must be routed back toward the client by an L3 upstream device.

If the L3 device is a stateful firewall, an additional exception must be given for such asymmetric routing.

Step 8. Client finishes TCP three-way handshake by ACK.

Step 9. HTTP GET for the target resource is sent by a client.

Step 10. NAD returns a redirect URL to the client with HTTP code 302 (page moved), on some NADs redirect can be returned inside of the HTTP 200 OK message in the location header.



DNS traffic needs to be excluded from redirection and permitted in DACL

SSL connection to redirect URL over port 8443
Connection protected by Client Provisioning portal certificate

Client provisioning policy check:
Policy check is based on:
User Agent – retrieved from GET request, used for OS type and Agent type selection
Session ID – retrieved from redirect URL, ISE uses this value to get all session data (AD /LDAP groups, Network Device Type/Location and so one)

Agent Download link presented to client. User downloads Network Setup Assistant

First NSP probe is an **HTTP GET** to default gateway IP. ***(Redirect URL expected as a result)***
Note: In case of VPN connection with MAC OS this probe skipped as MAC-OS doesn't support DG on VPN

HTTP GET Destination **Default Gateway**

Second NSP probe is an **HTTP GET** to *enroll.cisco.com* ***(Redirect URL expected as a result)***
Note: enroll.cisco.com should be successfully resolvable over corporate DNS, in case of VPN connection traffic to enroll.cisco.com should be routed through the tunnel

DNS request enroll.cisco.com
DNS reply = IP

HTTP GET Destination **enroll.cisco.com**

SSL connection to redirect URL over port 8905
Connection protected by ISE Admin certificate

Figure 1-2

Step 11. The client sends a DNS request for the FQDN from the redirect URL. FQDN must be resolvable on the DNS server side.

Step 12. SSL connection over port received in redirect URL is established (default 8443). This connection is protected by a portal certificate from the ISE side. **Client Provisioning Portal** (CPP) is presented to the user.

Step 13.Before you provide a download option to the client, ISE must pick the target client provisioning (CP) policy. The Operation System (OS) of the client detected from the Browser user-agent and other information required for CPP policy selection are retrieved from the authentication session (like AD/LDAP groups and so on). ISE knows the target session from the session id presented in the redirect URL.

Step 14. **Network Setup Assistant** (NSA) download link is returned to the client. The client downloads the application.

Note: Normally you can see NSA as part of BYOD flow for Windows and Android but as well this application can be used to install Anyconnect or its components from ISE.

Step 15.The user runs the NSA application.

Step 16. NSA sends the first discovery probe - HTTP /auth/discovery to the Default gateway. NSA expects redirect-url as a result.

Note: For connections over VPN on MAC OS devices this probe is ignored as MAC OS does not have a default gateway on the VPN adapter.

Step 17.NSA sends a second probe if the first one fails. The second probe is an HTTP GET /auth/discovery to `enroll.cisco.com`. This FQDN must be successfully resolvable by the DNS server. In a VPN scenario with a split tunnel, traffic to `enroll.cisco.com` must be routed through the tunnel.

Step 18. If any of the probes succeed, NSA establishes an SSL connection over port 8905 with information obtained from redirect-url. This connection is protected by the ISE admin certificate. Inside this connection NSA downloads Anyconnect.

Important considerations:

- Prior to ISE 2.2 release, SSL communication over port 8905 is a requirement for posture.
- To avoid certificate warnings both portal and admin certificates must be trusted on the client side.
- In multi-interface ISE deployments interfaces other than G0 can be bound to FQDN differently from system FQDN (with the use of `ip host` CLI command). This can cause problems with **Subject Name(SN)/Subject Alternative Name (SAN)** validation. If the client is redirected to FQDN from interface G1, for example, the system FQDN can differ from the FQDN in the redirect URL for the 8905 communication certificate. As a solution for this scenario, you can add FQDNs of additional interfaces in admin certificate SAN fields, or you can use a wildcard in the admin certificate.

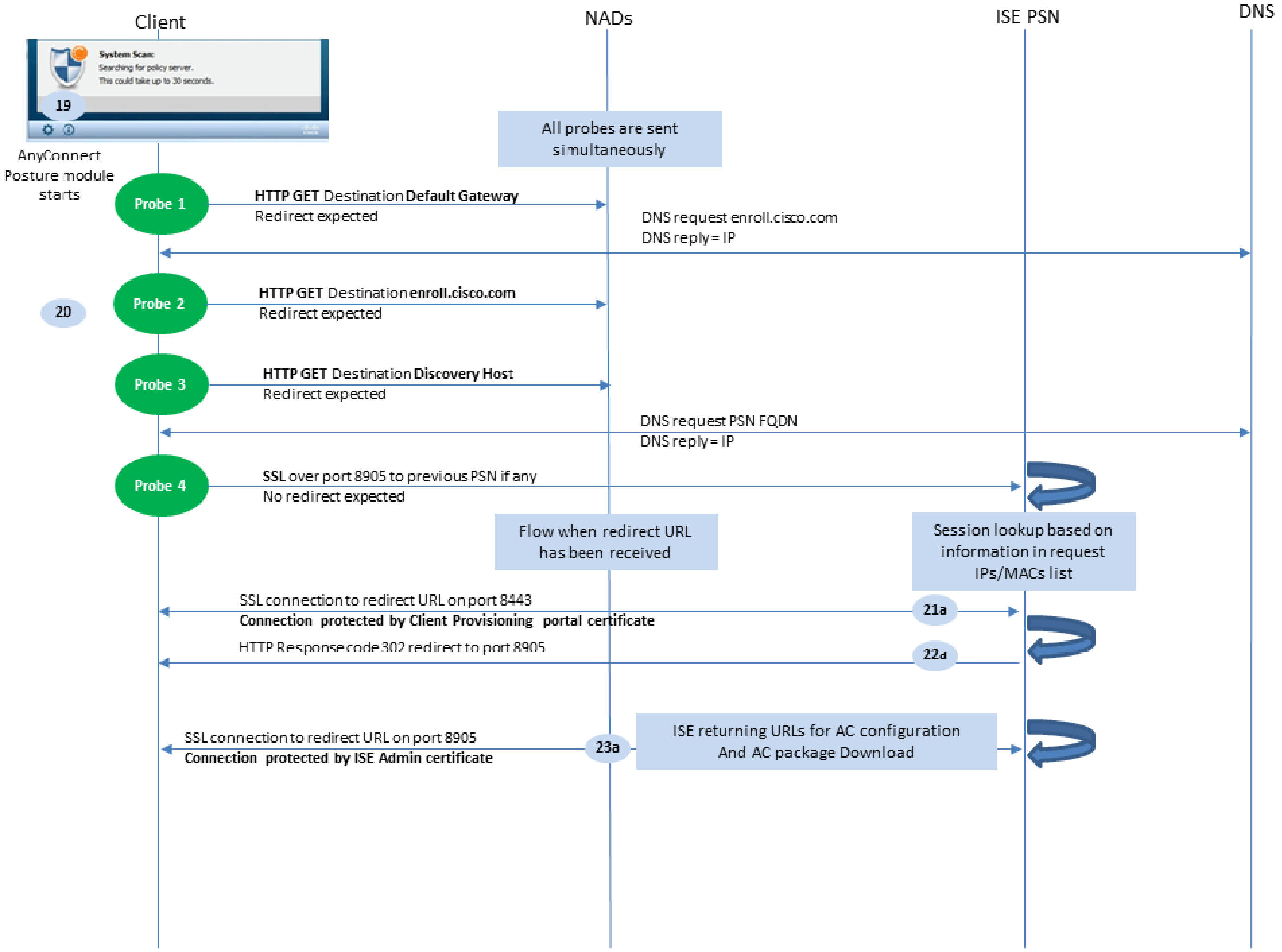

Client
NADs
ISE PSN
DNS
System Scan:
Searching for policy server.
This could take up to 30 seconds.
19
AnyConnect Posture module starts
All probes are sent simultaneously
Probe 1
HTTP GET Destination Default Gateway
Redirect expected
DNS request enroll.cisco.com
DNS reply = IP
20
Probe 2
HTTP GET Destination enroll.cisco.com
Redirect expected
Probe 3
HTTP GET Destination Discovery Host
Redirect expected
DNS request PSN FQDN
DNS reply = IP
Probe 4
SSL over port 8905 to previous PSN if any
No redirect expected
Flow when redirect URL has been received
Session lookup based on information in request IPs/MACs list
SSL connection to redirect URL on port 8443
Connection protected by Client Provisioning portal certificate
21a
HTTP Response code 302 redirect to port 8905
22a
SSL connection to redirect URL on port 8905
Connection protected by ISE Admin certificate
23a
ISE returning URLs for AC configuration
And AC package Download

Figure 1-3

Step 19.Anyconnect ISE posture process is launched.

Anyconnect ISE Posture module starts in any of these situations:

- After installation
- After the default gateway value change
- After the system user login event
- After the system power event

Step 20. At this stage, Anyconnect ISE Posture Module initiates policy server detection. This is accomplished with a series of probes that are sent at the same time by the Anyconnect ISE Posture module.

- Probe 1 - HTTP get /auth/discovery to default gateway IP. Consider that MAC OS devices do not have a default gateway on the VPN adapter. The expected result for the probe is redirect-url.
- Probe 2 - HTTP GET /auth/discovery to enroll.cisco.com. This FQDN needs to be successfully resolvable by the DNS server. In a VPN scenario with a split tunnel, traffic to enroll.cisco.com must be routed through the tunnel. The expected result for the probe is redirect-url.
- Probe 3 - HTTP get /auth/discovery to discovery host. The Discovery host value is returned from ISE during installation in the AC posture profile. The expected result for the probe is redirect-url.
- Probe 4 - HTTP GET /auth/status over SSL on port 8905 to previously connected PSN. This request contains information about client IPs and MACs list for session lookup on the ISE side. This problem is not presented during the first posture attempt. Connection is protected by an ISE admin certificate. As a result of this probe, ISE can return the session ID back to the client if the node where

the probe landed is the same node where the user has been authenticated.

Note: As a result of this probe, posture can be done successfully even without working redirection under some circumstances. Successful posture without redirection requires that the current PSN which authenticated the session must be the same as the previously successfully connected PSN. Keep in mind that prior to ISE 2.2, successful posture without redirection is more of an exception rather than a rule.

The next steps describe the posture process in the case when the redirect URL is received (flow marked with letter a) as a result of one of the probes.

Step 21. Anyconnect ISE Posture module establishes a connection to the client provisioning portal with the use of a URL retrieved during the discovery phase. At this stage, ISE makes client provisioning policy validation once again with the use of the information from the authenticated sessions.

Step 22.If client provisioning policy is detected, ISE returns redirect to port 8905.

Step 23. Agent establishes a connection to ISE over port 8905. During this connection, ISE returns URLs for the posture profile, compliance module, and anyconnect updates.

