CHAPTER 1

Overview of Cisco ISE

Cisco Identity Services Engine (ISE) is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. The unique architecture of Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. The administrator can then use that information to make proactive governance decisions by tying identity to various network elements including access switches, wireless LAN controllers (WLCs), virtual private network (VPN) gateways, and data center switches. Cisco ISE is a key component of the Cisco Security Group Access Solution.

Cisco ISE is a consolidated policy-based access control system that incorporates a superset of features available in existing Cisco policy platforms. Cisco ISE performs the following functions:

- Combines authentication, authorization, accounting (AAA), posture, and profiler into one appliance
- Provides for comprehensive guest access management for the Cisco ISE administrator, sanctioned sponsor administrators, or both
- Enforces endpoint compliance by providing comprehensive client provisioning measures and assessing device posture for all endpoints that access the network, including 802.1X environments
- Provides support for discovery, profiling, policy-based placement, and monitoring of endpoint devices on the network
- Enables consistent policy in centralized and distributed deployments that allows services to be delivered where they are needed
- Employs advanced enforcement capabilities including security group access (SGA) through the use of security group tags (SGTs) and security group access control lists (SGACLs)
- Supports scalability to support a number of deployment scenarios from small office to large enterprise environments

The following key functions of Cisco ISE enable you to manage your entire access network.

Provide Identity-Based Network Access

The Cisco ISE solution provides context-aware identity management in the following areas:

- Cisco ISE determines whether users are accessing the network on an authorized, policy-compliant device.
- Cisco ISE establishes user identity, location, and access history, which can be used for compliance and reporting.
- Cisco ISE assigns services based on the assigned user role, group, and associated policy (job role, location, device type, and so on).
- Cisco ISE grants authenticated users with access to specific segments of the network, or specific applications and services, or both, based on authentication results.

For more information, see Chapter 4, "Managing Identities and Admin Access."

Manage Various Deployment Scenarios

You can deploy Cisco ISE across an enterprise infrastructure, supporting 802.1X wired, wireless, and virtual private networks (VPNs).

The Cisco ISE architecture supports both stand-alone and distributed (also known as "high-availability" or "redundant") deployments where one machine assumes the primary role and another "backup" machine assumes the secondary role. Cisco ISE features distinct configurable personas, services, and roles, which allow you to create and apply Cisco ISE services where they are needed in the network. The result is a comprehensive Cisco ISE deployment that operates as a fully functional and integrated system.

You can deploy Cisco ISE nodes with one or more of the Administration, Monitoring, and Policy Service personas—each one performing a different vital part in your overall network policy management topology. Installing Cisco ISE with an Administration persona allows you to configure and manage your network from a centralized portal to promote efficiency and ease of use.

You can also choose to deploy the Cisco ISE platform as an Inline Posture node to perform policy enforcement and execute Change of Authorization (CoA) requests where users are accessing the network via WLCs and/or VPN concentrators that do not support the necessary functionality to facilitate Cisco ISE policy management.

For more information, see:

- Chapter 9, "Setting Up Cisco ISE in a Distributed Environment"
- Chapter 10, "Setting Up Inline Posture"

Provide Basic User Authentication and Authorization

User authentication policies in Cisco ISE enable you to provide authentication for a number of user login session types using a variety of standard authentication protocols including, but not limited to, Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), Protected Extensible Authentication Protocol (PEAP), and Extensible Authentication Protocol (EAP). Cisco ISE specifies the allowable protocol(s) that are available to the network devices on which the user tries to authenticate and specifies the identity sources from which user authentication is validated.

Cisco ISE allows for a wide range of variables within authorization policies to ensure that only authorized users can access the appropriate resources when they access the network. The initial release of Cisco ISE supports only RADIUS-governed access to the internal network and its resources.

