

Health Policy Enforcement Using NAP

Ravi Sankar
Technology Evangelist | Microsoft
ravi.sankar@microsoft.com

Agenda

- Introduction
- Components of Network Access Protection
- How Network Access Protection works

Introduction

- Challenge

- How to maintain computer health

- How to define and enforce computer health requirements

- Intranet computers
 - Home computers
 - Traveling portable computers

- Risk

- Malicious software attacks out-of-date computers

What is Network Access Protection?

- Platform that enforces compliance with health requirements for network access or communication
- Operating system components
 - Built into Microsoft® Windows Server® 2008 and Microsoft Windows Vista™
 - Separate client for Microsoft Windows® XP with Service Pack 2
- Application programming interfaces (APIs)
 - Allows for integration with third-party vendors

Aspects of Network Access Protection

- Health policy validation
- Health policy compliance
- Limited access

Health policy validation

- Computer that is trying to connect to or communicate on the network is validated against health requirement policies
- Compliant computers
 - Grant access
- Noncompliant computers
 - Grant unlimited access but log compliance state of computer
 - Monitoring-only environment
 - Limit access to restricted network
 - Restricted access environment
- Computers can be excepted

Health policy compliance

- Automatically update noncompliant computers
 - Monitoring-only environment
 - Noncompliant computers will have access to the network before they are updated
 - Restricted access environment
 - Noncompliant computers will have limited access until they are updated
- Automatically update compliant computers to guarantee ongoing compliance

Limited access

- Limiting network access
 - A specific amount of time
 - A restricted network
- Health update resources
 - Used by clients to obtain updates for compliance
 - Antivirus signature and operating system update servers
 - Located on the restricted network

Network Access Protection platform

- Built-in components of Windows
 - Define health requirement policies
 - Provide enforcement of health requirements
- Microsoft and third-party components
 - Provide health policy validation and compliance
 - System health agents (SHAs)
 - Determines the current health state of a computer
 - System health validators (SHVs)
 - Validates that the current health state of a computer meets the required health state

Built-in SHA and SHV

- Windows Security Health Agent
 - Firewall software installed and enabled
 - Antivirus software installed, enabled, and updated
 - Antispyware software installed, enabled, and updated
 - Automatic updates enabled
- Windows Security Health Validator

Scenarios for Network Access Protection

- Check the health and status of roaming portable computers
- Validate the health of desktop computers
- Determine the health of visiting portable computers
- Verify the compliance and health of unmanaged home computers

Components of Network Access Protection

- Network Access Protection enforcement methods
- Network Policy Server (NPS)
- Infrastructure components

Network Access Protection enforcement methods

- Internet Protocol security (IPsec)-protected communications
- IEEE 802.1X-authenticated network connections
- Remote access virtual private network (VPN) connections
- Dynamic Host Configuration Protocol (DHCP) configuration

IPsec enforcement

- Requires that incoming connection attempts are protected with IPsec and originate from compliant computers
 - Noncompliant computers cannot initiate communication with compliant computers
- A health certificate server obtains X.509 health certificates for compliant clients
 - Health certificate is used during IPsec authentication
- Strongest form of limited network access in Network Access Protection

802.1X enforcement

- 802.1X-authenticated connections have unlimited access only for compliant computers
 - Noncompliant computers have limited access
- Limited access
 - A set of Internet Protocol (IP) packet filters
 - A virtual LAN (VLAN) identifier
- Provides strong limited network access for 802.1X-authenticated connections

VPN enforcement

- Remote access VPN connections have unlimited access only for compliant computers
 - Noncompliant computers have limited access
- Limited access
 - A set of IP packet filters
- Provides strong limited network access for remote access VPN connections

DHCP enforcement

- IP configurations have unlimited access only for compliant computers
 - Noncompliant DHCP clients have IP configurations with limited access
- Limited access
 - Limited IP configuration and special routes in the IP routing table
- Weakest form of limited network access in Network Access Protection

Network Policy Server

- Remote Authentication Dial-In User Service (RADIUS) server and proxy for Windows Server

2008

–Replaces Internet Authentication Service (IAS) in Windows Server

2003

- Policy server for Network Access Protection

–Administrators define system health requirements as policies on a Network Policy Server