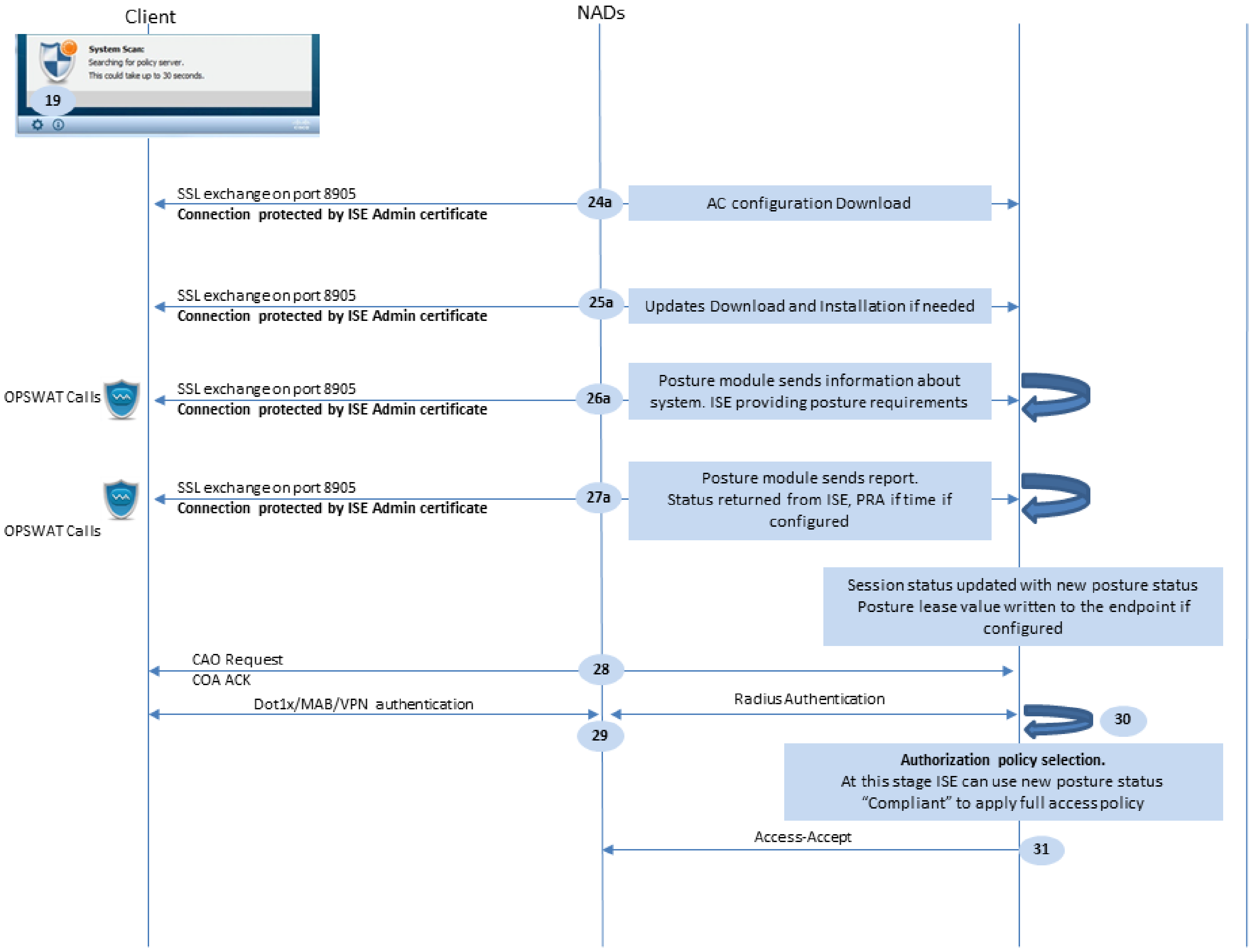

Client
NADs
System Scan:
Searching for policy server.
This could take up to 30 seconds.
19
SSL exchange on port 8905
Connection protected by ISE Admin certificate
24a
AC configuration Download
SSL exchange on port 8905
Connection protected by ISE Admin certificate
25a
Updates Download and Installation if needed
OPSWAT Calls
SSL exchange on port 8905
Connection protected by ISE Admin certificate
26a
Posture module sends information about system. ISE providing posture requirements
SSL exchange on port 8905
Connection protected by ISE Admin certificate
27a
Posture module sends report. Status returned from ISE, PRA if time if configured
OPSWAT Calls
Session status updated with new posture status Posture lease value written to the endpoint if configured
CAO Request
COA ACK
28
Dot1x/MAB/VPN authentication
29
Radius Authentication
30
Authorization policy selection.
At this stage ISE can use new posture status "Compliant" to apply full access policy
Access-Accept
31

Figure 1-4

Step 24.AC ISE Posture module configuration download from ISE.

Step 25.Updates download and installation if required.

Step 26. AC ISE Posture module collects initial information about the system (like OS version, installed security products, and their definition version). At this stage, the AC ISE posture module involves OPSWAT API to collect information about security products. The collected data is sent to ISE. As a reply to this request, ISE provides a posture requirements list. The requirements list is selected as a result of posture policy processing. To match the correct policy, ISE uses the device OS version (present in the request) and session id value to pick other required attributes (AD/LDAP groups). The session ID value is sent by the client as well.

Step 27. At this step, the client involves OPSWAT calls and other mechanisms to check posture requirements. The final report with the requirements list and their status are sent to ISE. ISE needs to make the final decision about the endpoint compliance status. If the endpoint is marked as non-compliant at this step, a set of remediation actions is returned. For the compliant endpoint, ISE writes compliance status into the session and as well puts the last posture timestamp to the endpoint attributes if Posture Lease is configured. The posture result is sent back to the endpoint. In the case of Posture Reassessment (PRA) time for PRA is put by ISE into this packet as well.

In a non-compliant scenario take these points into account:

- Some remediation actions (like display text messages, link remediation, file remediation, and others) are executed by the posture agent itself.
- Other remediation types (like AV. AS, WSUS, and SCCM) require OPSWAT API communication between the posture agent and the target product. In this scenario posture agent just sends a remediation request to the product. Remediation itself is done by the security products directly.

Note: In case when security product has to communicate with external resources (Internal/External Update servers) you must ensure that this communication is allowed in Redirect-ACL/DACL.

Step 28.ISE sends a COA request to the NAD which must trigger a new authentication for the user. NAD must confirm this request by COA ACK. Keep in mind that for the VPN cases COA push is used, so no new authentication request is sent. Instead, ASA removes previous authorization parameters (redirect URL, redirect ACL, and DACL) from the session and applies new parameters from the COA request.

Step 29.New authentication request for the user.

Important considerations:

- Typically for Cisco NAD COA, reauth is used by ISE, and this instructs NAD to initiate a new authentication request with the previous session ID.
- On the ISE side, the same session ID value is an indication that previously collected session attributes must be reused (complaint status in our case) and a new authorization profile based on those attributes must be assigned.
- In case of a session ID change, this connection is treated as new, and the full posture process is restarted.
- In order to avoid re-posture at each session id change, a posture lease can be used. In this scenario, information about the posture status is stored in the endpoint attributes which stays on the ISE even if the session ID gets changed.

Step 30. A new authorization policy is selected on the ISE side based on posture status.

Step 31. Access-Accept with new authorization attributes is sent to the NAD.

The next flow describes the scenario when the redirect URL is not retrieved (marked with letter b) by any posture probe and the previously connected PSN has been queried by the last probe. All steps here are exactly the same as in the case with redirect URL except the replay which is returned by PSN as a result of Probe 4. If this probe landed on the same PSN which is an owner for the current authentication session, the replay contains the session id value which is later used by the posture agent to finish the process. In case when previously connected headend is not the same as the current session owner, session lookup fails and an empty response is returned to the AC ISE posture module. As an ultimate result of this, the No Policy Server Detected message is returned to the end user.

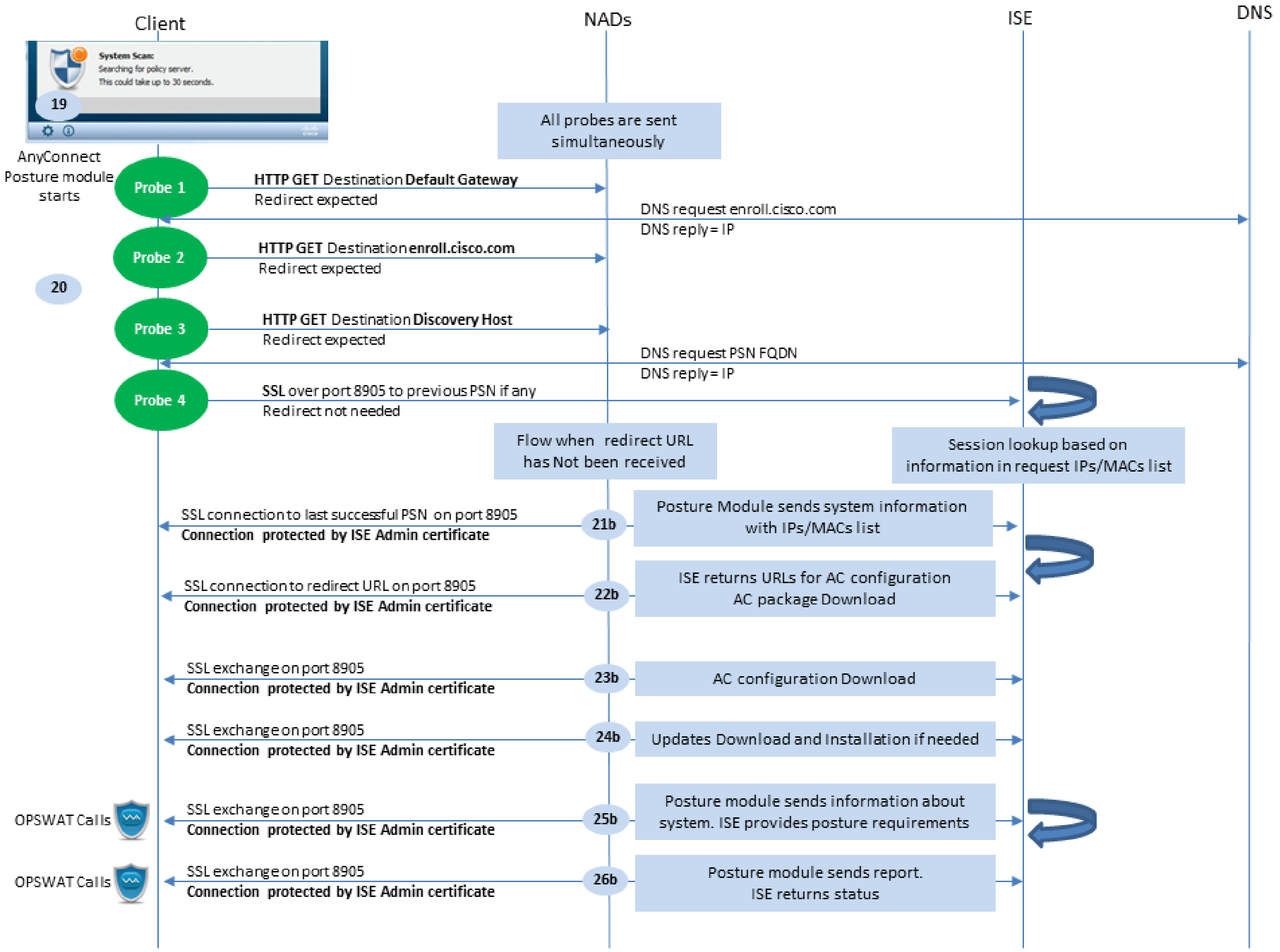
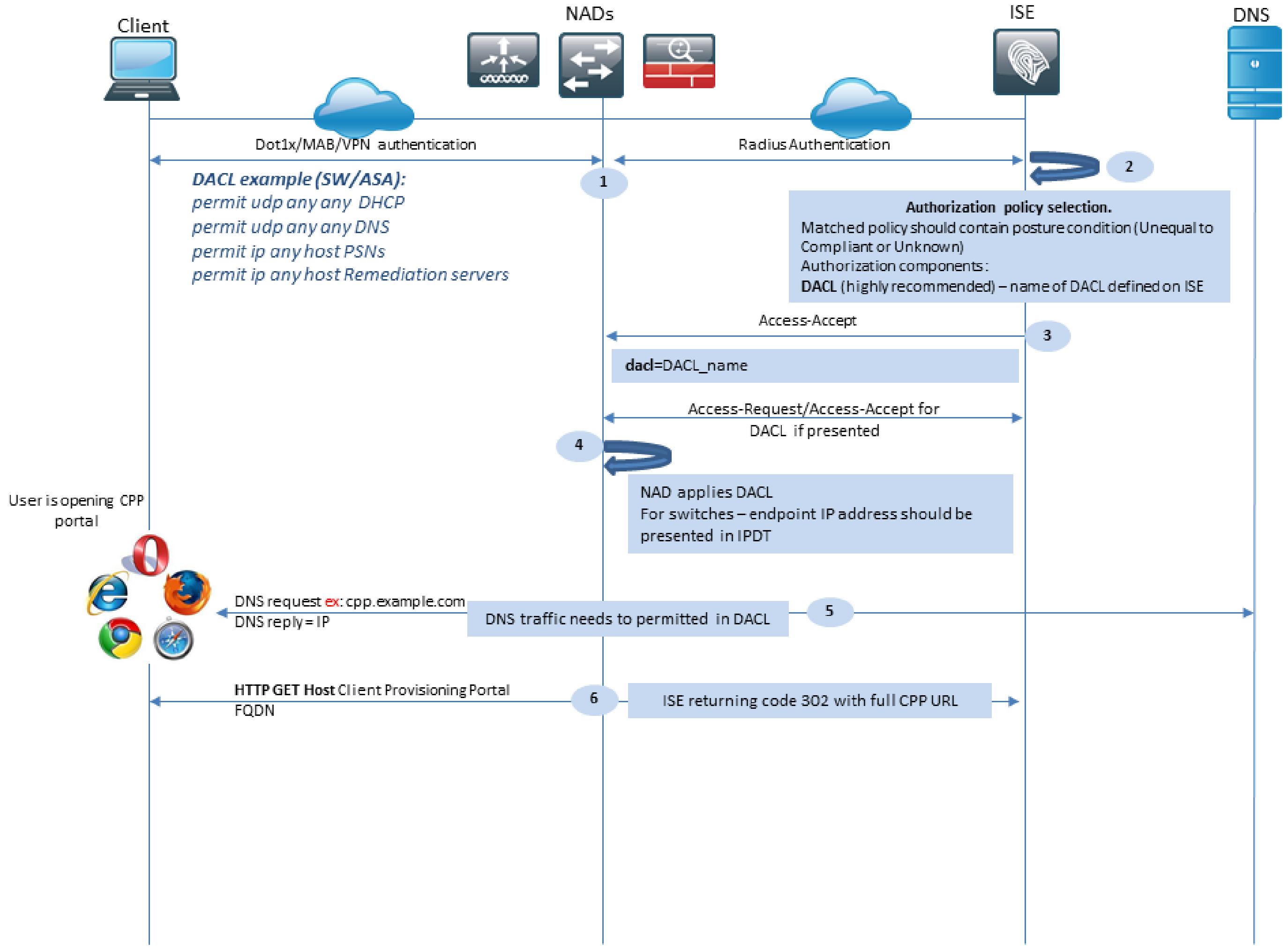

