



CHAPTER 1

Overview

SNMP Version 3 provides secure communication of SNMP transactions with an SNMP agent by providing authentication and privacy options through the User-based Security Model (USM) and View-based Access Control Model (VACM). SNMP Versions 1 and 2c have no knowledge of the user for access control to MIBs, nor do they provide encrypted privacy options for authentication. VACM support has been deferred to a future release.

This chapter describes the installation, configuration, and use of CiscoWorks and several third-party tools that can communicate with the adaptive security appliance through SNMP Version 3 on a device running ASA 5500 series software Version 8.2(1) or higher.

The chapter includes the following sections:

- [Network Management Tools, page 1-1](#)
- [Network Topology, page 1-2](#)
- [Adaptive Security Appliance Setup, page 1-2](#)

Network Management Tools

This document describes the following network management tools:

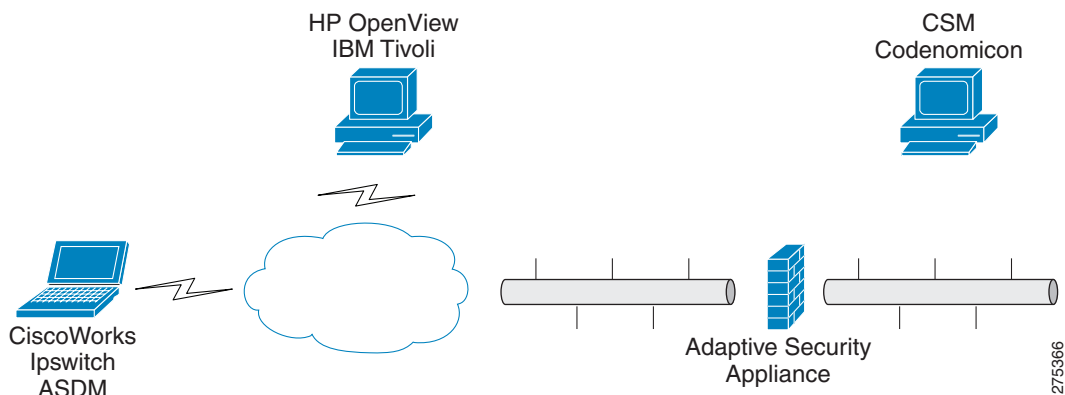
- Net-SNMP (CLI application)
- IWL SilverCreek, the SNMP Test Suite
- Ipswitch WhatsUp Gold
- HP OpenView NNM
- CiscoWorks for Windows LMS

Cisco has tested these tools for interoperability between the NMS and the adaptive security appliance.

Network Topology

Figure 1-1 shows the network topology for implementing SNMP Version 3.

Figure 1-1 Network Topology for SNMP Version 3 Implementation



Adaptive Security Appliance Setup

The adaptive security appliance requires that you configure the SNMP server group, the SNMP server user associated with the group, and the SNMP server host, which specifies the user for receiving SNMP traps.

To configure SNMP Version 3 operations, the required sequence of commands is as follows:

- **snmp-server group**
- **snmp-server user**
- **snmp-server host**

The following shows an example adaptive security appliance configuration:

```
hostname# snmp-server group authPriv v3 priv
hostname# snmp-server group authNoPriv v3 auth
hostname# snmp-server group noAuthNoPriv v3 noauth

hostname# snmp-server user md5des authPriv v3 auth md5 mysecretpass priv des passphrase
hostname# snmp-server user md5user authNoPriv v3 auth md5 mysecretpass
hostname# snmp-server user noauthuser noAuthNoPriv v3

hostname# snmp-server host mgmt 10.0.0.1 version 3 md5des
hostname# snmp-server host mgmt 10.0.0.2 version 3 md5des
hostname# snmp-server host mgmt 10.0.0.3 version 3 md5des

hostname# snmp-server location Anywhere, USA
hostname# snmp-server contact admin@example.com
hostname# snmp-server enable traps snmp authentication linkup linkdown coldstart
hostname# snmp-server enable traps syslog
hostname# snmp-server enable traps ipsec start stop
hostname# snmp-server enable traps entity config-change fru-insert fru-remove
hostname# snmp-server enable traps remote-access session-threshold-exceeded
```