



HP Software Forum

THINGS CHANGE. BE READY.

JUNE 19 – 23, 2006

MIAMI BEACH, FLORIDA



Title: HP OpenView Network Node Manager
SPI for SNMPv3

Session #: 326

Speakers: Jeff Scheaffer, HP OpenView NSM
David Reid, SNMP Research



OpenView Forum
ADVOCACY • COMMUNITY • EDUCATION

The new *HP OpenView Network Node Manager SPI for SNMPv3* supports secure SNMP and SNMP management through firewalls.

This session provides an overview and discussion of secure network management, including:

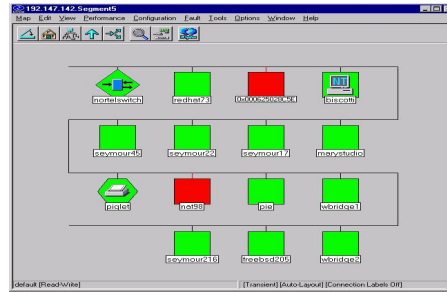
- the current Internet-Standard Management Framework;
- the security and administration features of SNMPv3;
- the technical architecture and configuration of the NNM SPI for SNMPv3;
- how to securely extend SNMP management through firewalls;
- elements of a complete solution.

The current Internet- Standard Management Framework

The security and administration features of SNMPv3

SNMP in One Slide

Manager

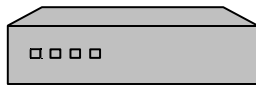


Requests

Responses

Notifications

Agents



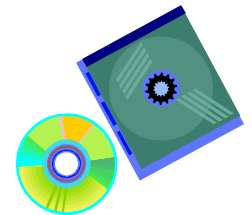
Networking Equipment



Servers



PCs



Software Applications

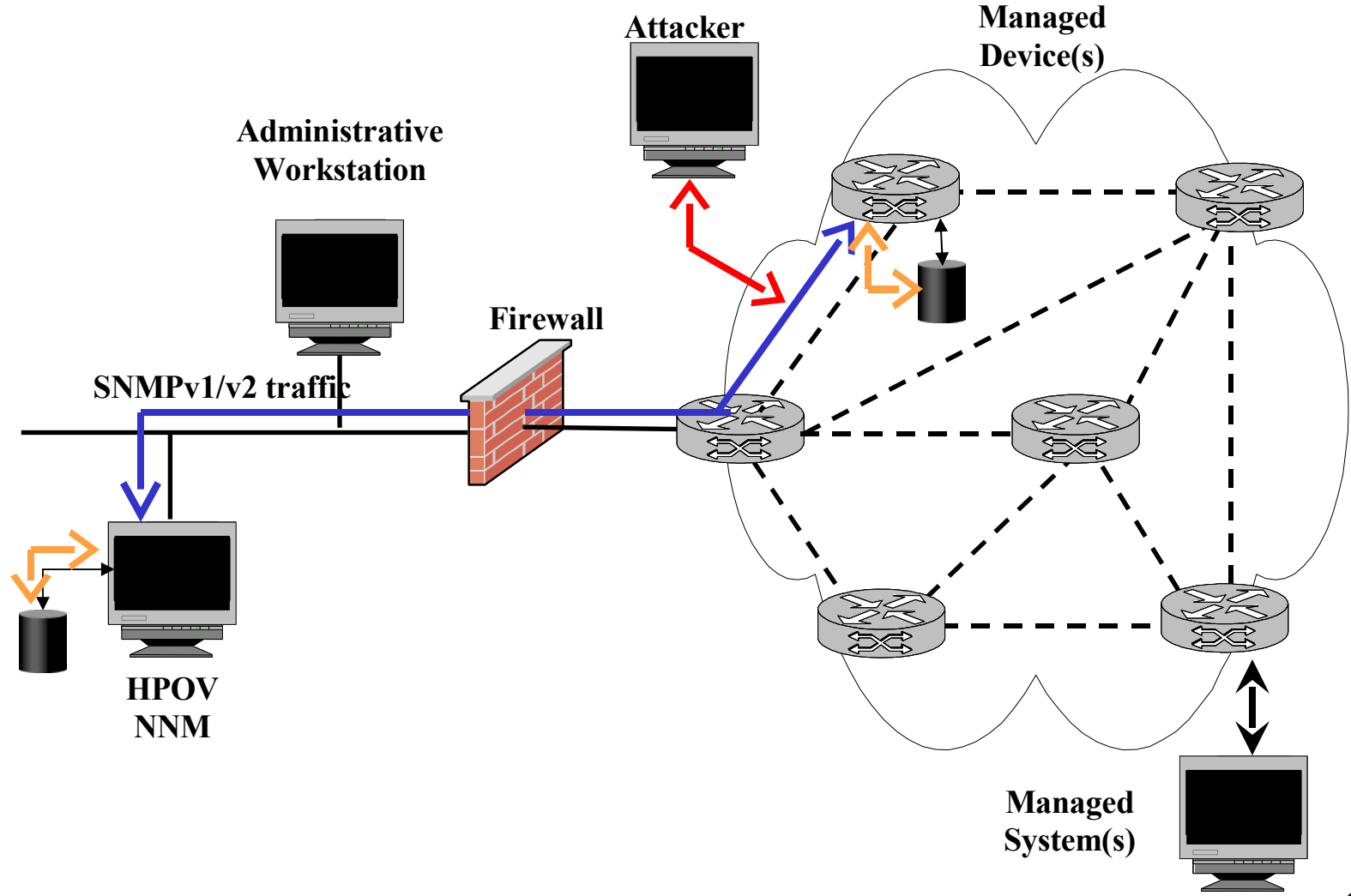
- ✓ Common organization structure for management information (SMI)
- ✓ One naming space for all management “objects” (MIB)
- ✓ Communications Protocol (SNMP)