Client
NADs
ISE
DNS
System Scan:
Searching for policy server.
This could take up to 30 seconds.
19
AnyConnect Posture module starts
All probes are sent simultaneously
Probe 1
HTTP GET Destination Default Gateway
Redirect expected
DNS request enroll.cisco.com
DNS reply= IP
Probe 2
HTTP GET Destination enroll.cisco.com
Redirect expected
20
Probe 3
HTTP GET Destination Discovery Host
Redirect expected
DNS request PSN FQDN
DNS reply= IP
Probe 4
SSL over port 8905 to previous PSN if any
Redirect not needed
Flow when redirect URL has Not been received
Session lookup based on information in request IPs/MACs list
SSL connection to last successful PSN on port 8905
Connection protected by ISE Admin certificate
21b
Posture Module sends system information with IPs/MACs list
SSL connection to redirect URL on port 8905
Connection protected by ISE Admin certificate
22b
ISE returns URLs for AC configuration AC package Download
SSL exchange on port 8905
Connection protected by ISE Admin certificate
23b
AC configuration Download
SSL exchange on port 8905
Connection protected by ISE Admin certificate
24b
Updates Download and Installation if needed
OPSWAT Calls
SSL exchange on port 8905
Connection protected by ISE Admin certificate
25b
Posture module sends information about system. ISE provides posture requirements
OPSWAT Calls
SSL exchange on port 8905
Connection protected by ISE Admin certificate
26b
Posture module sends report. ISE returns status

Figure 1-5

Posture Flow Post ISE 2.2

ISE 2.2 and newer versions support both redirection and redirectionless flows simultaneously. This is the detailed explanation for redirectionless posture flow:


Client
NADs
ISE
DNS
Dot1x/MAB/VPN authentication
Radius Authentication
1
2
3
4
5
6
Access-Accept
Access-Request/Access-Accept for DACL if presented
User is opening CPP portal
DNS request ex: cpp.example.com
DNS reply = IP
HTTP GET Host Client Provisioning Portal FQDN

DACL example (SW/ASA):
permit udp any any DHCP
permit udp any any DNS
permit ip any host PSNs
permit ip any host Remediation servers

Authorization policy selection.
Matched policy should contain posture condition (Unequal to Compliant or Unknown)
Authorization components:
DACL (highly recommended) – name of DACL defined on ISE

dacl=DACL_name

NAD applies DACL
For switches – endpoint IP address should be presented in IPDT

DNS traffic needs to permitted in DACL

ISE returning code 302 with full CPP URL

Figure 2-1

Step 1.Authentication is the first step of the flow. It can be dot1x, MAB, or VPN.

Step 2.ISE has to choose the authentication and authorization policy for the user. In posture, the scenario chosen authorization policy must contain a reference to the posture status, which initially must be either unknown or not applicable. To cover both these cases, conditions with posture status unequal compliance can be used. For a posture with no redirection, there is no need to use any Web Redirection configuration in the authorization profile. You can still consider the use of a DACL or Airspace ACL to limit user access at the stage when posture status is not available.

Step 3.ISE returns Access-Accept with authorization attributes.

Step 4. If the DACL name is returned in Access-Accept, NAD initiates DACL content download and applies the authorization profile to the session after it is obtained.

Step 5. The new approach assumes that redirection is not possible, so the user must enter the client provisioning portal FQDN manually. FQDN of the CPP portal must be defined in the portal configuration on the ISE side. From the DNS server perspective, A-record must point to the ISE server with the PSN role enabled.

Step 6. The client sends HTTP to get to the client provisioning portal FQDN, this request is parsed on the ISE side and the full portal URL is returned back to the client.

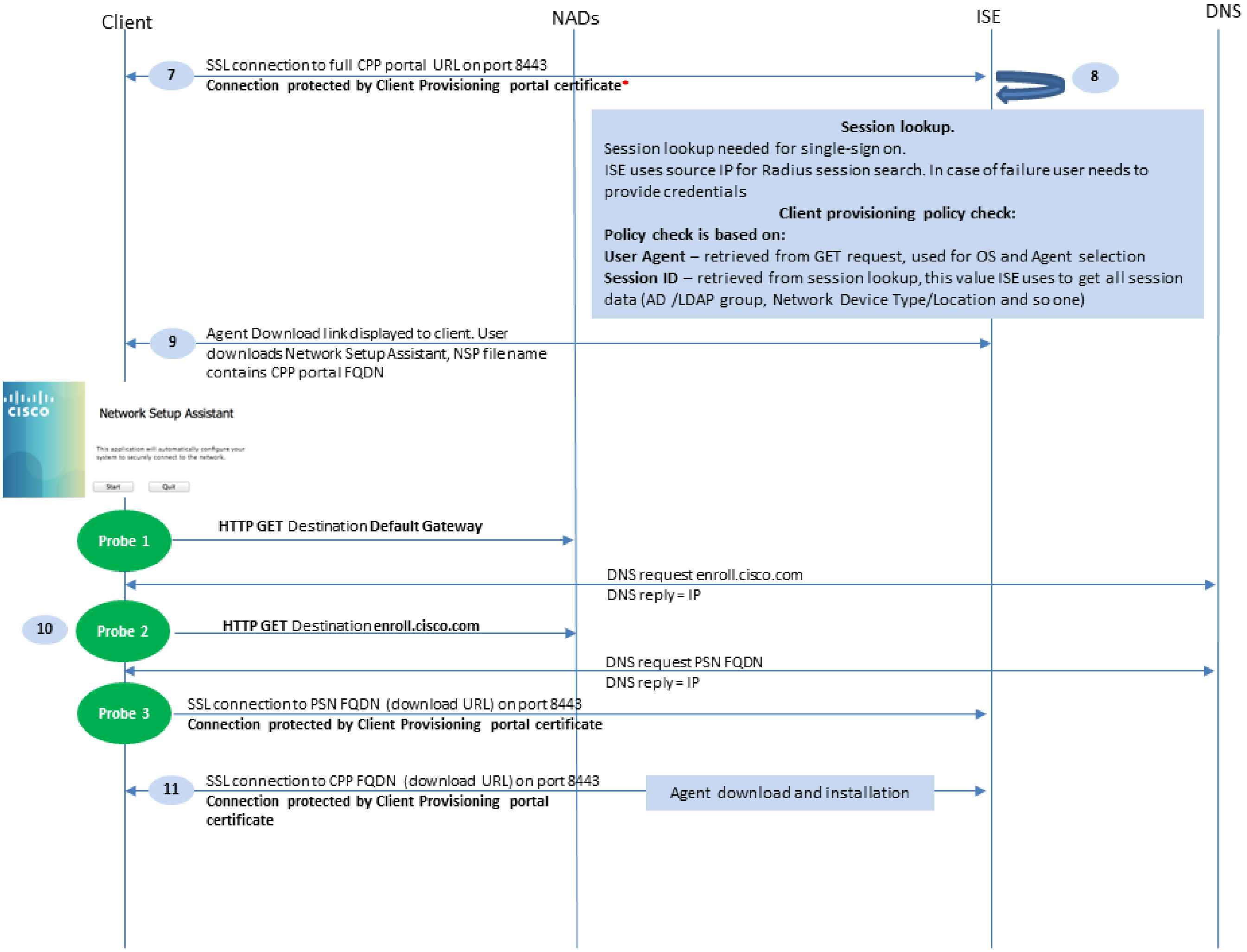

Client
NADs
ISE
DNS
7
SSL connection to full CPP portal URL on port 8443
Connection protected by Client Provisioning portal certificate*
8
Session lookup.
Session lookup needed for single-sign on.
ISE uses source IP for Radius session search. In case of failure user needs to provide credentials
Client provisioning policy check:
Policy check is based on:
User Agent – retrieved from GET request, used for OS and Agent selection
Session ID – retrieved from session lookup, this value ISE uses to get all session data (AD /LDAP group, Network Device Type/Location and so one)
9
Agent Download link displayed to client. User downloads Network Setup Assistant, NSP file name contains CPP portal FQDN
cisco
Network Setup Assistant
Start
Quit
Probe 1
HTTP GET Destination Default Gateway
DNS request enroll.cisco.com
DNS reply = IP
10
Probe 2
HTTP GET Destination enroll.cisco.com
DNS request PSN FQDN
DNS reply = IP
Probe 3
SSL connection to PSN FQDN (download URL) on port 8443
Connection protected by Client Provisioning portal certificate
11
SSL connection to CPP FQDN (download URL) on port 8443
Connection protected by Client Provisioning portal certificate
Agent download and installation

Figure 2-2

Step 7.SSL connection over port received in redirect URL is established (default 8443). This connection is protected by a portal certificate from the ISE side. The Client Provisioning Portal (CPP) is presented to the user.

Step 8. At this step two events occur on ISE:

- Single Sign On (SSO) - ISE attempts to look up previous successful authentication. ISE uses the source IP address from the packet as a search filter for live radius sessions.

Note: Session is retrieved based on a match between the source IP in the packet and Framed IP address in the session. The framed IP address is normally retrieved by ISE from the interim accounting updates, so it is required to have accounting enabled on the NAD side. Also, you must remember that SSO is only possible on the node which owns the session. If, for example, the session is authenticated on PSN 1, but the FQDN itself points to PSN2, the SSO mechanism fails.

- Client provisioning policy lookup - in case of a successful SSO, ISE can use data from authenticated session and User-agent from the client browser. In case of an unsuccessful SSO, the user must provide credentials and after user authentication information is retrieved from Internal and External Identity stores (AD/LDAP/Internal groups), it can be used for client provisioning policy check.

Note: Due to the Cisco bug ID CSCvd11574, you can see an error at the time of client provisioning policy selection for the non-SSO cases when the external user is a member of multiple AD/LDAP groups added in external identity store configuration. The mentioned defect is fixed that starts from ISE 2.3 FCS and the fix requires to use of CONTAINS in condition with AD group instead of EQUAL.

Step 9. After the client provisioning policy selection, ISE displays the agent download URL to the user. After you click on download NSA, the application is pushed to the user. NSA filename contains the FQDN of the CPP portal.

Step 10.At this step, NSA runs probes to establish a connection to the ISE. Two probes are classic ones, and the third one is designed to allow ISE discovery in environments without url redirection.

- NSA sends the first discovery probe - HTTP /auth/discovery to the Default gateway. NSA expects redirect-url as a result.
- NSA sends a second probe if the first one fails. The second probe is an HTTP GET /auth/discovery to enroll.cisco.com. This FQDN must be successfully resolvable by the DNS server. In a VPN scenario with a split tunnel, traffic to enroll.cisco.com must be routed through the tunnel.
- NSA sends the third probe over the CPP portal port to the client provisioning portal FQDN. This request contains information about the portal session-id which allows ISE to identify which resources have to be provided.

Step 11. NSA downloads Anyconnect and/or specific modules. The download process is done over the client provisioning portal port.