–Provides health requirement validation against configured policies

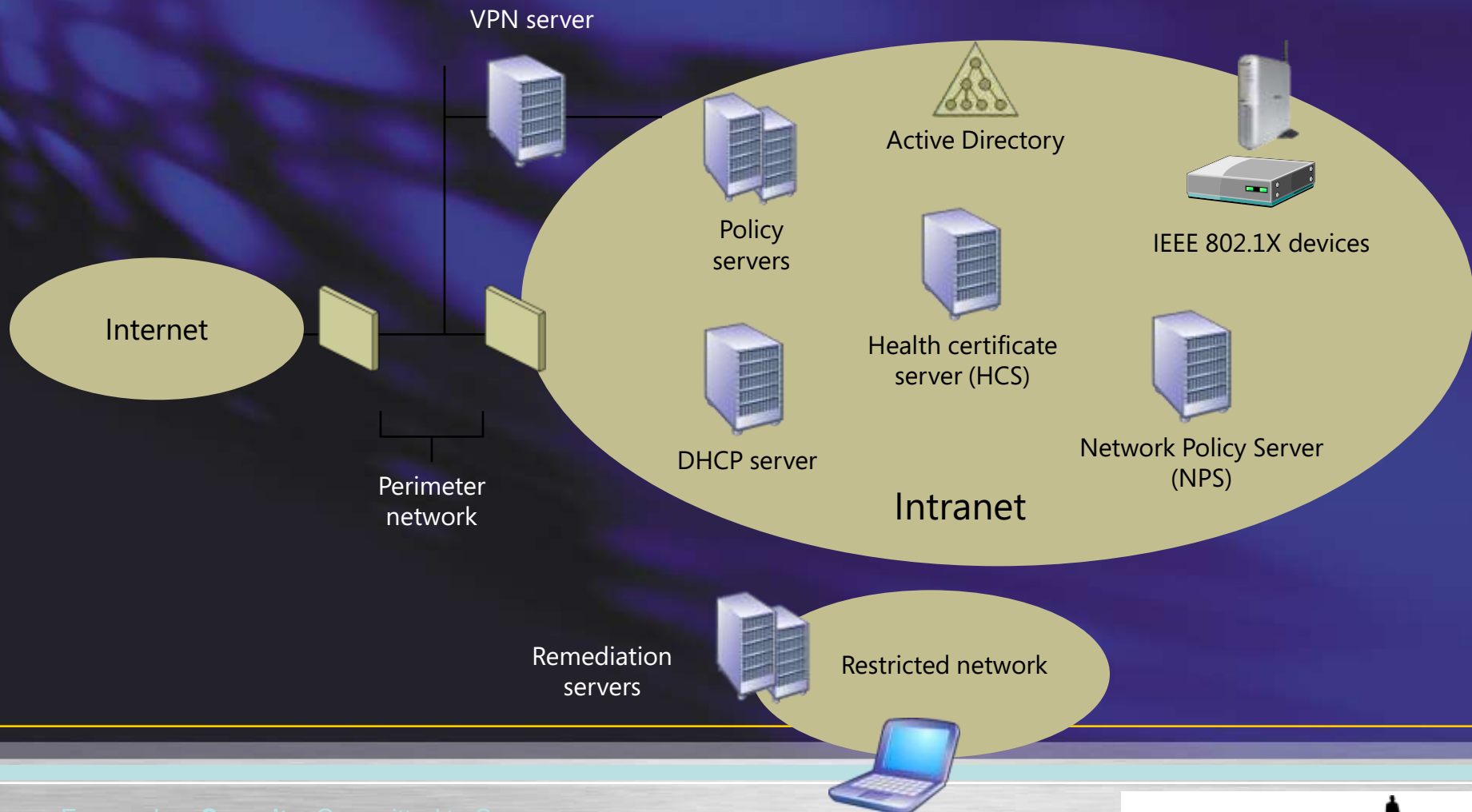
Infrastructure components of NAP

- Active Directory® directory service
 - Stores computer and user account information to authenticate and authorize connections
- Health certificate server
 - Obtains health certificates for compliant clients
- Remediation servers
 - Used by SHAs on noncompliant clients to obtain required updates
- Policy servers
 - Used by SHVs to validate the current health status of a NAP client