Features of SNMPv3: Security and Administrative Framework

- Security
 - Authentication – who is doing the communicating
 - Privacy – protection from disclosure
 - Authorization – what operations are allowed (e.g., read, write, notify)
 - Access control – what information objects can be read or written
- Administrative framework to support the above

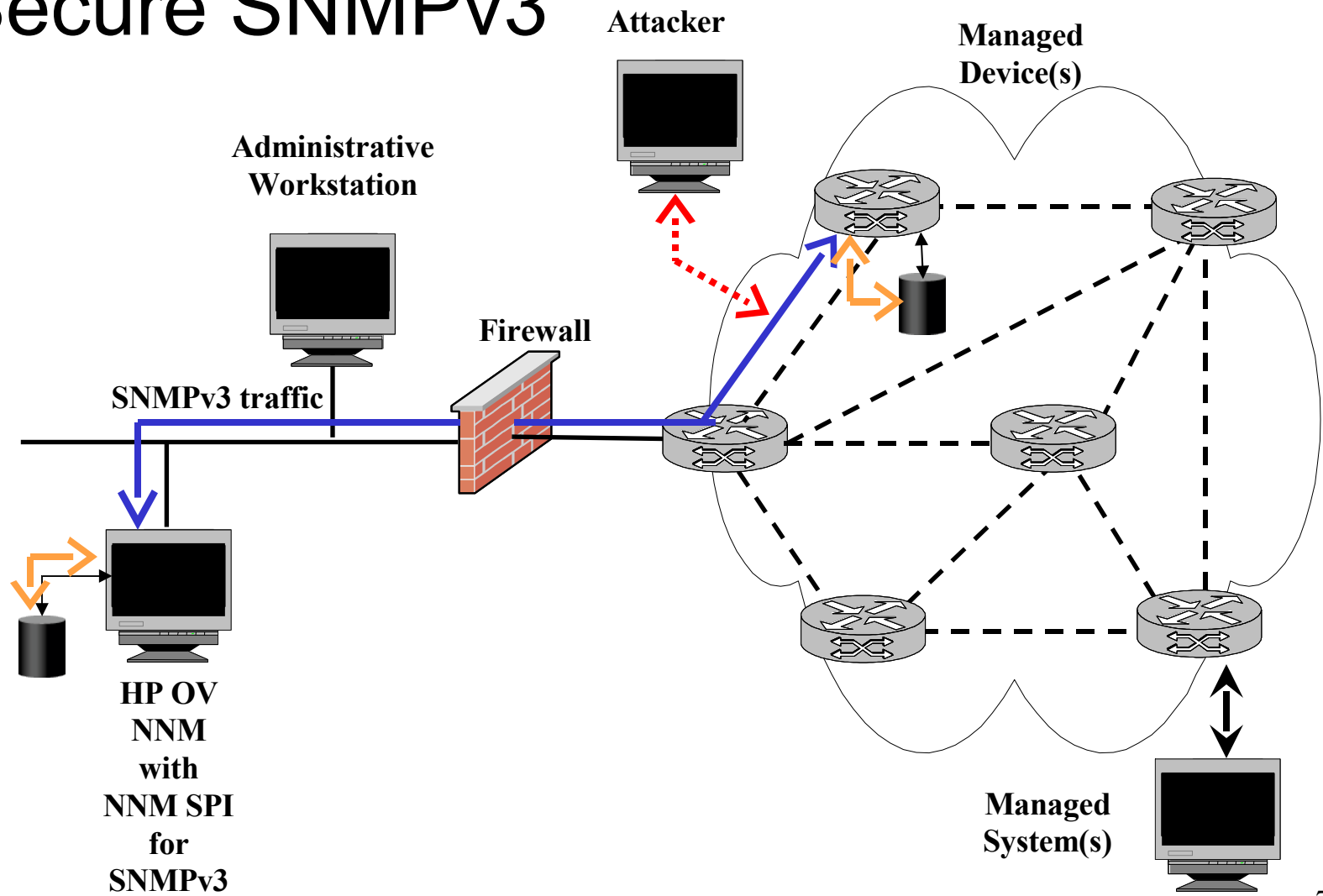


SNMPv1/SNMPv2c Not Secure





Secure SNMPv3



SNMPv3 Includes Everything in Versions 1 and 2c Plus...

- Authentication:
 User-based authentication of messages
- Privacy:
 The ability to encrypt management messages
- Authorization:
 The concept of users
- View-based access control:
 Restriction on what data may be read/written
- Administrative framework to support the above

Authentication

- The process of reliably determining the identity of the sender of a message
- Verify that the message received is the one sent
- Protects against following threats:
 - Masquerade (spoof sender)
 - Modification of information (change content)
 - Modification of message stream (timing, limited replay)
- Standard specifies MD5 and SHA1 for strong authentication
 - Private key model with localized keys
 - More than good enough for virtually all applications today

Privacy

- Protection from the unauthorized disclosure of data
- Encrypt SNMP payload for privacy
- Private key model with localized keys
- Standard specifies DES (56-bit)
- Standard is extensible for stronger cryptography
 - Triple-DES (168-bit keys)
 - AES (128, 192, and 256 bit keys)
 - ... Others possible ...