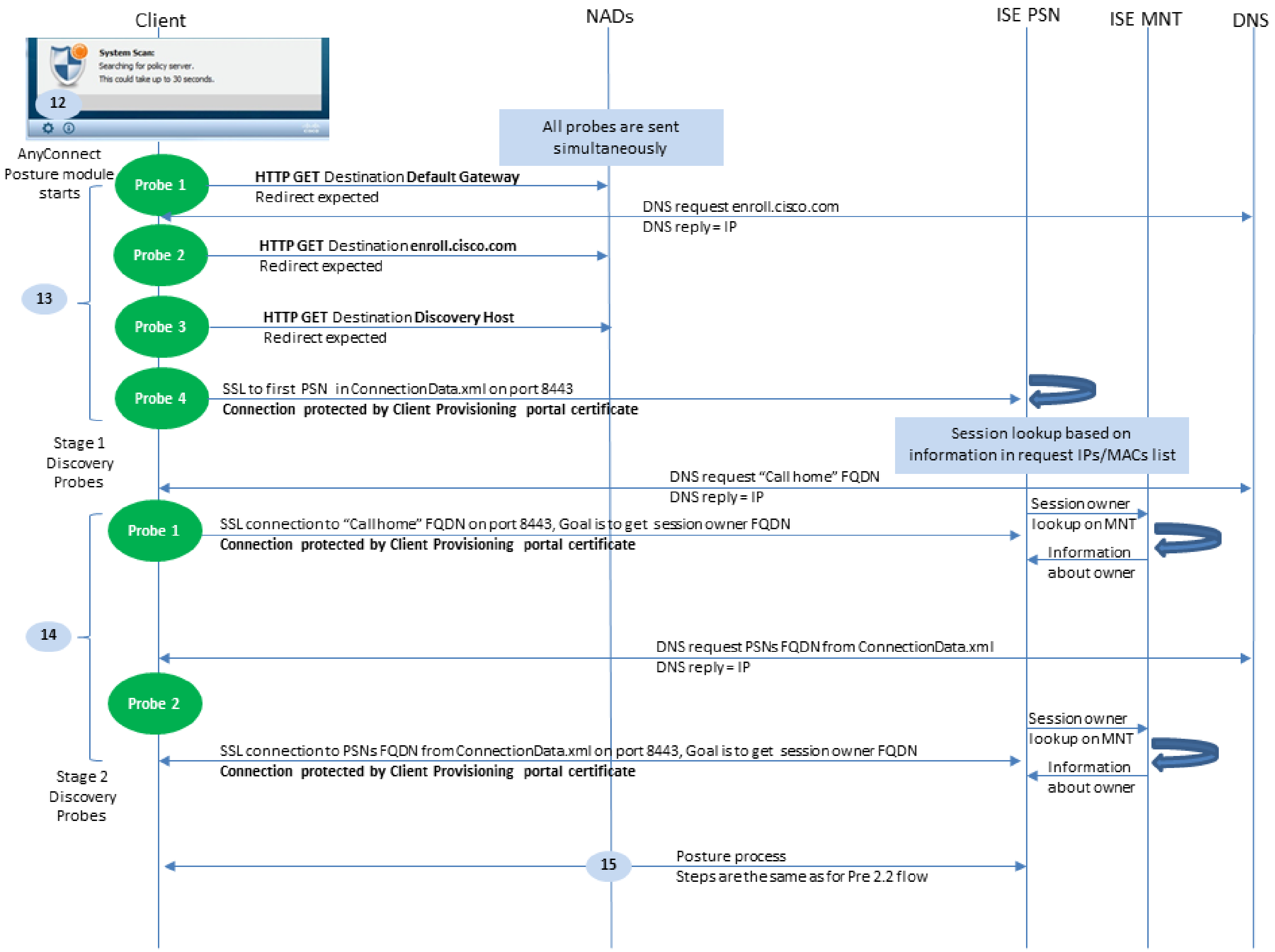

Client
NADs
ISE PSN
ISE MNT
DNS
System Scan:
Searching for policy server.
This could take up to 30 seconds.
12
AnyConnect Posture module starts
All probes are sent simultaneously
Probe 1
HTTP GET Destination Default Gateway
Redirect expected
DNS request enroll.cisco.com
DNS reply= IP
Probe 2
HTTP GET Destination enroll.cisco.com
Redirect expected
13
Probe 3
HTTP GET Destination Discovery Host
Redirect expected
Probe 4
SSL to first PSN in ConnectionData.xml on port 8443
Connection protected by Client Provisioning portal certificate
Session lookup based on information in request IPs/MACs list
Stage 1 Discovery Probes
DNS request "Call home" FQDN
DNS reply= IP
Probe 1
SSL connection to "Call home" FQDN on port 8443, Goal is to get session owner FQDN
Connection protected by Client Provisioning portal certificate
Session owner lookup on MNT
Information about owner
14
DNS request PSNs FQDN from ConnectionData.xml
DNS reply= IP
Probe 2
SSL connection to PSNs FQDN from ConnectionData.xml on port 8443, Goal is to get session owner FQDN
Connection protected by Client Provisioning portal certificate
Session owner lookup on MNT
Information about owner
Stage 2 Discovery Probes
15
Posture process
Steps are the same as for Pre 2.2 flow

Figure 2-3

Step 12. In ISE 2.2, the posture process is divided into two stages. The first stage contains a set of traditional posture discovery probes to support backward compatibility with deployments that rely on the url redirect.

Step 13. The first stage contains all traditional posture discovery probes. To get more details about the probes, review Step 20. in the pre-ISE 2.2 posture flow.

Step 14.Stage two contains two discovery probes that allow the AC ISE posture module to establish a connection to the PSN where the session is authenticated in environments where redirection is not supported**.** During stage two, all probes are sequential.

- Probe 1 - During the first probe, the AC ISE posture module tries to establish with IP/FQDNs from the 'Call Home List'. A list of the targets for the probe must be configured in the AC posture profile on the ISE side. You can define IPs/FQDNs separated by commas, with a colon you can define the port number for each Call Home destination. This port must be equal to the port on which the client provisioning portal run. On the client side information about call home servers is located in ISEPostureCFG.xml, this file can be found in the folder - C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\.
  In case the call home target does not own the session, a lookup for the owner is needed at this stage. AC ISE Posture module instructs ISE to start owner lookup with the use of a special target URL - /auth/ng-discovery request. It also contains the client IPs and MACs list. After this message is received by the PSN session, a lookup is first done locally (this lookup uses both IPs and MACs from the request sent by the AC ISE posture module). If the session is not found, PSN initiates an MNT node query. This request contains only the MACs list, as a result, the FQDN of the owner must be obtained from

the MNT. After this, PSN returns owners FQDN back to the client. The next request from the client is sent to session owner FQDN with auth/status in URL and list of IPs and MACs.

- Probe 2 - At this stage, the AC ISE posture module tries PSN FQDNs which are located in ConnectionData.xml. You can find this file in C:\Users\<current user>\AppData\Local\Cisco\Cisco AnyConnect Secure Mobility Client\. AC ISE Posture module creates this file after the first posture attempt. The file contains a list of ISE PSNs FQDNs. The content of the list can be dynamically updated during the next connection attempts. The end goal of this probe is to get the FQDN of the current session owner. Implementation is identical to Probe 1. with the only difference in probe destination selection. The file itself is located in the folder of the current user in case the device is used by multiple users. Different user is not able to use information from this file. This can lead users to the chicken and egg problem in environments without redirection when Call home targets are not specified.

Step 15. After information about the session owner is obtained, all subsequent steps are identical to the pre-ISE 2.2 flow.

Configure

For this document, ASAv is used as a network access device. All tests are conducted with posture over VPN. ASA configuration for posture over VPN support is outside of the scope of the document. For more details refer to ASA Version 9.2.1 VPN Posture with ISE Configuration Example.

Note: For Deployment with VPN users, the recommended setting is redirection-based posture. Configuration of callhomelist is not recommended. For all non-vpn-based users, ensure DACL is applied such that they do not talk to PSN where posture is configured.

Network Diagram

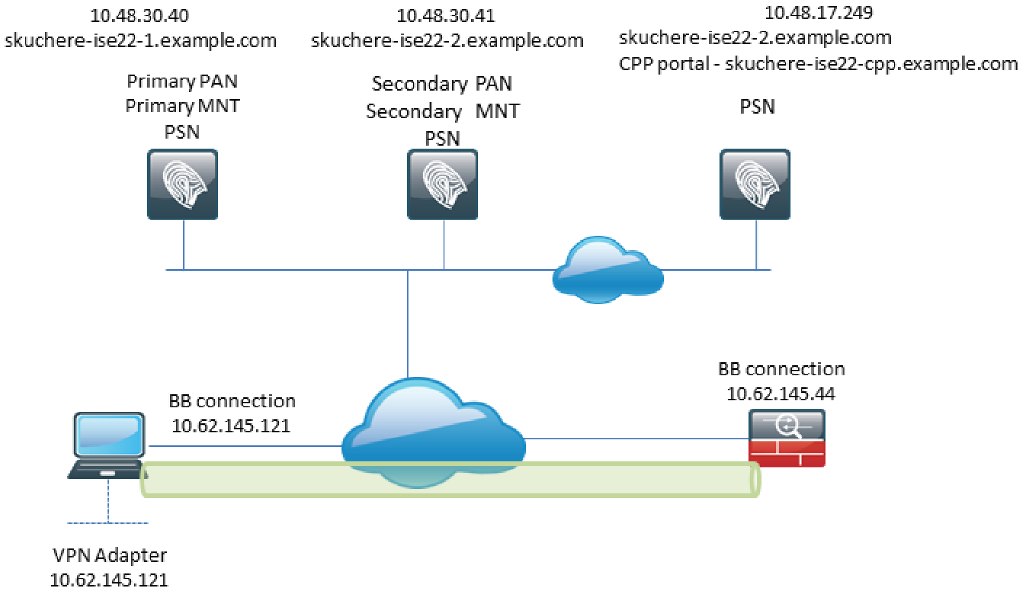


Figure 3-1

This topology is used in tests. With ASA, it is possible to easily simulate the scenario when the SSO mechanism for the Client Provisioning portal fails on the PSN side, because of the NAT feature. In the case of regular posture flow over VPN, SSO must work fine since NAT is normally not enforced for VPN IPs when users enter the corporate network.

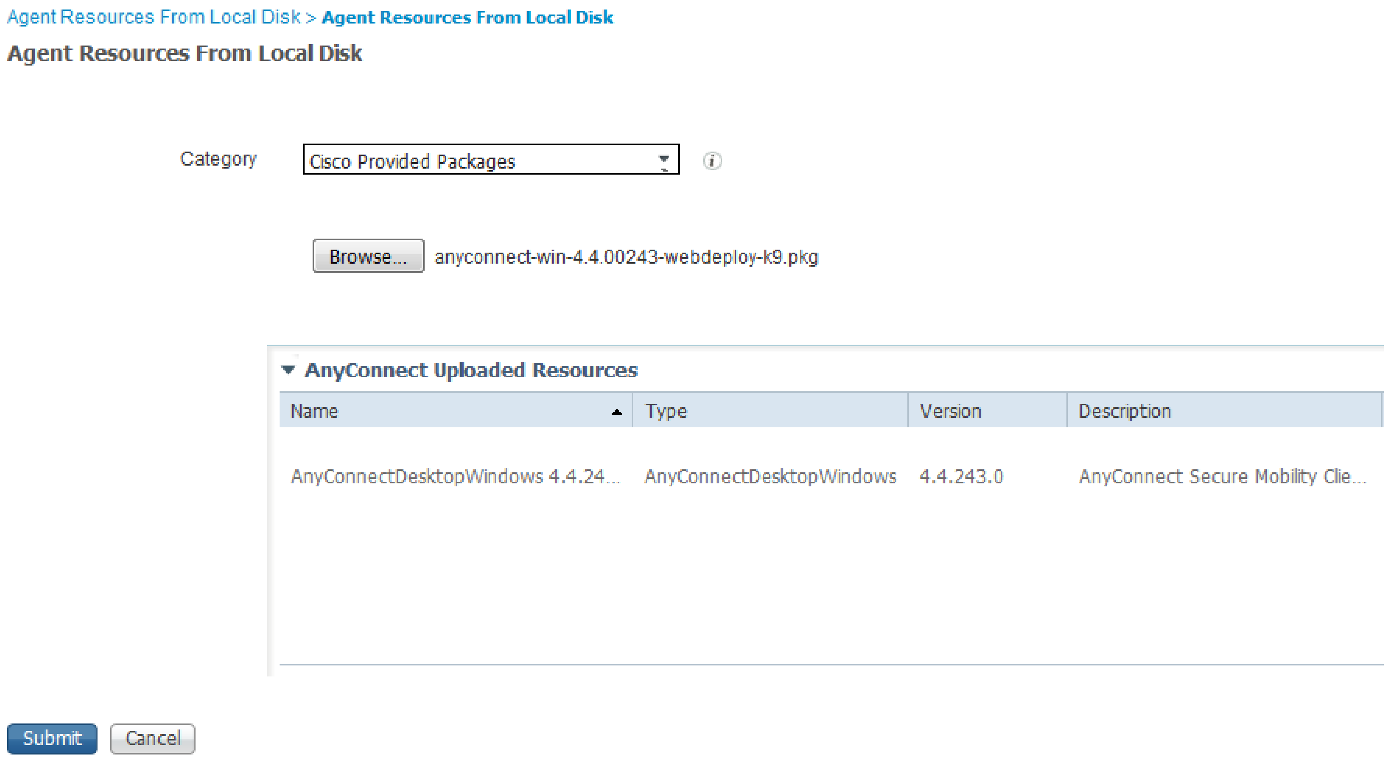
Configurations

Client Provisioning Configuration

These are the steps to prepare the Anyconnect configuration.

Step 1. Anyconnect package download. Anyconnect package itself is not available for direct download from ISE so before you begin, ensure that AC is available on your PC. This link can be used for AC download - https://www.cisco.com/site/us/en/products/security/secure-client/index.html. In this document, anyconnect-win-4.4.00243-webdeploy-k9.pkg package is used.

Step 2. In order to upload the AC package to ISE, navigate to Policy > Policy Elements > Results > Client Provisioning > Resourcesand click Add. Choose Agent resources from the local disk. In the new window, choose Cisco Provided Packages, click browse and choose the AC package on your PC.



Agent Resources From Local Disk > **Agent Resources From Local Disk**

Agent Resources From Local Disk

Category: Cisco Provided Packages

Browse... anyconnect-win-4.4.00243-webdeploy-k9.pkg

AnyConnect Uploaded Resources

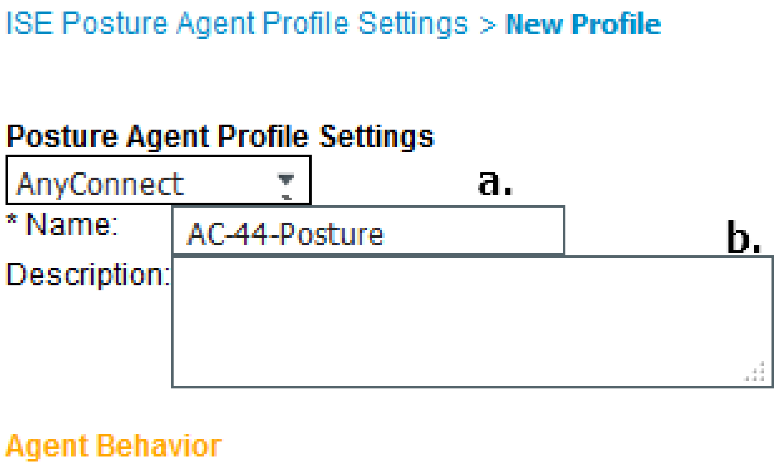
Name	Type	Version	Description
AnyConnectDesktopWindows 4.4.24...	AnyConnectDesktopWindows	4.4.243.0	AnyConnect Secure Mobility Clie...