At the most fundamental level, Cisco ISE supports 802.1X, MAC authentication bypass (MAB), and browser-based Web authentication login for basic user authentication and access via both wired and wireless networks. Upon receiving an authentication request, the "outer part" of the authentication policy is used to select the set of protocols that are allowed to be used when processing the request. Then, the "inner part" of the authentication policy is used to select the identity source that is used to authenticate the request. The identity source may consist of a specific identity store or an identity store sequence that lists a set of accessible identities until the user received a definitive authorization response.

Once authentication succeeds, the session flow proceeds to the authorization policy. (There are also options available that allow Cisco ISE to process the authorization policy even when the authentication did not succeed.) Cisco ISE enables you to configure behavior for "authentication failed," "user not found," and "process failed" cases, and also to decide whether to reject the request, drop the request (no response is issued), or continue to the authorization policy. In cases where Cisco ISE continues to perform authorization, you can use the "AuthenicationStaus" attribute in the "NetworkAccess" dictionary to incorporate the authentication result as part of the authorization policy.

The authorization policy result is Cisco ISE assigning an authorization profile that might also involve a downloadable ACL specifying traffic management on the network policy enforcement device. The downloadable ACL specifies the RADIUS attributes that are returned during authentication and that define the user access privileges granted once authenticated by Cisco ISE.

For more information, see:

- Chapter 16, "Managing Authentication Policies"
- Chapter 17, "Managing Authorization Policies and Profiles"

Support for FIPS 140-2 Implementation

Cisco ISE, Release 1.1 introduces Federal Information Processing Standard (FIPS) 140-2 Common Criteria EAL2 compliance. FIPS 140-2 is a United States government computer security standard that is used to accredit cryptographic modules. Cisco ISE uses an embedded FIPS 140-2 implementation using validated C3M and Cisco ACS NSS modules, per FIPS 140-2 Implementation Guidance section G.5 guidelines.

In addition, the FIPS standard places limitations on the use of certain algorithms, and in order to enforce this standard, you must enable FIPS operation in Cisco ISE. Cisco ISE enables FIPS 140-2 compliance via RADIUS Shared Secret and Key Management measures and provides SHA-256 encryption and decryption capabilities for certificates. While in FIPS mode, any attempt to perform functions using a non-FIPS compliant algorithm fails, and, as such, certain authentication functionality is disabled.

When you turn on FIPS mode in Cisco ISE, the following functions are affected:

- IEEE 802.1X environment
  - EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
  - EAP-Transport Layer Security (EAP-TLS)
  - PEAP
  - RADIUS

Note Other protocols like EAP-Message Digest 5 (EAP-MD5), Lightweight Extensible Authentication Protocol (LEAP), and PAP are not compatible with a FIPS 140-2 compliant system and are disabled while Cisco ISE is in FIPS mode.

- Secure Shell (SSH) clients can only use SSHv2
- Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL)
- Inline Posture node RADIUS Key Wrap
- HTTPS protocol communication for both Administrator ISE nodes and Inline Posture nodes

For more information, see the specific FIPS 140-2 configuration options:

- Chapter 6, "Managing Network Devices"
- Chapter 8, "Administering Cisco ISE" (Enabling FIPS Mode in Cisco ISE, page 8-2)
- Chapter 13, "Managing Certificates"
- Chapter 16, "Managing Authentication Policies"

Support Common Access Card Functions

Cisco ISE supports U.S. government users who authenticate themselves using Common Access Card (CAC) authentication devices. A CAC is an identification badge with an electronic chip containing a set of X.509 client certificates that identify a particular employee of, for example, the U.S. Department of

Defense (DoD). Access via the CAC requires a card reader into which the user inserts the card and enters a PIN. The certificates from the card are then transferred into the Windows certificate store, where they are available to applications such as the local browser running Cisco ISE.

Benefits of using a CAC card to authenticate include these:

- Common Access Card X.509 certificates are the identity source for 802.1X EAP-TLS authentication.
- Common Access Card X.509 certificates are also the identity source for authentication and authorization to Cisco ISE administration.