Authorization

- Each request is associated with a SNMPv3 “user” (system, person, or role)
- A user is a member of a group
- Mechanism to specify what each network manager (user) can do (read, write, notify)
- The management application determines how its “users” (operators) map to SNMPv3 “users”

Access Control

- Like authorization, access control is performed by group
- Every SNMPv3 “group” (and therefore every user) has three associated lists of what objects can be accessed on each device (read, write, notify)
- This is very fine grained, down to individual instances, if desired
- Simple or complex combinations
- Examples:
 - Read access to all network statistics
 - Read/write access to configure notifications (e.g., traps)

SNMPv3 Administrative Framework

- All of this configuration information is stored in Management Information Base (MIB) tables
- Administrative subsystems defined by standards
 - User-based Security Model (USM)
 - View-based Access Control Model (VACM)
- Standard supports remote configuration of:
 - Users
 - Groups
 - Views
 - Keys (generated from pass-phrases)
 - Older versions including community strings, if any

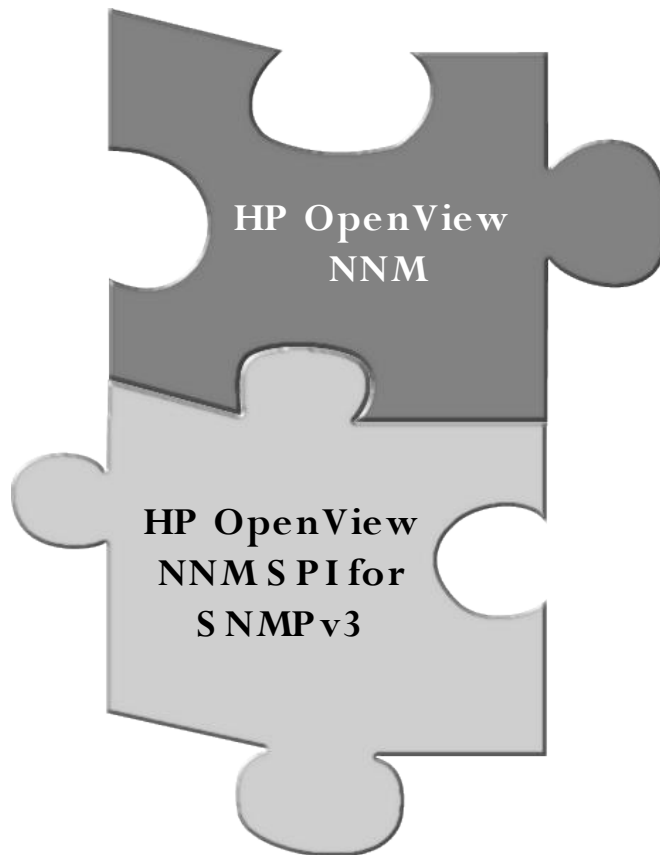
SNMPv3 Typical Deployment Scenarios

- A few “user” names are associated with management stations (e.g., ow1, nnmbldg4)
- Authentication used for all communications
- Both Authentication and Privacy used for sets
- Authentication and Privacy used for retrieval of sensitive information (e.g., routing tables)
- SNMP security configuration management is done by
 - Hand: Editing or copying over local configuration files
 - Security configuration distribution application(s) via SNMPv3 set requests

HP OpenView NNM and SNMPv3

- Desired Solution
 - Manage using familiar tools and procedures (e.g., NNM)
 - Manage using existing complementary applications
 - Manage using appropriate SNMP level
 - SNMPv1 and SNMPv2c for monitoring older devices in trusted environments
 - SNMPv3 for managing critical systems in less trusted regions
 - SNMPv3 for managing remote sites through less trusted regions
 - SNMPv3 for all configuration operations
 - Common repository for security configuration data

