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 Secure Firewall ASA through SNMP Version 3 on a device running ASA software Version 8.2(1) or higher.

The chapter includes the following sections:

Network Management Tools

This document describes the following network management tools:

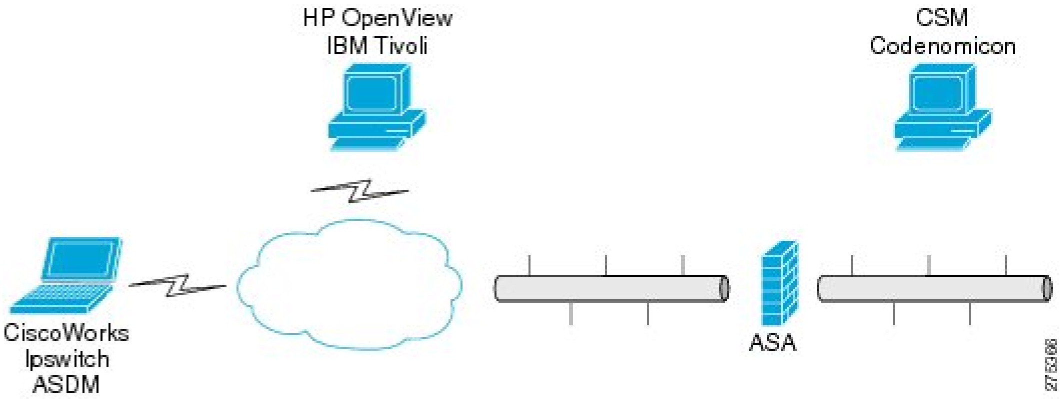
- Net-SNMP (CLI application)
- IWL SilverCreek, the SNMP Test Suite
- Ipswitch WhatsUp Gold
- HP OpenView NNM
- CiscoWorks for Windows LMS

Cisco has tested these tools for interoperability between the NMS and the ASA.

Network Topology

The following figure shows the network topology for implementing SNMP Version 3.

Figure 1: Network Topology for SNMP Version 3 Implementation



ASA Setup

The ASA 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 ASA configuration:

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

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

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

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