Figure 3-2

Click Submit to finish the import.

Step 3. The compliance module must be uploaded to ISE. On the same page, click Add and choose the Agent resources from Cisco site. In the resource list, you must check a compliance module. For this document, the AnyConnectComplianceModuleWindows 4.2.508.0 compliance module is used.

Step 4. Now AC posture profile must be created. Click Add and choose the NAC agent or Anyconnect posture profile.


ISE Posture Agent Profile Settings > **New Profile**

Posture Agent Profile Settings

AnyConnect

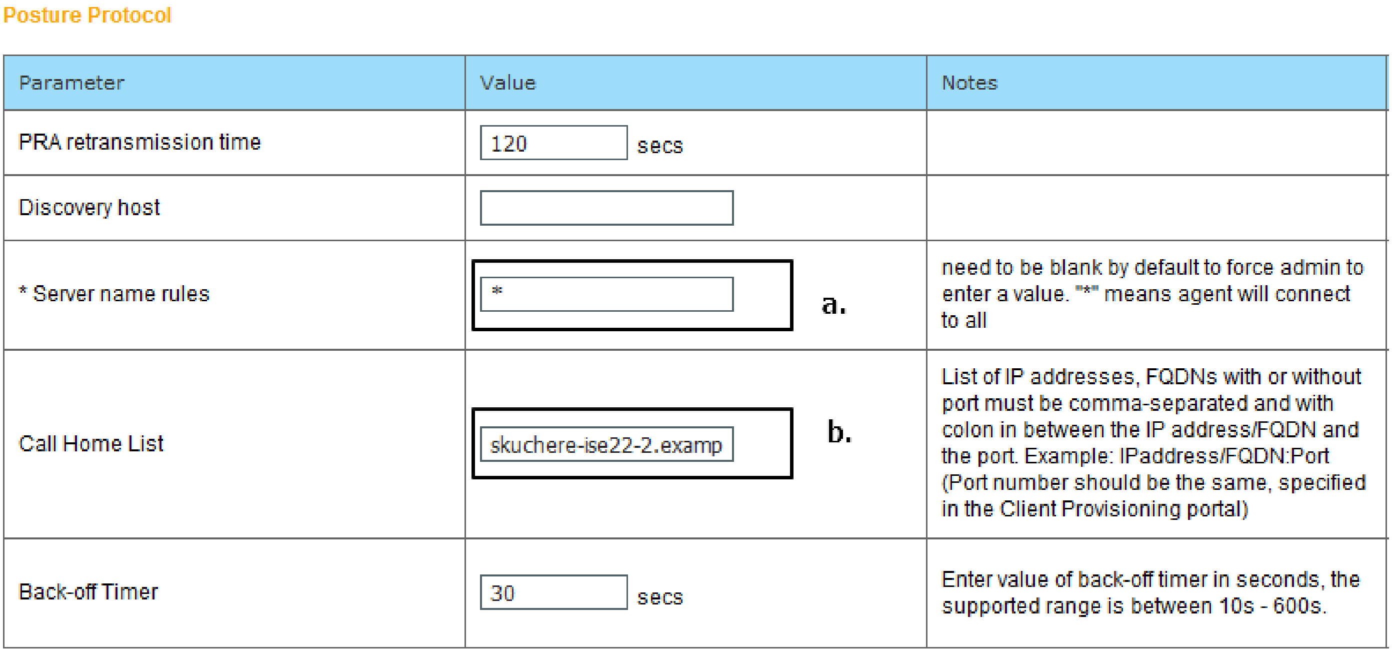
* Name: AC-44-Posture

Description:

Agent Behavior

Figure 3-3

- Choose the type of profile. AnyConnect must be used for this scenario.
- Specify profile name. Navigate to the Posture Protocol section of the profile.


Posture Protocol

Parameter	Value	Notes
PRA retransmission time	120 secs	
Discovery host		
* Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent will connect to all
Call Home List	skuchere-ise22-2.examp	List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.

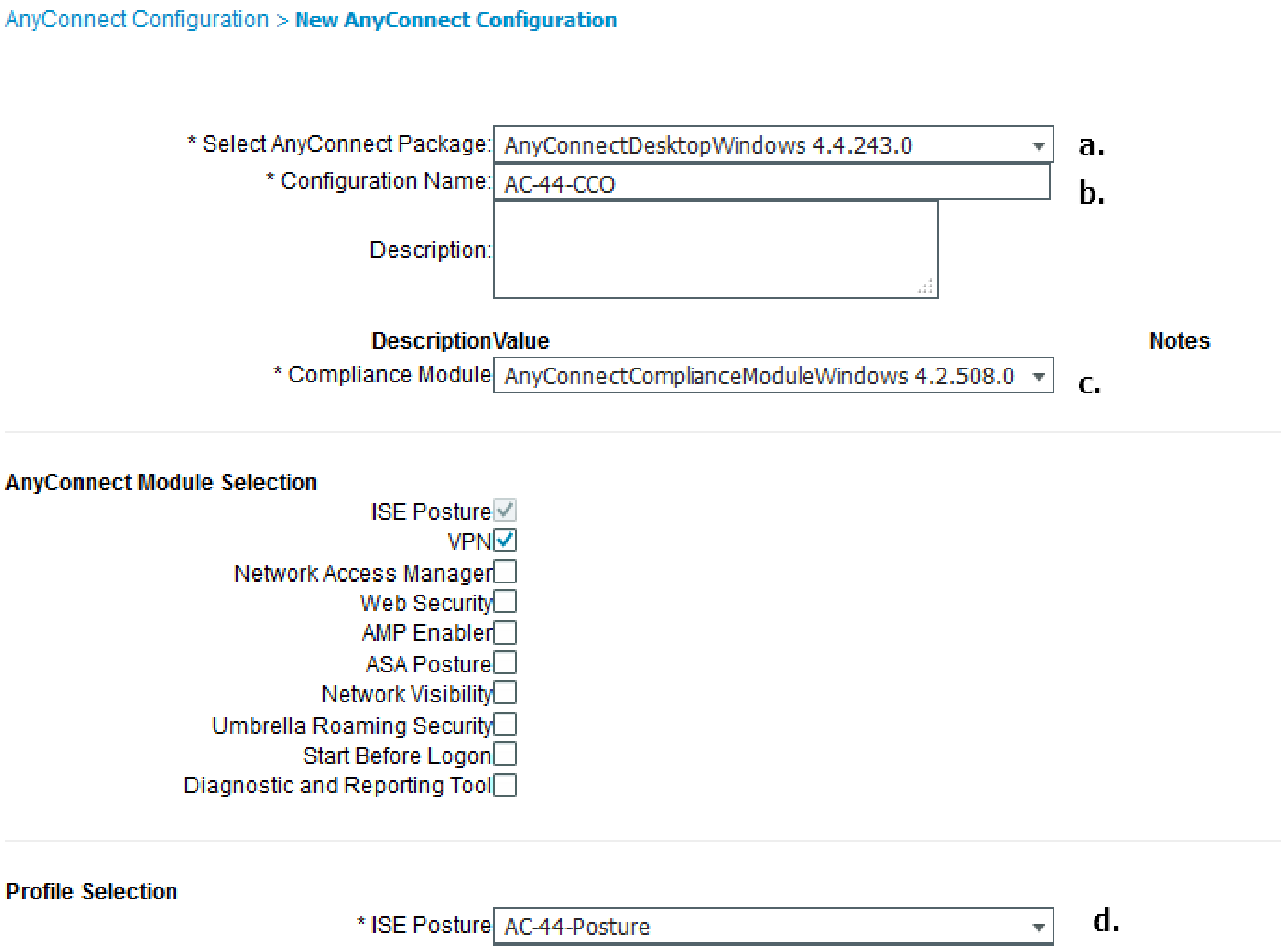
Figure 3-4

- Specify the Server Name Rules, this field cannot be empty. The field can contain FQDN with wildcard which restricts AC ISE posture module connection to PSNs from the appropriate namespace. Put a star if any FQDN must be allowed.
- Names and IPs specified here are in use during stage 2 of posture discovery. You can separate names by coma as well port numbers can be added after FQDN/IP with the use of the colon. In case the AC deployed out-of-band (not from the ISE client provisioning portal) with the use of the GPO or any other software provisioning system presence of Call Home addresses become essential since this is only one probe that can reach ISE PSN successfully. This means that in the case of Out-Of-Band AC provisioning, the administrator must create an AC ISE posture profile with the use of the AC profile editor and provision this file along with AC installation.

Note: Keep in mind that the presence of Call home addresses is critical for multiuser PCs. Review

Step 14. in Posture flow post-ISE 2.2.

Step 5.Create AC configuration. Navigate to Policy > Policy Elements > Results > Client Provisioning > Resources, click Add, then choose AnyConnect Configuration.



AnyConnect Configuration > **New AnyConnect Configuration**

* Select AnyConnect Package: AnyConnectDesktopWindows 4.4.243.0 a.

* Configuration Name: AC-44-CCO b.

Description:

DescriptionValue **Notes**

* Compliance Module AnyConnectComplianceModuleWindows 4.2.508.0 c.

AnyConnect Module Selection

ISE Posture ☑
VPN ☑
Network Access Manager □
Web Security □
AMP Enabler □
ASA Posture □
Network Visibility □
Umbrella Roaming Security □
Start Before Logon □
Diagnostic and Reporting Tool □

Profile Selection

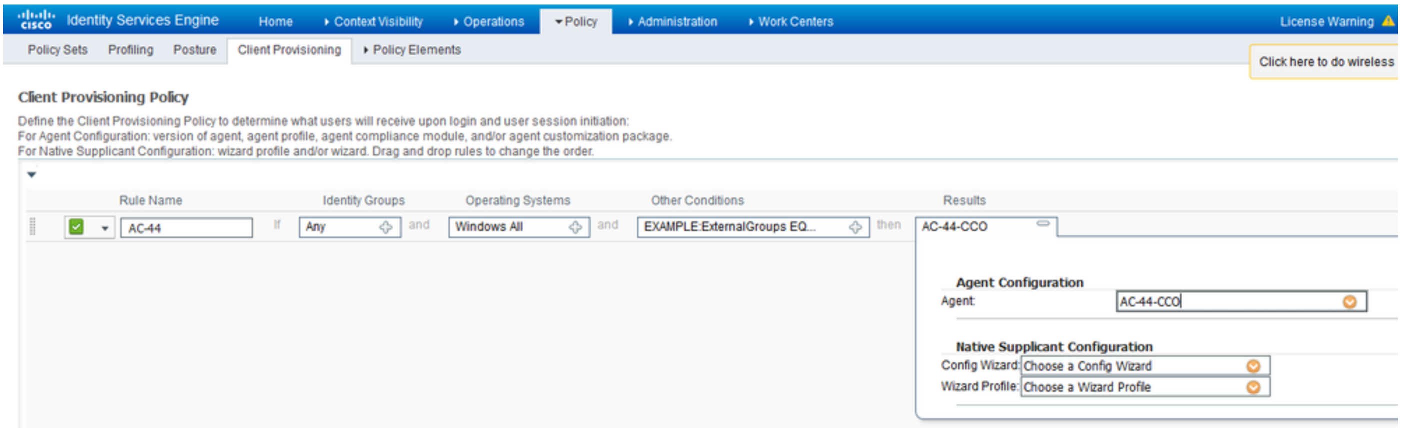
* ISE Posture AC-44-Posture d.

Figure 3-5

- Choose the AC package.
- Provide AC configuration name.
- Choose the compliance module version.
- Choose the AC posture configuration profile from the drop-down list.

Step 6. Configure client provisioning policy. Navigate to Policy > Client Provisioning. In the case of the initial configuration, you can fill empty values in the policy presented with defaults. If you need to add a policy to the posture configuration that exists, navigate to the policy that can be reused and choose Duplicate Above or Duplicate Below . A brand-new policy can also be created.

This is an example of the policy used in the document.



Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
✓ AC-44	If	Any	and	Windows All	and	EXAMPLE:ExternalGroups EQ...	then	AC-44-CCO

Agent Configuration
Agent: AC-44-CCO

Native Supplicant Configuration
Config Wizard: Choose a Config Wizard
Wizard Profile: Choose a Wizard Profile

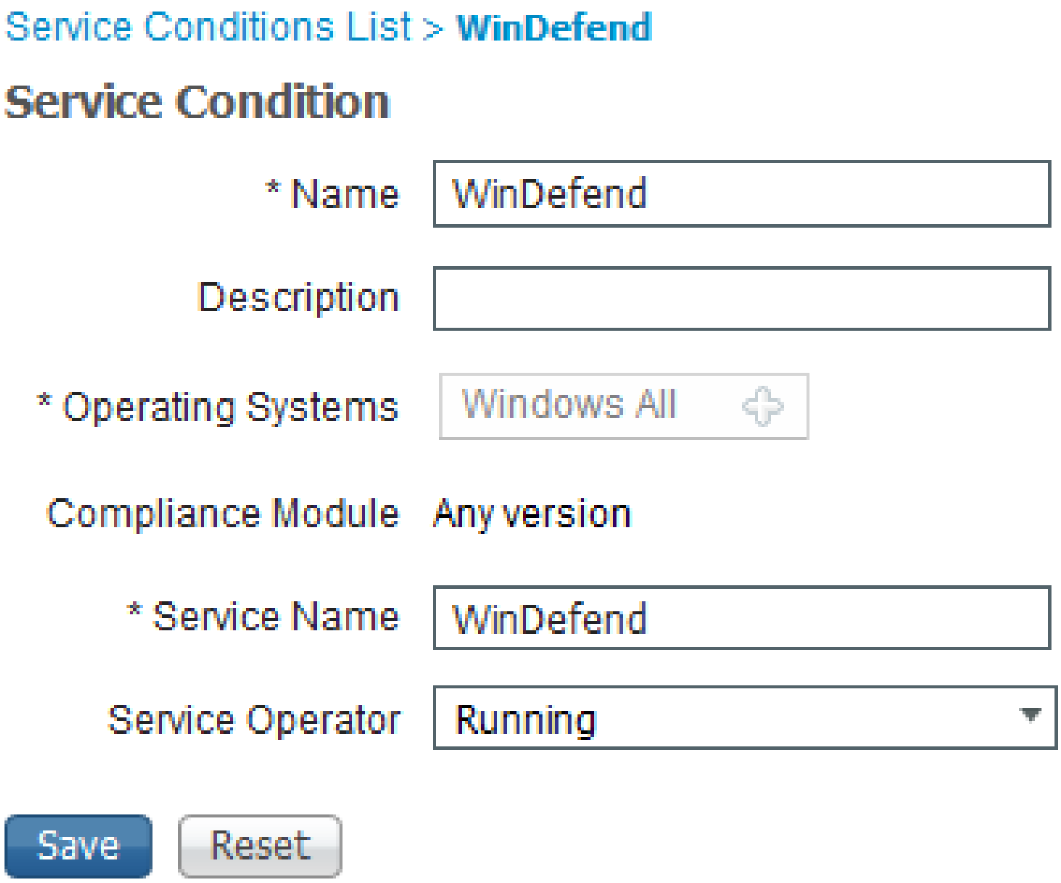
Figure 3-6

Choose your AC configuration in the result section. Keep in mind, that in case of SSO failure ISE can have only attributes from login to portal. These attributes are limited to information that can be retrieved about users from internal and external identity stores. In this document, the AD group is used as a condition in the Client Provisioning policy.

Posture Policies and Conditions

A simple posture check is used. ISE is configured to check the status of the Window Defender service on the end device side. Real-life scenarios can be much more complicated but general configuration steps are the same.

Step 1. Create posture condition. Posture conditions are located in Policy > Policy Elements > Conditions > Posture. Choose the type of posture condition. Here is an example of a Service condition that must check if the Windows Defender service is running.



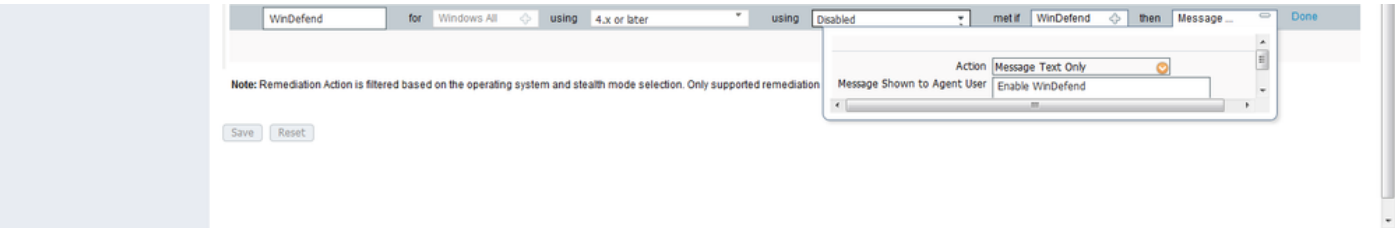
Service Conditions List > **WinDefend**

Service Condition

* Name	WinDefend
Description	
* Operating Systems	Windows All
Compliance Module	Any version
* Service Name	WinDefend
Service Operator	Running

Figure 3-7

Step 2.Posture requirements configuration. Navigate to Policy > Policy Elements > Results > Posture > Requirements. This is an example of a Window Defender check:



WinDefend for Windows All using 4.x or later using Disabled met if WinDefend then Message ...

Action: Message Text Only

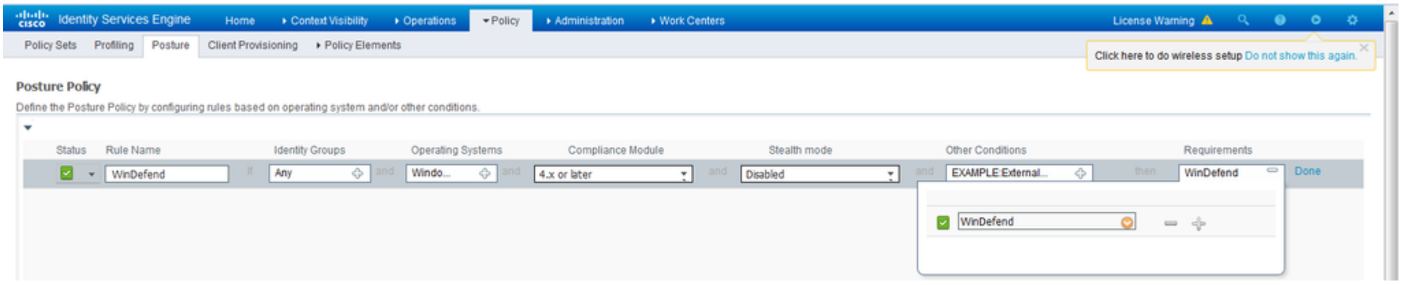
Message Shown to Agent User: Enable WinDefend

Note: Remediation Action is filtered based on the operating system and stealth mode selection. Only supported remediation

Figure 3-8

Choose your posture condition in the new requirement and specify remediation action.

Step 3. Posture policy configuration. Navigate to Policy > Posture. Here, you can find an example of the policy used for this document. The policy has Windows Defender requirement assigned as mandatory and only contains external AD group name as a condition.



Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

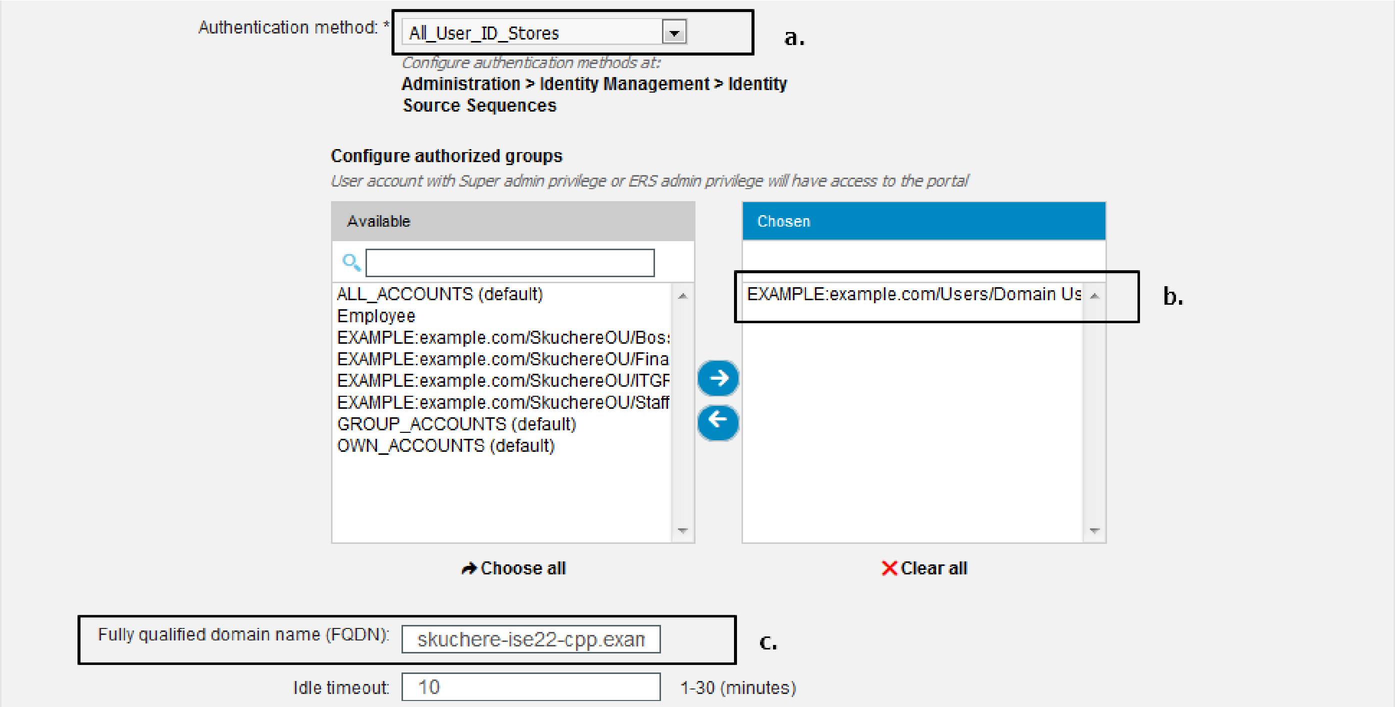
Status	Rule Name		Identity Groups		Operating Systems		Compliance Module		Stealth mode		Other Conditions		Requirements
☑	WinDefend	If	Any	and	Windo...	and	4.x or later	and	Disabled	and	EXAMPLE:External...	then	WinDefend

☑ WinDefend

Figure 3-9

Configure the Client Provisioning Portal

For posture without redirection, the configuration of the client provisioning portal must be edited. Navigate to Administration > Device Portal Management > Client Provisioning. You can either use the default portal or create your own. The same portal can be used for both postures with and without redirection.



Authentication method: * All_User_ID_Stores

Configure authentication methods at:
Administration > Identity Management > Identity Source Sequences

Configure authorized groups

User account with Super admin privilege or ERS admin privilege will have access to the portal

Available:
ALL_ACCOUNTS (default)
Employee
EXAMPLE:example.com/SkuchereOU/Bos:
EXAMPLE:example.com/SkuchereOU/Fina
EXAMPLE:example.com/SkuchereOU/ITGF
EXAMPLE:example.com/SkuchereOU/Staff
GROUP_ACCOUNTS (default)
OWN_ACCOUNTS (default)

Chosen:
EXAMPLE:example.com/Users/Domain Us

Fully qualified domain name (FQDN): skuchere-ise22-cpp.exan

Idle timeout: 10 1-30 (minutes)

Figure 3-10

These settings must be edited in the portal configuration for the non-redirection scenario:

- In Authentication, specify Identity Source Sequence that must be used if SSO cannot locate a session for the user.
- As per the selected Identity Source Sequence list of available groups is populated. At this point, you must select groups that are authorized for portal login.
- FQDN of the client provisioning portal must be specified for scenarios when AC needs to be deployed from the client provisioning portal. This FQDN must be resolvable to ISE PSNs IPs. Users must be instructed to specify the FQDN in the web browser during the first connection attempt.

Configure Authorization Profiles and Policies

Initial access for clients when posture status is not available must be restricted. This can be achieved in multiple ways:

- DACL Assignment - During the restricted access phase, DACL can be assigned to the user to limit access. This approach can be used for Cisco Network Access Devices.
- VLAN Assignment - Before successful posture users can be put in restricted VLAN, this approach must work fine for almost any NAD vendor.
- Radius Filter-Id - With this attribute, ACL locally defined on NAD can be assigned to the user with unknown posture status. As this is a standard RFC attribute, this approach must work well for all NAD vendors.

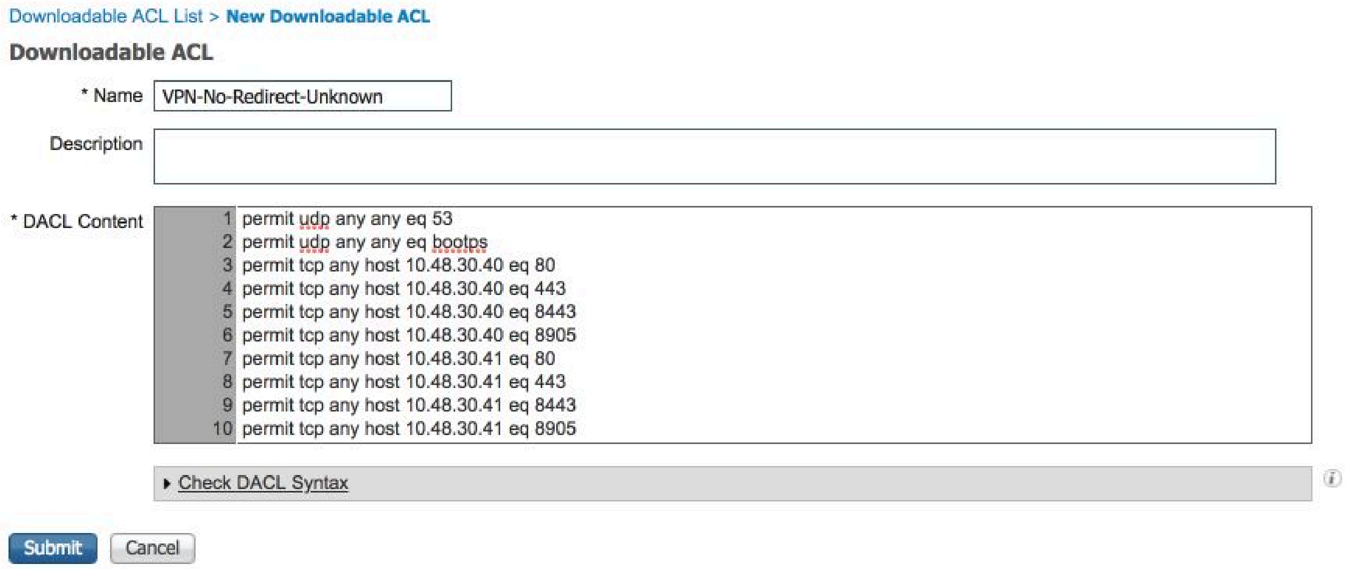
Step 1. Configure DACL. Since this example is based on ASA, a NAD DACL can be used. For real-life scenarios, you must consider VLAN or Filter-ID as possible options.