Security Solution



=





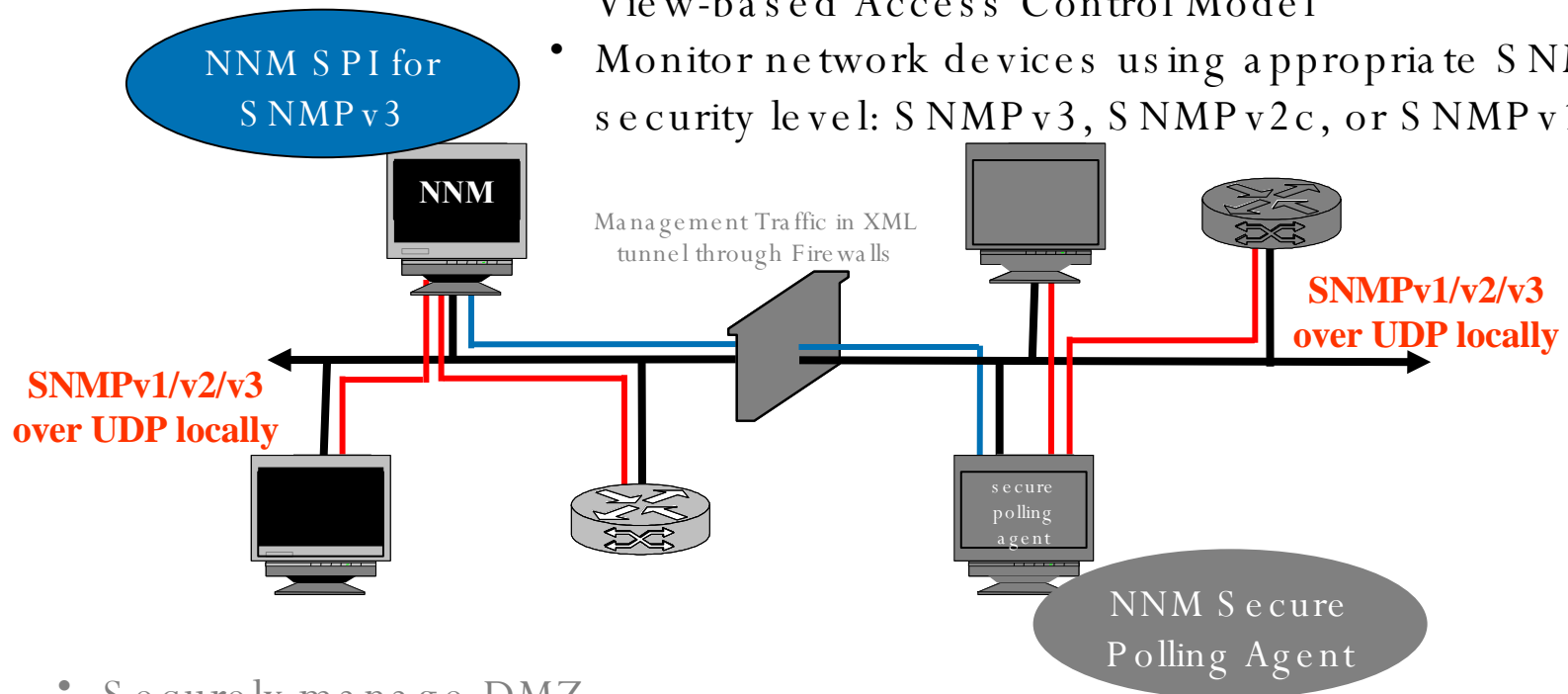
HP OpenView NNM SPI for SNMP v3

HP OpenView NNM SPI for SNMPv3

- Integration was jointly developed by HP and SNMP Research
- Maps outbound SNMP requests to SNMPv3 requests sent to target agent
- Converts SNMPv3 responses from agent and sends back to NNM
- Receives notifications (traps and informs)
- Includes security configuration datastore
- Includes SNMPv3 Configuration Wizard application

HP OpenView NNM SPI for SNMPv3

- S N M P v 3 S P I s supporting S N M P v 3 s t a n d a r d s :
- User-based Security Model
- View-based Access Control Model
- Monitor network devices using appropriate S N M P security level: S N M P v 3, S N M P v 2 c, or S N M P v 1



- Securely manage DMZ
- Manage S N M P v 1 / S N M P v 2 c / S N M P v 3 devices behind a fire wall
- Securely manage multiple isolated sites over insecure Internet infrastructure

s e c u r e S N M P
m a n a g e m e n t t h r o u g h
f i r e w a l l s

Management challenges presented by security firewalls

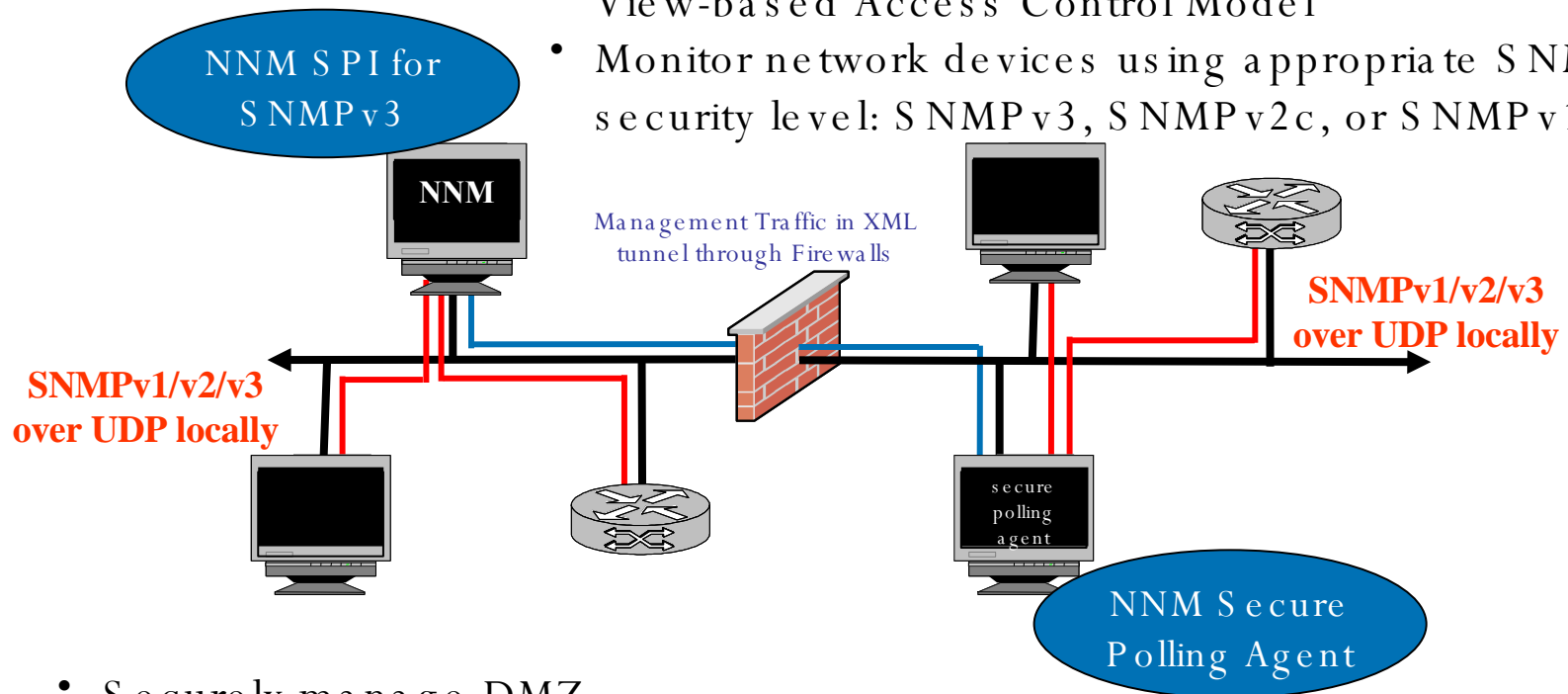
- Many sites continue to depend on legacy (i. e., SNMPv1 and SNMPv2c) SNMP versions which provide no security.
- Network administrators are reluctant to allow SNMP-based management through firewalls.
 - In many sites, nearly all UDP traffic is disallowed across firewalls
 - Many SNMP agents in managed devices are not adequately configured or configurable to restrict the management information they divulge.
- Many sites disable ICMP across firewalls