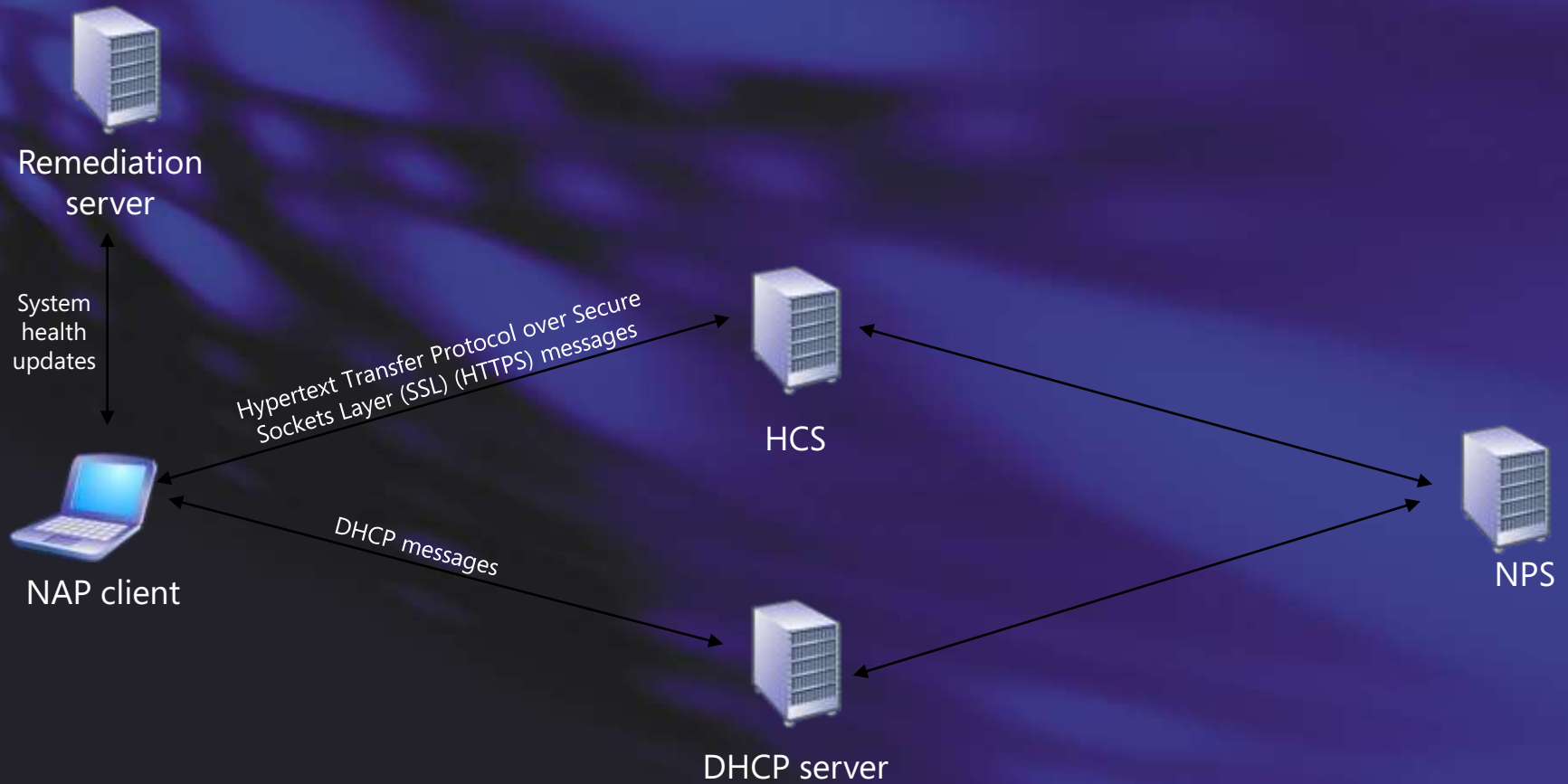
How Network Access Protection Works

- IPsec enforcement
- 802.1X enforcement
- VPN enforcement
- DHCP enforcement

Components of the Network Access Protection platform

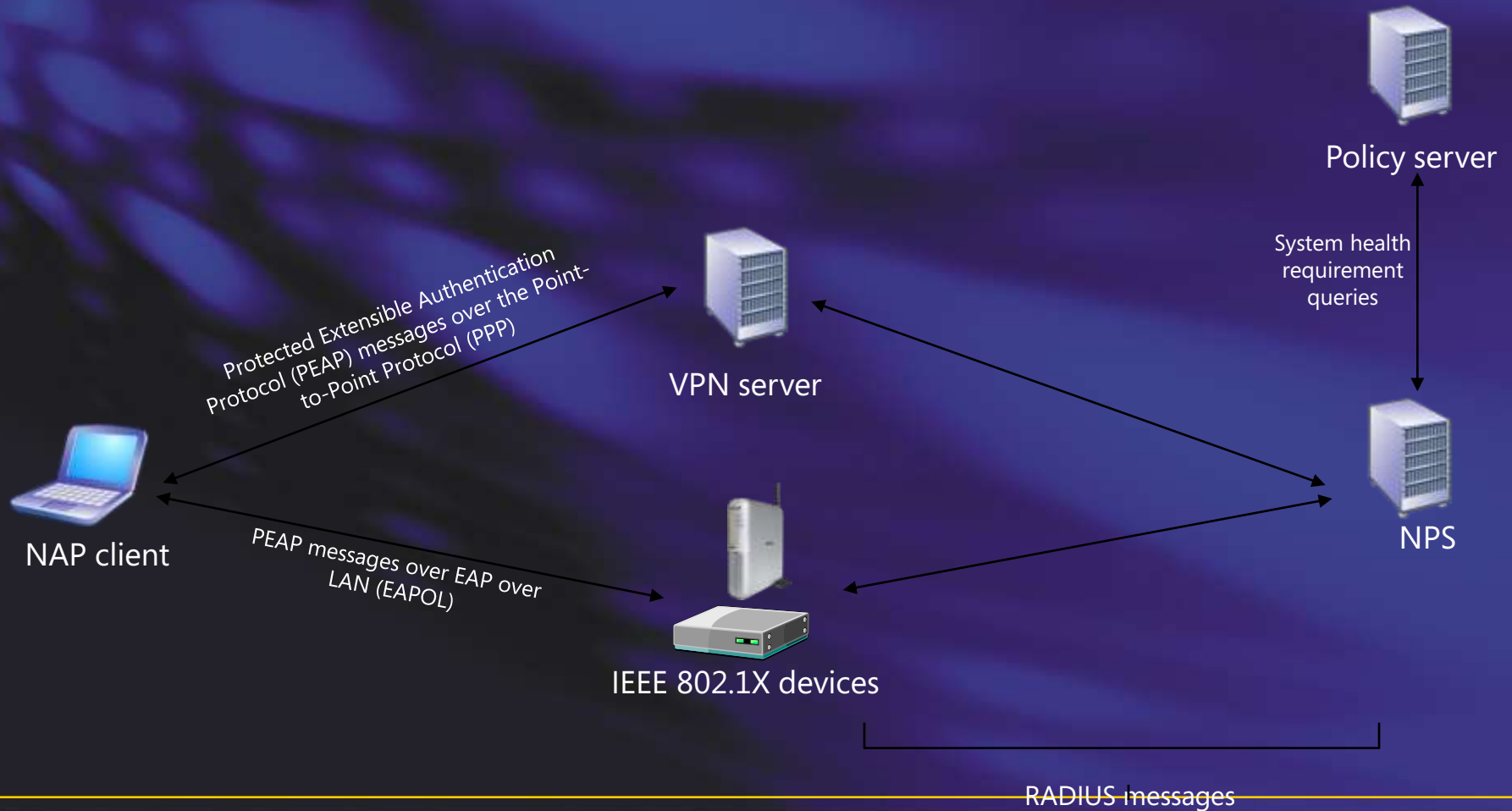


Network Access Protection component interaction



Remote Authentication Dial-in User Service
(RADIUS) messages

Network Access Protection component interaction (2)



Network Access Protection resources

- Network Access Protection Web site
 - <http://www.microsoft.com/nap>
- “Introduction to Network Access Protection” white paper
 - <http://www.microsoft.com/technet/itsolutions/network/nap/napoverview.mspx>

- Network Access Protection

Net work Access Protection	Network Access Quarantine Control
Internal, VPN and Remote Access Client	Only VPN and Remote Access Clients
IPSec, 802.1X, DHCP and VPN	DHCP and VPN
NAP NPS and Client included in Windows Server 2008 ; NAP client included in Vista	Installed from Windows Server 2003 Resource Kit