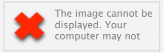
CCNP Security - SISAS
Posture Assessment

Posture Services

- Posture Policy defines the health requirements of endpoints
- Through posture policies, ISE defines a Windows/Mac endpoint compliance requirements
  - Antivirus, Antispyware, firewall, OS updates
  - Processes running, file existence, registry entries
- ISE collects endpoint data and matches it against its posture policies
- Endpoint data collected through
  - NAC Agent
  - AnyConnect Posture module available in AnyConnect 4.0



NAC Agent Overview

- NAC Agent
  - Temporary web agent based on ActiveX or Java (Windows)
    - Limited remediation
  - Permanent agent (Windows and Mac)
    - Automatic remediation
- NAC Agent compliance module (OPSWAT) used for antivirus and antispyware vendor support
- NAC Permanent Agent deployment options
  - Manual installation, not scalable
  - Unattended installation, customization available
  - ISE Client Provisioning Policy
    - Can also be used to automatically update NAC Agent or compliance module

The image cannot be displayed. Your computer may not

NAC Agent Connectivity Requirements

- NAC Agent communicates directly with ISE
  - Supplicant requires IP connectivity to ISE
  - NAD is completely bypassed, makes sense as it does not understand posture data
- TCP 8443 to ISE
  - Required if NAC Agent is installed through CPP
- UDP / TCP 8909 to ISE
  - Required for NAC Agent wizard installation via CPP
- UDP / TCP 8905 to ISE
  - Used by SWISS protocol (report collected data to ISE)
  - Required for ISE discovery and NAC Agent update
- ISE no longer uses legacy port 8906 for SWISS protocol

The image cannot be displayed. Your computer may not

Posture Services

- » Posture status options for an endpoint
  - Unknown, no data was collected from the endpoint
    - Usually means NAC Agent is not installed
    - Could be that it is not running or does not have ISE connectivity
  - Noncompliant, at least one requirement is not satisfied
    - Remediation process can be started automatically
  - Compliant, all requirements are satisfied
- » Posture status is used as condition in authorization policies
  - Network access is thus granted based on the health / security state of the endpoint

The image cannot be displayed. Your computer may not

Posture Assessment Work Flow

» How AAA order of processing is changed

- Supplicant Authentication
- Initial Authorization Policy pushed (posture status Unknown)
- Posture Discovery and Assessment starts
    - Posture data is received by ISE from NAC Agent
    - Posture state is changed to Compliant or Noncompliant
- ISE triggers CoA requesting endpoint re-authentication
- Supplicant Authentication same as in first step
- Intermediate authorization is applied if posture status is Noncompliant
    - Remediation starts, fixes problems, posture status changes to Compliant
    - ISE triggers CoA requesting endpoint re-authentication
- Final authorization is applied if posture status is Compliant

Posture Configuration Steps on Supplicant

- Install NAC Agent
  - Ideally, provision the FQDN of ISE PSN, to avoid ISE dynamic discovery
  - FQDN automatically provisioned if Agent installed via CPP
- ISE Discovery process
  - HTTP discovery probe on port 80 to ISE PSN, if configured
  - HTTPS discovery probe on port 8905 to ISE PSN, if configured
  - HTTP discovery probe on port 80 to default gateway
  - HTTPS reconnect probe on 8905 to previously contacted ISE PSN
- To avoid endpoint being quarantined for remediation
  - Ensure endpoint satisfies security policies configured on ISE

Posture Configuration Steps on NAD

- NAD is not aware of the posture process
- NAD just receives authentication status and authorization to be applied from ISE
- Allow NAC Agent connectivity with ISE
  - Requires static pre-authentication ACL

Posture Configuration Steps on ISE

- CoA is enabled by default for posture assessment
- Configure posture policies
  - Per operating system
  - Per group of users
- Configure authorization policies with posture status as condition
  - For Unknown status, redirect to client provisioning portal
  - For Noncompliant status, restrict access for remediation to work
  - For Compliant status, grant network access as desired
- Optionally configure client provisioning policies
  - Only when NAC Agent has not been pre-deployed
  - Required downloading of NAC Agent and compliance module to ISE

Q&A