HP OpenView NNM Secure Polling Agent

- Manage securely to multiple isolated sites over insecure Internet infrastructure
- Manage SNMPv1/SNMPv2c devices behind a firewall
 - Preserve vast investment in SNMP-based management
 - Do not have to upgrade all devices inside the firewall
 - May want to upgrade to defend against threats from within
- Manage SNMPv3 devices behind a firewall that does not allow any SNMP traffic through the firewall

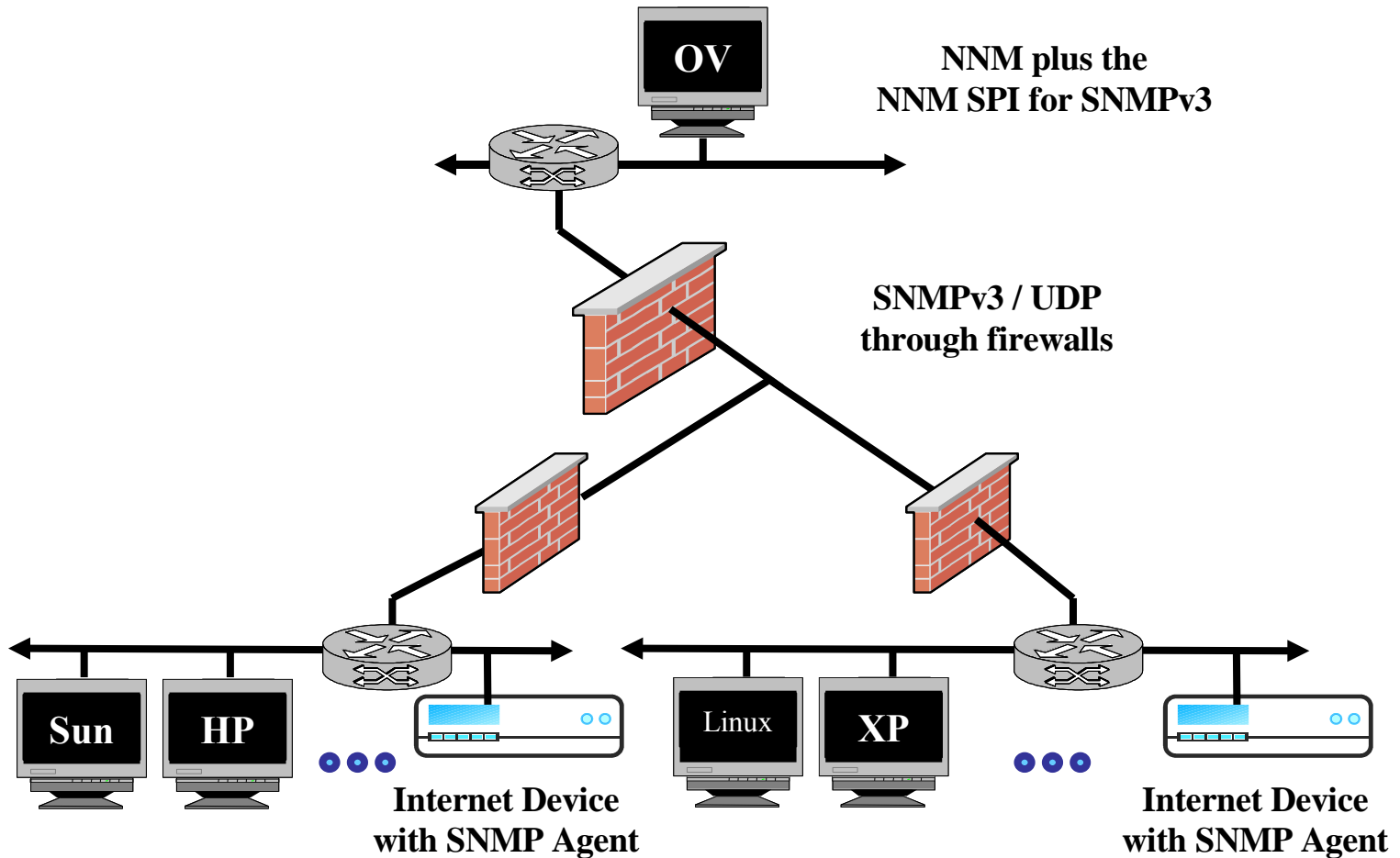
HP OpenView NNM Secure Polling Agent

- S N M P v 3 S P I s supporting S N M P v 3 s t a n d a r d s :
- User-based Security Model
- View-based Access Control Model
- Monitor network devices using appropriate S N M P security level: S N M P v 3, S N M P v 2 c, or S N M P v 1

