firefly

Implementing Cisco Network Admission Control

Length
3 days

Format
Lecture/lab

Version
3.0

NAC

Course Description

Network Access Devices (NADs) enforce admission control policy on switches. These devices demand host security credentials and relay this information to policy servers, where network admission control decisions are made. Based on customer-defined policy, the network enforces the appropriate admission control decision. This 3-day, lab-intensive course teaches you how to implement network-based access control using Cisco routers, switches, and wireless APs.

Who Should Attend

This course is designed for network professionals who are responsible for implementing network security using Cisco Network Access Control.

Recommended Prerequisites

- CCSP certification or equivalent knowledge
- Basic knowledge of the Microsoft Windows operating system

Related Courses

- Securing Cisco Network Devices (SND)
- Securing Networks with Cisco Routers and Switches (SNRS)

Learning Objectives

After completing this course, you will be able to:

- Understand how Cisco NAC operates
- Configure Cisco Secure ACS to operate as a Cisco NAC AAA policy server
- Configure Cisco IOS routers, switches, and access points to act as Cisco NAC NADs
- Configure Cisco agents to act as Cisco NAC clients
- Configure a Trend Micro policy server to operate as an external Cisco NAC policy server

Implementing Cisco Network Admission Control

Course Outline

Module 1: Implementing Cisco Network Admission Control

Lesson 1: Understanding Cisco NAC
Introduction to Cisco Network Admission Control
Cisco NAC Components
NAC Deployment Comparisons
Understanding the Cisco NAC Posture Validation Process
Understanding the Cisco NAC Status Query Process
EAP-FAST
Protected Access Credential
Understanding Access Restrictions for Postured Clients
Understanding Cisco NAC Deployment Scenarios

Lesson 2: Configuring Cisco Secure ACS for Cisco NAC
Using Cisco Secure ACS as a Cisco NAC AAA Policy Server
NAC Features
Task 1: Install the Cisco Secure ACS Server
Task 2: Import Vendor AVPs
Task 3: Add a NAD AAA Client
Task 4: Configure the Administrator Interface and Admininstrator Access
Task 5: Install and Configure the Cisco Secure ACS Certificate
Task 6: Configure Global Authentication
Task 7: Configure Service Logs
Task 8: Configure Shared Profile Components
Task 9: Configure Posture Validation
Task 10: Configure Group and Vendor Attributes
Task 11: Create Network Access Profiles
Task 12: Configure a Clientless User, NRH, or NAH

Lesson 3: Configuring Cisco Routers for Cisco NAC
Using Cisco Routers as Cisco NAC Network Access Devices
Task 1: Configure AAA
Task 2: Configure a RADIUS Server
Task 3: Configure an Interface ACL
Task 4: Configure an Intercept ACL
Task 5: Configure a Cisco NAC Global Policy
Task 6: Configure the Cisco NAC Interface
Task 7: Configure Clientless Host (NAH or NRH) Support
Task 8: Set EAPoUDP Timers
Task 9: Enable a Cisco IOS HTTP Server
Task 10: Enable EAPoUDP Logging
Using Cisco IOS NAD Troubleshooting Commands

Lesson 4: Configuring Cisco Switches for Cisco NAC
Using Cisco Switches as Cisco NAC Network Access Devices
Common Switch Configurations
Configure AAA
Configure a RADIUS Server
Configure an Interface ACL
Configure a Cisco NAC Global Policy
Configure the Cisco NAC Interface
Configure Clientless Host Support (NAH or NRH)
Set EAPoUDP Timers
Enable a Cisco IOS HTTP Server
Enable EAPoUDP Logging
NAC L2 IP Commands
NAC L2 802.1x Commands
Using Cisco IOS Switch NAD Troubleshooting Commands

Implementing Cisco Network Admission Control