In order to create DACL, navigate to Policy > Policy Elements > Results > Authorization > Downloadable ACLsand click Add**.**

During the unknown posture state, at least these permissions must be provided:

- DNS traffic
- DHCP traffic
- Traffic to ISE PSNs (ports 80 and 443 for a possibility to open friendly FQDN of portal. Port on which CP portal is running is 8443 by default and port 8905 for backward compatibility)
- Traffic to remediation servers if needed

This is an example of DACL without remediation servers:



Downloadable ACL List > **New Downloadable ACL**

Downloadable ACL

* Name VPN-No-Redirect-Unknown

Description

* DACL Content

```
permit udp any any eq 53
permit udp any any eq bootps
permit tcp any host 10.48.30.40 eq 80
permit tcp any host 10.48.30.40 eq 443
permit tcp any host 10.48.30.40 eq 8443
permit tcp any host 10.48.30.40 eq 8905
permit tcp any host 10.48.30.41 eq 80
permit tcp any host 10.48.30.41 eq 443
permit tcp any host 10.48.30.41 eq 8443
permit tcp any host 10.48.30.41 eq 8905
```

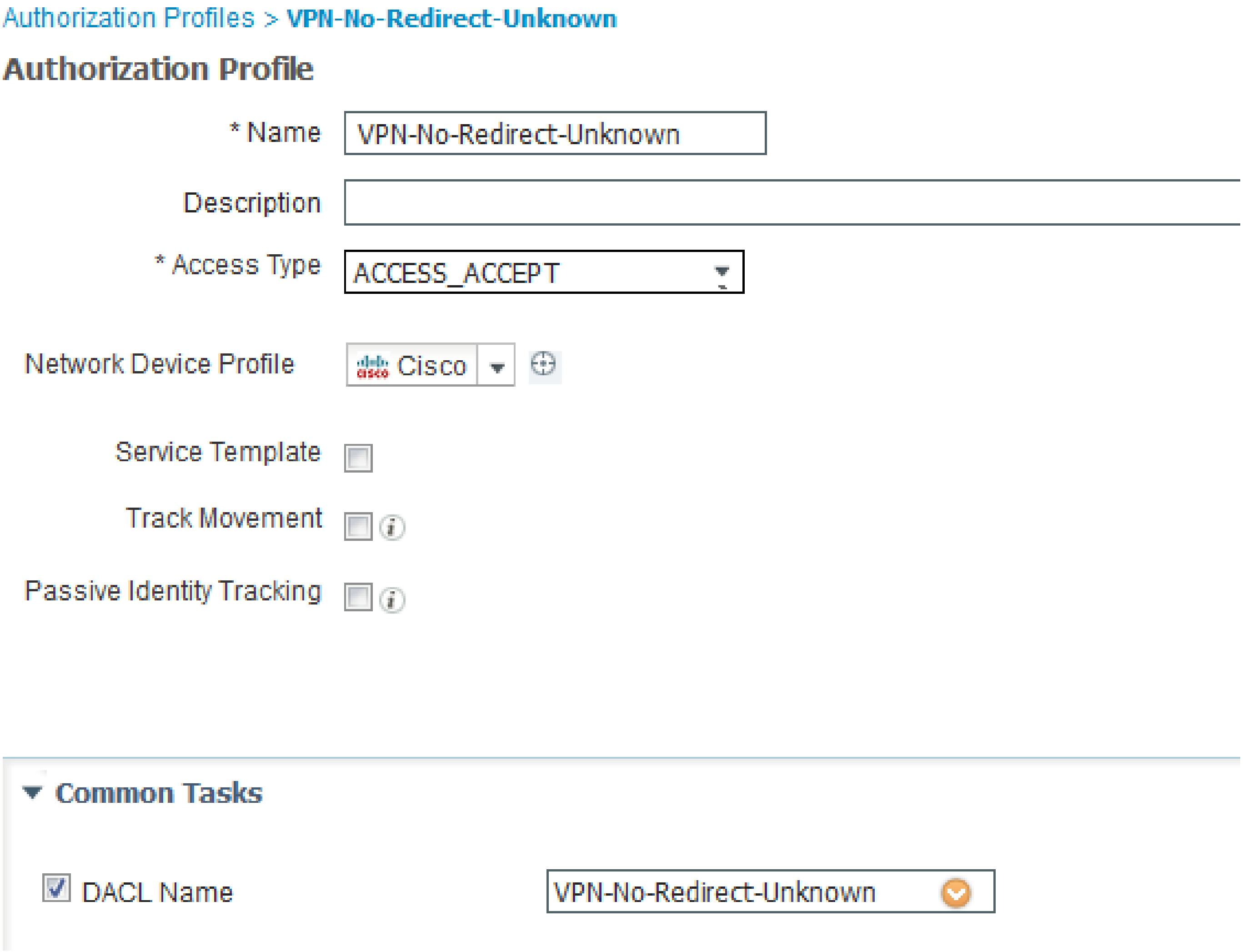
Figure 3-11

Step 2. Configure authorization profile.

As usual for posture two authorization profiles are required. The first one must contain any kind of network access restrictions (profile with DACL used in this example). This profile can be applied to the authentications for which posture status is not equal to compliant. The second authorization profile can contain just permit access and can be applied for sessions with posture status equal to compliance.

To create an authorization profile navigate to Policy > Policy Elements > Results > Authorization > Authorization Profiles.

Example of the restricted access profile:



Authorization Profiles > **VPN-No-Redirect-Unknown**

Authorization Profile

* Name: VPN-No-Redirect-Unknown

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

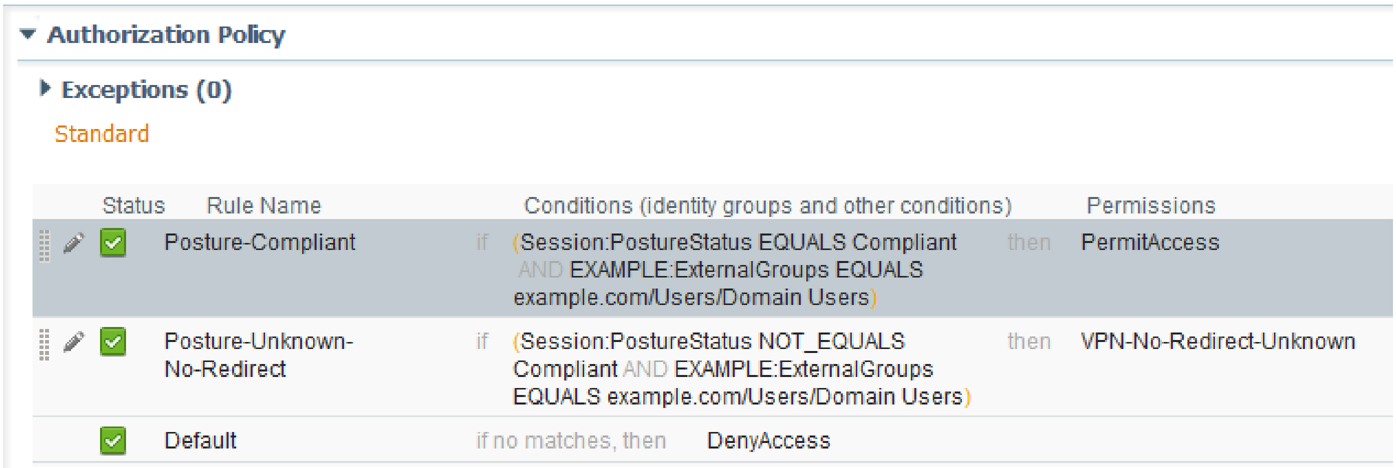
☑ DACL Name: VPN-No-Redirect-Unknown

Figure 3-12

In this example, the default ISE profile PermitAccess is used for the session after a successful posture status check.

Step 3. Configure authorization policy. During this step, two authorization policies must be created. One is to match the initial authentication request with unknown posture status and the second one is to assign full access after a successful posture process.

This is an example of simple authorization policies for this case:



Authorization Policy

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Posture-Compliant	if	(Session:PostureStatus EQUALS Compliant AND EXAMPLE:ExternalGroups EQUALS example.com/Users/Domain Users)	then	PermitAccess
✓	Posture-Unknown-No-Redirect	if	(Session:PostureStatus NOT_EQUALS Compliant AND EXAMPLE:ExternalGroups EQUALS example.com/Users/Domain Users)	then	VPN-No-Redirect-Unknown
✓	Default	if no matches, then	DenyAccess		

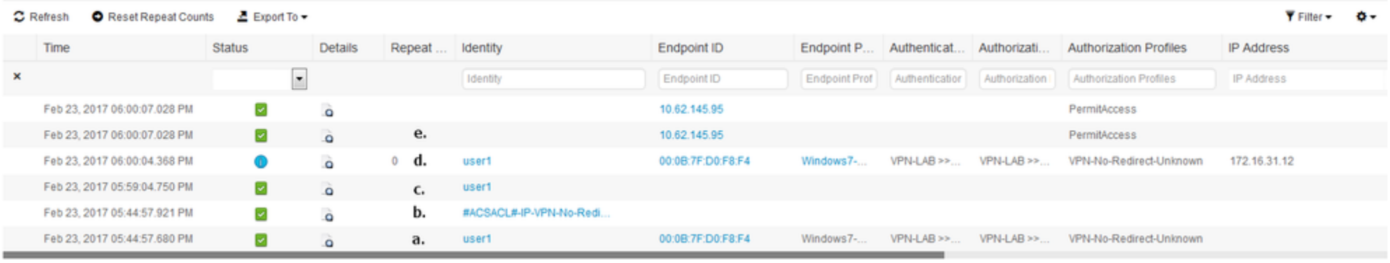
Figure 3-13

Configuration of Authentication policy is not a part of this document but you must keep in mind that before authorization policy processing successful authentication must happen.

Verify

Basic verification of the flow can consist of three main steps:

Step 1. Authentication flow verification.



Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Profiles	IP Address
Feb 23, 2017 06:00:07.028 PM	✓				10.62.145.95				PermitAccess	
Feb 23, 2017 06:00:07.028 PM	✓		e.		10.62.145.95				PermitAccess	
Feb 23, 2017 06:00:04.368 PM	●		0 d.	user1	00:0B:7F:D0:F8:F4	Windows7-...	VPN-LAB >>...	VPN-LAB >>...	VPN-No-Redirect-Unknown	172.16.31.12
Feb 23, 2017 05:59:04.750 PM	✓		c.	user1						
Feb 23, 2017 05:44:57.921 PM	✓		b.	#ACSACL#-IP-VPN-No-Redi...						
Feb 23, 2017 05:44:57.680 PM	✓		a.	user1	00:0B:7F:D0:F8:F4	Windows7-...	VPN-LAB >>...	VPN-LAB >>...	VPN-No-Redirect-Unknown	

Figure 4-1

1. Initial authentication. For this step, you can be interested in the validation of which the authorization profile has been applied. If an unexpected authorization profile has been applied, investigate a detailed authentication report. You can open this report with a click on the magnifying glass in the Details column. You can compare attributes in detailed authentication reports with conditions in the authorization policy which you expect to match.

2. DACL download event. This string is presented only in the case when the authorization profile selected for the initial authentication contains a DACL name.

3. Portal authentication - This step in the flow indicates that the SSO mechanism failed to locate the user session. This can happen due to multiple reasons:
   - NAD is not configured to send accounting messages or Framed IP address is not present in them
   - CPP portal FQDN has been resolved to the IP of the ISE node different from the node where the initial authentication has been processed
   - The client is located behind the NAT

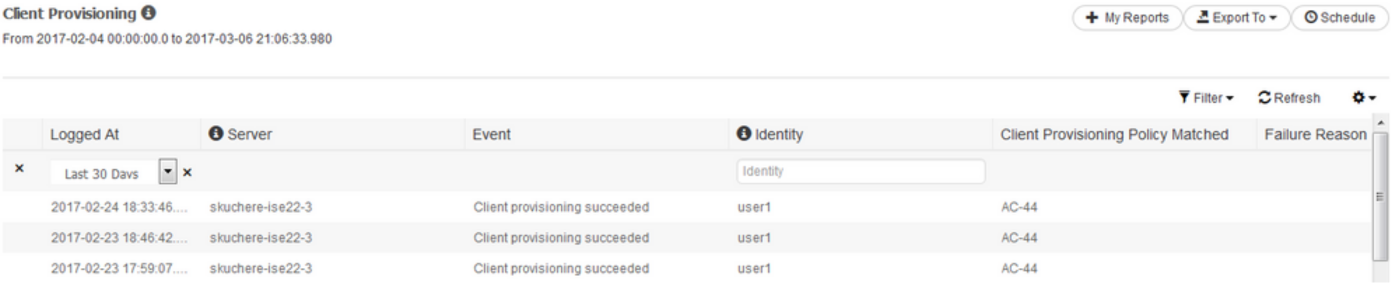
4. Session data change. In this particular example, the session state has changed from Unknown to Compliant.