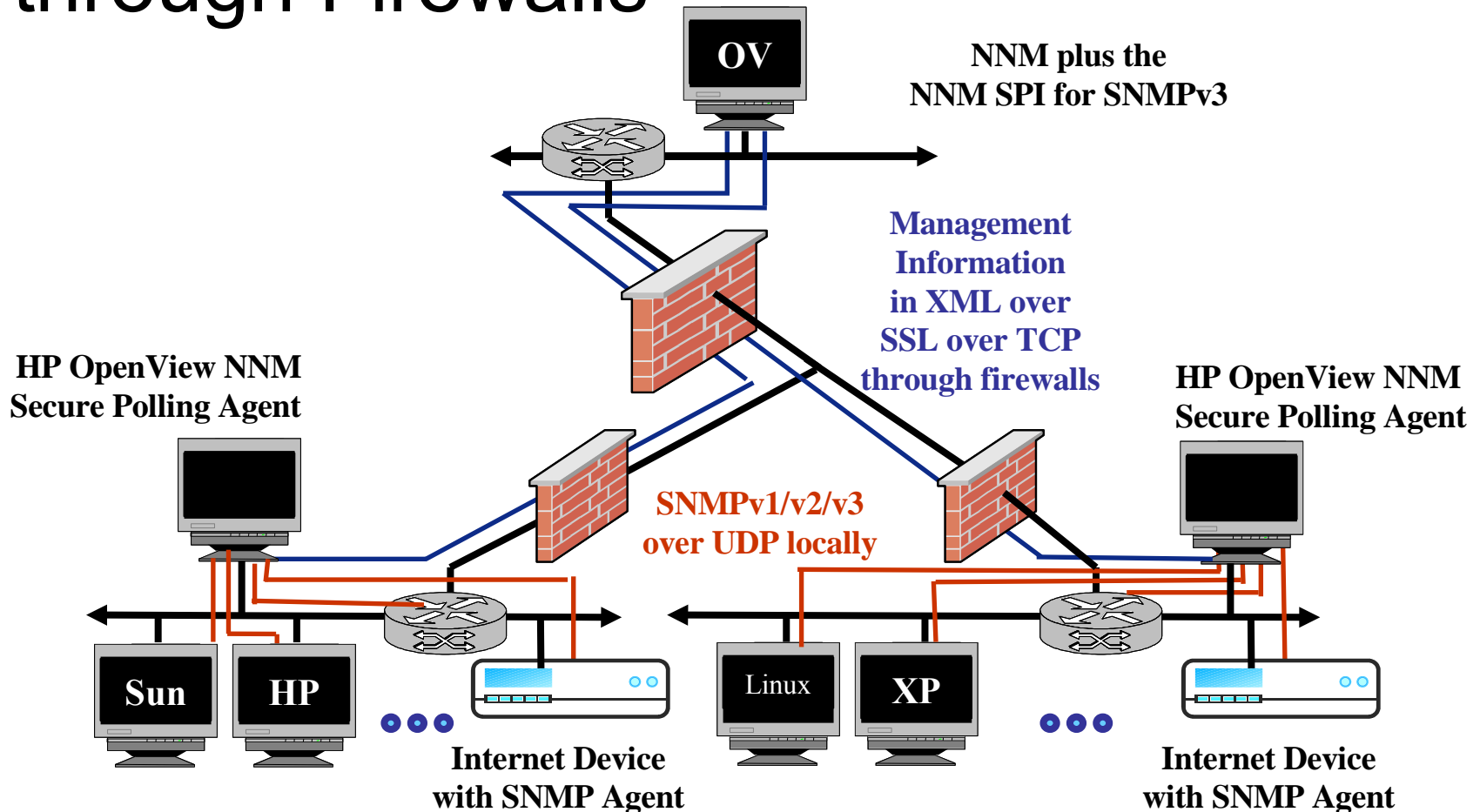


- Securely manage DMZ
- Manage S N M P v 1 / S N M P v 2 c / S N M P v 3 devices behind a fire wall
- Securely manage multiple isolated sites over insecure Internet infrastructure

SNMPv3 over UDP through Firewalls



Management Traffic in XML tunnel through Firewalls



Key Elements of a Complete Solution

- Secure agents
- Secure management applications
- Administrative policies
- Configuration management of users, keys, etc
- Coexist with legacy systems

Secure Agents

- SNMPv3 agents available on most networking devices
- SNMPv3 agents available on most open operating systems and embedded real-time operating systems
- For integrated network and system management, smart agents based on SNMPv3 are available
 - Support common SNMPV3 administrative framework
 - Network monitoring
 - Host resource monitoring
 - File system monitoring
 - Critical application monitoring
 - Log file monitoring
 - Service monitoring
- More info on secure agents tomorrow at 8:30, session 325

Secure Management Applications

- HP OpenView Network Node Manager with HP OpenView NNM SPI for SNMPv3
- After initial configuration, NNM functions work transparently
 - MIB Browser
 - Node polling
 - Data collection
- Partner applications which use NNM SNMP stack will also work transparently

Administrative Policies

- Parts of an enterprise security policy include:
 - Who can see what?
 - Who can change what?
 - How are “users” defined?
 - What level of authentication?
 - What level of encryption?
 - How often are keys changed?
 - Who can change security configurations?
 - How are configurations changed/audited?

Configuration Management Issues

- Users, keys, notifications, etc. must be configured on both managers and agents
- Keys are generated from pass-phrases, pass-phrases not stored on managed devices
- Keys need to be changed periodically
- Configuration must be updated in a timely manner (e.g., deny rights to a terminated employee)
- Configuration needs to be done remotely from a security management station, using a secure and private method

Configuration Management Issues: SNMPv3 Remote Administration

- Need to configure manager platforms and agents in accordance with enterprise policies
- Can do it with “vi” or “edit” but really need something more friendly and powerful
- Security dependent on correct configurations
- Wizard and/or policy-based tools
- Configurable agents
- Configurable managers

Configuration Management Applications

- Configuration Management applications are very helpful to reduce complexity and human error
 - One agent at a time “wizard” application
 - Policy-based, multiple-target distribution application



SNMPv3 Configuration Wizard

The screenshot shows a window titled "SNMPv3 Configuration Wizard" with a blue header bar. Below the header, the text "Security Configurations" is displayed in a large, bold font. Underneath, it shows "Configuration by systemAdmin on ultra101" and "SNMPv3 USM User to Create netReporter". The main area contains the instruction "Select the maximum security level for this SNMPv3 USM user:" followed by three radio button options: "No Authentication or Privacy (noAuthNoPriv)", "Authentication without Privacy (authNoPriv)", and "Authentication with Privacy (authPriv) (recommended)". The "Authentication with Privacy" option is selected. At the bottom, there are several buttons: "Help", "Exit", "<< Restart", "< Back", "Next", and "Commit".