Cisco ISE only supports login to the administrator user interface. It does not support CAC authentication for the following access methods:

- You cannot use CAC authentication login to manage the Cisco ISE Command Line Interface.
- External REST API (Monitoring and Troubleshooting) and Endpoint Protection Services APIs are outside the scope of the CAC authentication.
- Guest Services and Guest Sponsor Administration access does not support the CAC authentication method in Cisco ISE.

For more information on setting up Cisco ISE up for CAC authentication, see Chapter 8, “Administering Cisco ISE.”

Incorporate Client Posture Assessment

To ensure that the imposed network security measures remain relevant and effective, Cisco ISE enables you to validate and maintain security capabilities on any client machine that accesses the protected network. By employing posture policies that are designed to ensure that the most up-to-date security settings or applications are available on client machines, the Cisco ISE administrator can ensure that any client machine that accesses the network meets, and continues to meet, the defined security standards for enterprise network access. Posture compliance reports provide Cisco ISE with a snapshot of the compliance level of the client machine at the time of user login, as well as any time a periodic reassessment takes place.

Posture assessment and compliance takes place using one of the following agent types available in Cisco ISE:

- Cisco NAC Web Agent—A temporal agent the user installs on his/her system at the time of login that is no longer visible on the client machine once the login session terminates.
- Cisco NAC Agent—A persistent agent that, once installed, remains on a Windows or Mac OS X client machine to perform all user login and security compliance functions for Windows XP, Windows Vista, Windows 7, or Mac OS 10.5 and 10.6 clients, respectively.

For more information, see:

- Chapter 19, “Configuring Client Provisioning Policies”
- Chapter 20, “Configuring Client Posture Policies”

Define Sponsors and Manage Guest Sessions

Cisco ISE administrators and employees that are granted appropriate access to the Cisco ISE guest registration portal as guest sponsors can create temporary guest login accounts and specify available network resources to allow guests, visitors, contractors, consultants, and customers to access the network. Guest access sessions have expiration timers associated with them, so they are effective in controlling guest access to a specific day, time period, and so forth.

All aspects of a guest user session (including account creation and termination) are tracked and recorded in Cisco ISE so that you can provide audit information and troubleshoot session access, as necessary.

For more information, see:

- Chapter 21, "User Access Management"
- *Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1*

Manage Wireless and VPN Traffic with Inline Posture Nodes

Inline Posture nodes are gatekeeping nodes that enforce Cisco ISE access policies and handle CoA requests. After initial authentication (using EAP/802.1X and RADIUS), client machines must still go through posture assessment. The posture assessment process determines whether the client should be restricted, denied, or allowed full access to the network. When a client accesses the network through a WLC or VPN device, the Inline Posture node has the responsibility for the policy enforcement and CoA that the other network devices are unable to accommodate. It is for this reason that a Cisco ISE can be deployed as an Inline Posture node behind other network access devices on your network, such as WLCs and VPN concentrators.

For more information, see Chapter 10, "Setting Up Inline Posture."

Profile Endpoints on the Network

The Profiler service assists in identifying, locating, and determining the capabilities of all endpoints on your network (known as identities in Cisco ISE), regardless of their respective device types, in order to ensure and maintain appropriate access to your enterprise network. The Cisco ISE Profiler function uses a number of probes to collect attributes for all endpoints on your network, and pass them to the Profiler analyzer where the known endpoints are classified according to their associated policies and the identity groups.

For more information, see Chapter 18, "Configuring Endpoint Profiling Policies."

Install on a Variety of Hardware and VMware Platforms

Cisco ISE comes preinstalled on a range of physical appliances with various performance characteristics. The Cisco Application Deployment Engine (ADE) and Cisco ISE software run on either a dedicated Cisco ISE 3300 Series appliance or on a VMware server (Cisco ISE VM). The Cisco ISE software image does not support the installation of any other packages or applications on this dedicated platform. The inherent scalability of Cisco ISE allows you to add appliances to a deployment and increase performance and resiliency, as needed.

For more detailed information on hardware platforms and installing Cisco ISE, see the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*