5. COA to the network access device. This COA must be successful to push new authentication from the NAD side and new authorization policy assignments on the ISE side. If COA has failed, you can open a detailed report to investigate the reason. The most common issues with COA can be:
   - COA timeout - In such case either the PSN which has sent the request is not configured as a COA client on the NAD side, or the COA request has been dropped somewhere on the way.
   - COA negative ACK - Indicate that COA has been received by NAD but due to some reason COA operation cannot be confirmed. For this scenario, a detailed report must contain a more detailed explanation.

As ASA is used as a NAD for this example, you can see no subsequent authentication request for the user. This happens due to the fact ISE uses COA push for ASA which avoids VPN service interruption. In such a scenario, COA itself contains new authorization parameters, so reauthentication is not needed.

Step 2.Client provisioning policy selection verification - For this, you can run a report on ISE which can help you to understand which client provisioning policies were applied for the user.

Navigate to Operations > Reports Endpoint and Users > Client Provisioning and run the report for the date which you need.



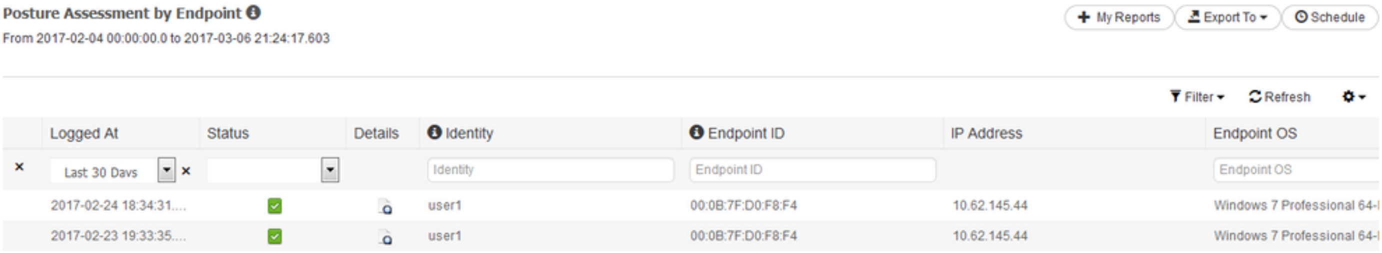
Client Provisioning
From 2017-02-04 00:00:00.0 to 2017-03-06 21:06:33.980

Logged At	Server	Event	Identity	Client Provisioning Policy Matched	Failure Reason
Last 30 Days			Identity		
2017-02-24 18:33:46....	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44	
2017-02-23 18:46:42....	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44	
2017-02-23 17:59:07....	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44	

Figure 4-2

With this report, you can verify what client provisioning policy was selected. Also, in case of failure, reasons must be presented in the Failure Reason column.

Step 3.Posture report verification - Navigate to Operations > Reports Endpoint and Users > Posture Assessment by Endpoint.



Posture Assessment by Endpoint
From 2017-02-04 00:00:00.0 to 2017-03-06 21:24:17.603

Logged At	Status	Details	Identity	Endpoint ID	IP Address	Endpoint OS
Last 30 Days			Identity	Endpoint ID		Endpoint OS
2017-02-24 18:34:31....	✓		user1	00:0B:7F:D0:F8:F4	10.62.145.44	Windows 7 Professional 64-I
2017-02-23 19:33:35....	✓		user1	00:0B:7F:D0:F8:F4	10.62.145.44	Windows 7 Professional 64-I

Figure 4-3

You can open a detailed report from here for each particular event to check, for example, to which session ID this report belongs, which exact posture requirements were selected by ISE for the endpoint and the status for each requirement.

Troubleshoot

General Information

For posture process troubleshooting, these ISE components must be enabled to debug on the ISE nodes where the posture process can happen:

- client-webapp - The component responsible for agent provisioning. Target log files guest.log and ise-psc.log.
- guestacess - The component responsible for client provisioning portal component and session owner lookup (when the request comes to the wrong PSN). Target log file - guest.log.
- provisioning - The component responsible for client provisioning policy processing. Target log file - guest.log.
- posture - All posture-related events. Target log file - ise-psc.log.

For client-side troubleshooting, you can use these:

- acisensa.log -In case of client provisioning failure on the client side, this file is created in the same folder to which NSA has been downloaded (downloads directory for Windows normally).
- AnyConnect_ISEPosture.txt - This file can be found in the DART bundle in the directory Cisco AnyConnect ISE Posture Module. All information about ISE PSN discovery and general steps of posture flow is logged into this file.

Troubleshooting Common Problems

SSO Related Issues

In case of a successful SSO, you can see these messages in the ise-psc.log, this set of messages indicates that session lookup has finished successfully and authentication on the portal can be skipped.

<#root>

```
2016-11-09 15:07:35,951 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu

looking for Radius session with input values : sessionId: null, MacAddr: null, ipAddr: 10.62.145.121


2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu

Found session c0a801010002600058232bb8 using ipAddr 10.62.145.121
```

Text Window 5-1

You can use the endpoint IP address as a search key to find this information.

A bit later in the guest log, you must see that authentication has been skipped:

<#root>

```
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] guestaccess.flowmanager.step.cp.CPI
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] com.cisco.ise.portalSessionManager.
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] com.cisco.ise.portalSessionManager.
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] guestaccess.flowmanager.step.cp.CPI

Login step will be skipped, as the session =c0a801010002600058232bb8 already established for mac address

2016-11-09 15:07:36,066 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cpm.guestaccess.flowmanager.process
```

Text Window 5-2

In case the SSO does not work, the ise-psc log file contains information about session lookup failure:

<#root>

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRu

looking for session using IP 10.62.145.44

2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cisco.cpm.posture.runtime.PostureRu

No Radius session found
```

Text Window 5-3

In the guest.log in such a case, you must see full user authentication on the portal:

<#root>

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.flowmanager.step.St
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.flowmanager.step.St
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.flowmanager.step.St

Returning next step =LOGIN

2017-02-23 17:59:00,780 INFO [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.flowmanager.step.Ste
```

Text Window 5-4

In case of authentication failures on the portal, you must focus on the portal configuration verification - Which identity store is in use? Which groups are authorized for login?

Troubleshoot Client Provisioning Policy Selection

In case of client provisioning policies failures or incorrect policy processing, you can check the guest.log file for more details:

<#root>

```
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.C


2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.common.utils.OSMappe
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.common.utils.OSMappe
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.C
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.C
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.C
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.C
2017-02-23 17:59:07,505 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.C

:user1:- CP Policy Status =SUCCESS, needToDoVlan=false, CoaAction=NO_COA
```

Text Window 5-5

In the first string, you can see how information about the session is injected into the policy selection engine, in case of no policy match or incorrect policy match, you can compare attributes from here with your client provisioning policy configuration. The last string indicates the policy selection status.

Troubleshoot Posture Process

On the client side, you must be interested in the investigation of the probes and their results. This is an example of a successful stage 1 probe:

```
******************************************

Date : 02/23/2017
Time : 17:59:57
Type : Unknown
Source : acise

Description : Function: Target::Probe
Thread Id: 0x4F8
File: SwiftHttpRunner.cpp
Line: 1415
Level: debug

PSN probe skuchere-ise22-cpp.example.com with path /auth/status, status is -1..

******************************************
```

Text Window 5-6

At this stage, PSN returns to AC information about the session owner. You can see these couple of messages later:

```
******************************************

Date : 02/23/2017
Time : 17:59:58
Type : Unknown
Source : acise

Description : Function: Target::probeRecentConnectedHeadEnd
Thread Id: 0xBE4
File: SwiftHttpRunner.cpp
Line: 1674
Level: debug

Target skuchere-ise22-2.example.com, posture status is Unknown..

******************************************
```

Text Window 5-7

Session owners return to the agent all the required information:

```
******************************************

Date : 02/23/2017
Time : 17:59:58
Type : Unknown
Source : acise

Description : Function: SwiftHttpRunner::invokePosture
Thread Id: 0xFCC
File: SwiftHttpRunner.cpp
Line: 1339
Level: debug

MSG_NS_SWISS_NEW_SESSION, <?xml version="1.0" ?>
<root>
 <IP></IP>
 <FQDN>skuchere-ise22-2.example.com</FQDN>
 <PostureDomain>posture_domain</PostureDomain>
 <sessionId>c0a801010009e00058af0f7b</sessionId>
 <configUri>/auth/anyconnect?uuid=106a93c0-9f71-471c-ac6c-a2f935d51a36</configUri>
 <AcPackUri>/auth/provisioning/download/81d12d4b-ff58-41a3-84db-5d7c73d08304</AcPackUri>
 <AcPackPort>8443</AcPackPort>
 <AcPackVer>4.4.243.0</AcPackVer>
 <PostureStatus>Unknown</PostureStatus>
 <PosturePort>8443</PosturePort>
 <PosturePath>/auth/perfigo_validate.jsp</PosturePath>
 <PRAConfig>0</PRAConfig>
 <StatusPath>/auth/status</StatusPath>
 <BackupServers>skuchere-ise22-1.example.com,skuchere-ise22-3.example.com</BackupServers>
</root>
.

******************************************
```

Text Window 5-8

From the PSN side, you can focus on these messages in the guest.log when you expect the initial request that comes to the node does not own the session:

<#root>

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
```

```
mac_list from http request ==> 00:0B:7F:D0:F8:F4,00:0B:7F:D0:F8:F4
```

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
```

```
iplist from http request ==> 172.16.31.12,10.62.145.95
```

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,368 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,369 ERROR [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
```

```
Session Info is null
```

```
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
```

```
Performing MNT look up for macAddress ==> 00-0B-7F-D0-F8-F4
```

```
2017-02-23 17:59:56,539 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
```

```
Performed MNT lookup, found session 0 with session id c0a801010009e00058af0f7b
```

```
2017-02-23 17:59:56,539 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
```

Text Window 5-9

Here you can see that PSN first tries to find a session locally, and after failure initiates a request to MNT with the use of the IPs and MACs list to locate the session owner.

A little bit later you must see a request from the client on the correct PSN:

<#root>

```
2017-02-23 17:59:56,790 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
```

```
ooking for session using session ID: null, IP addrs: [172.16.31.12, 10.62.145.95], mac Addrs [00:0B:7F:D
```

```
2017-02-23 17:59:56,790 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,791 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,792 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,792 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
```

```
Found session c0a801010009e00058af0f7b using ipAddr 172.16.31.12
```

Text Window 5-10

As a next step, PSN performs client provisioning policy lookup for this session:

<#root>

```
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] com.cisco.cpm.swiss.SwissServer -:::
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,795 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 17:59:58,203 DEBUG [http-bio-10.48.30.41-8443-exec-8][] com.cisco.cpm.swiss.SwissServer -:::
2017-02-23 17:59:58,907 DEBUG [http-bio-10.48.30.41-8443-exec-10][] cisco.cpm.posture.util.AgentUtil -:
```

```
Increase MnT counter at CP:ClientProvisioning.ProvisionedResource.AC-44-Posture
```

Text Window 5-11

In the next step, you can see the process of posture requirements selection. At the end of the step, a list of requirements is prepared and returned to the agent:

<#root>

```
2017-02-23 18:00:00,372 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureHan
```

```
About to query posture policy for user user1 with endpoint mac 00-0b-7f-d0-f8-f4
```

```
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureMan
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,432 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePol
2017-02-23 18:00:03,884 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cpm.posture.runtime.agent.AgentXmlGen
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cpm.posture.runtime.agent.AgentXmlGen
```

```
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cpm.posture.runtime.agent.AgentXmlGen
2017-02-23 18:00:04,069 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureHand
 <version>ISE: 2.2.0.470</version>
 <encryption>0</encryption>
 <package>
 <id>10</id>
 <name>WinDefend</name>
 <description>Enable WinDefend</description>
 <version/>
 <type>3</type>
 <optional>0</optional>
 <action>3</action>
 <check>
 <id>WinDefend</id>
 <category>3</category>
 <type>301</type>
 <param>WinDefend</param>
 <operation>running</operation>
 </check>
 <criteria>(WinDefend)</criteria>
 </package>
</cleanmachines>
```

Text Window 5-12

Later, you can see that the posture report was received by PSN:

```
2017-02-23 18:00:04,231 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureHan
2017-02-23 18:00:04,231 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureHan
```

Text Window 5-13

At the end of the flow, ISE marks the endpoint as compliant and initiates COA:

```
2017-02-23 18:00:04,272 INFO [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureMana
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureCoA
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureCoA
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureCoA
2017-02-23 18:00:04,273 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureCoA
2017-02-23 18:00:04,273 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureCoA
```

Text Window 5-14