SNMPv3 Configuration Wizard

Security Configurations

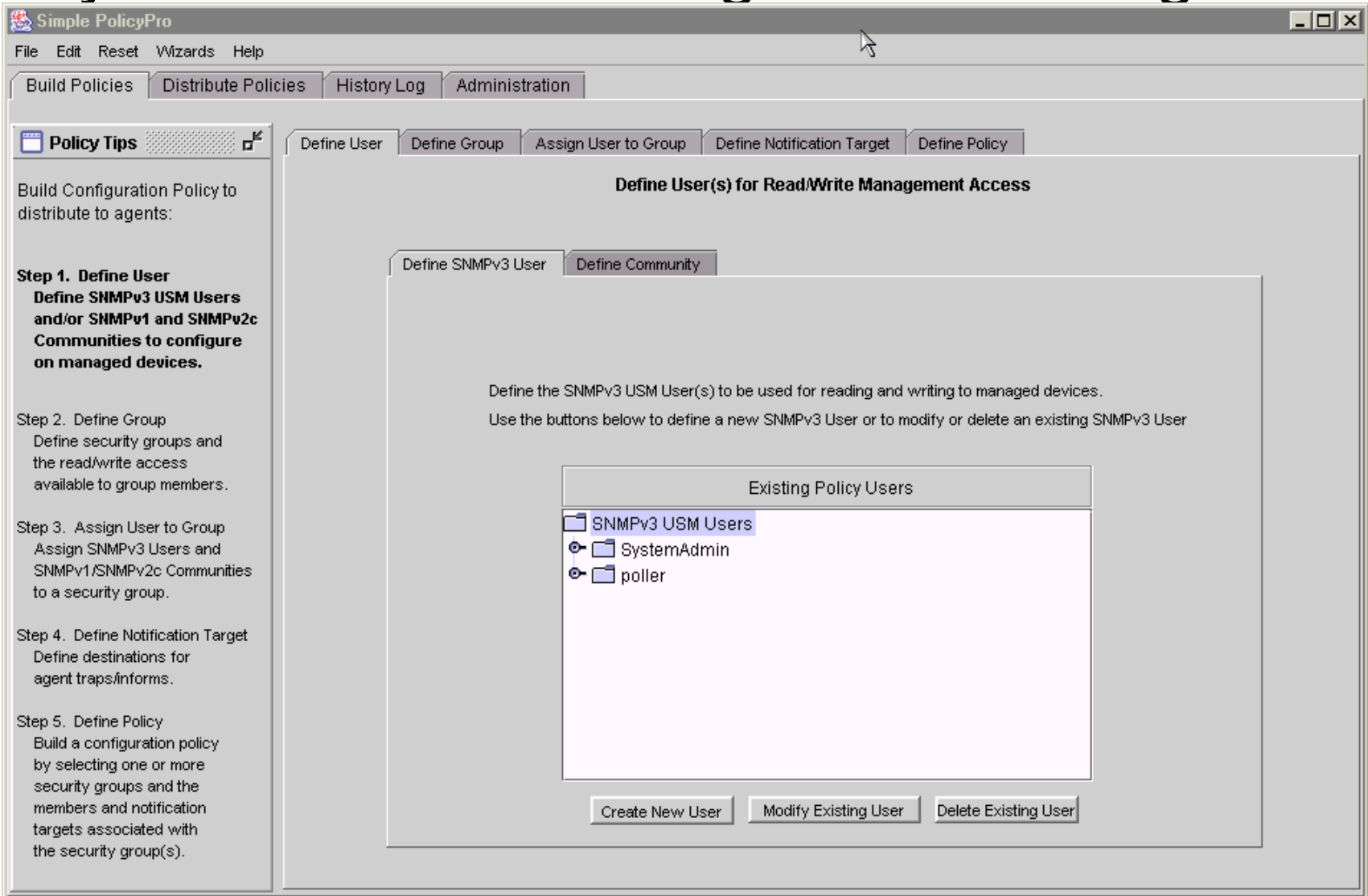
Configuration by **systemAdmin** on **ultra101**
SNMPv3 USM User to Create **netReporter**

Select the maximum security level for this SNMPv3 USM user:

- No Authentication or Privacy (**noAuthNoPriv**)
- Authentication without Privacy (**authNoPriv**)
- Authentication with Privacy (authPriv) (recommended)**

Help **Exit** **<< Restart** **< Back** **Next** **Commit**

Policy-based SNMP Configuration Management



The screenshot displays the Simple PolicyPro application window. The main menu includes File, Edit, Reset, Wizards, and Help. The interface is divided into several panes and tabs:

- Build Policies** (selected), **Distribute Policies**, **History Log**, and **Administration** tabs are visible at the top.
- A **Policy Tips** pane on the left provides instructions for building configuration policies.
- The main workspace contains a sequence of tabs: **Define User** (selected), **Define Group**, **Assign User to Group**, **Define Notification Target**, and **Define Policy**.
- Under the **Define User** tab, there are sub-tabs for **Define SNMPv3 User** (selected) and **Define Community**.
- The central area is titled **Define User(s) for Read/Write Management Access** and contains the following text:

Define the SNMPv3 USM User(s) to be used for reading and writing to managed devices.
Use the buttons below to define a new SNMPv3 User or to modify or delete an existing SNMPv3 User
- A list box titled **Existing Policy Users** shows a tree structure:
 - SNMPv3 USM Users (selected)
 - SystemAdmin
 - poller
- At the bottom of the workspace are three buttons: **Create New User**, **Modify Existing User**, and **Delete Existing User**.

Coexist with Legacy Systems

- Some managed systems will not have SNMPv3 agents
- Cannot upgrade all agents at once
- NNM SPI for SNMPv3 is multi-lingual, so fully supports a heterogeneous SNMPv1 / SNMPv2c/ SNMPv3 agent environment
 - Old agent, old packet, old rules, old response
 - New agent, new packet, new rules, new response
- Properly handle SNMPv1 traps
- Properly handle SNMPv2c traps and informs



final comment...

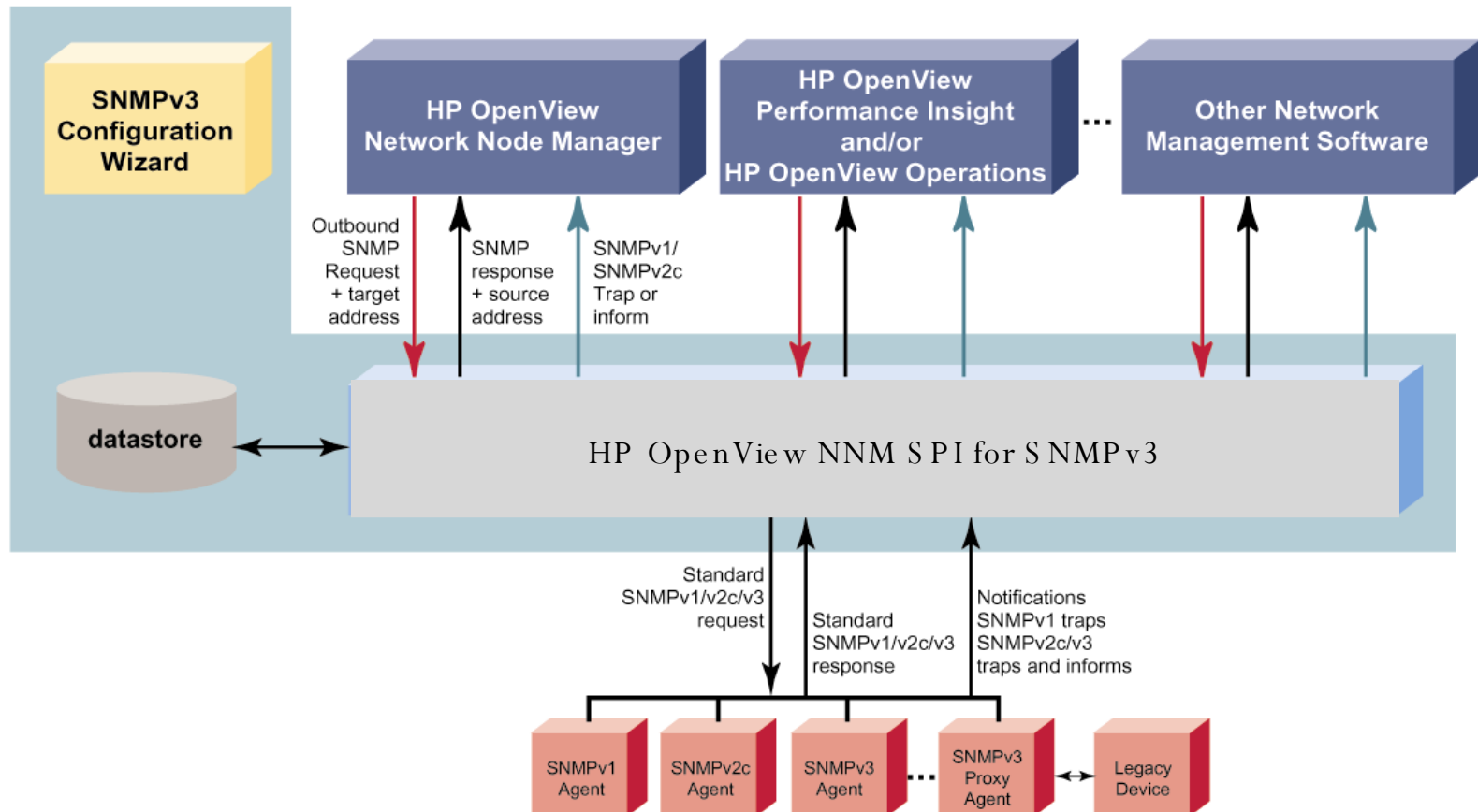
Summary

- SNMPv3 provides secure management capabilities
- Secure SNMPv3 is available in today using the HP OpenView NNM SPI for SNMPv3 and SNMPv3 enabled agents
- HP OpenView Network Node Manager, the HP OpenView NNM SPI for SNMPv3, and the HP OpenView NNM Secure Polling Agent allows secure management through firewalls, even when managing SNMPv1/SNMPv2c devices
- After security credentials have been configured, operation using the NNM SPI for SNMPv3 is transparent to NNM functions
- Available today from SNMP Research. Available soon from HP.



Thank you!

HP OpenView NNM SPI for SNMPv3



HP OpenView NNM Secure Polling Agent

