Configuring Network Access Protection

Another way that you can have security is to allow users to access resources based on the identity of the client computer. This new security solution is called *Network Access Protection*. Determined by the client needs, network administrators now have the ability to define granular levels of network access using NAP. NAP also allows administrators to determine client access based on compliancy with corporate governance policies. The following are some of the NAP features:

Network Layer Protection *Network layer protection* is the ability to secure communications at the Network layer of the OSI model.

All communications travel through the seven layers of the OSI model. Starting at the top (layer 7), the seven layers are the Application, Presentation, Session, Transport, Network, Data-Link, and Physical layers.

DHCP Enforcement If a computer wants to receive unlimited IPv4 network access, the computer must be compliant with corporate governance policies. *DHCP enforcement* verifies that a computer is compliant before granting unlimited access. If a computer is noncompliant, the computer receives an IPv4 address that has limited network access and a default user profile. One advantage of using DHCP is that you can set up user classes so that specific machines (for example, noncompliant DHCP systems) can get specific rules or limited access to the network.

When a client computer attempts to receive an IP address from DHCP, the DHCP enforcement checks the health policy requirements of the system to make sure they meet the compliancy.

VPN Enforcement *VPN enforcement* works a lot like DHCP enforcement, except that VPN enforcement verifies the compliancy of the system before the VPN connection is given full access to the network.

IPsec Enforcement *IPsec enforcement* will allow a computer to communicate with other computers as long as the computers are IPsec compliant. You have the ability to configure the requirements for secure communications between the two compliant computer systems. You can configure the IPsec communications based on IP address or TCP/UDP port numbers.

802.1X Enforcement For a computer system to have 802.1X unlimited access to network connections (Ethernet 802.11 or wireless access point), the computer system must be 802.1X compliant. *802.1X enforcement* verifies that the connecting system is 802.1X connection compliant. Noncompliant computers will obtain only limited access to network connections.

Flexible Host Isolation *Flexible host isolation* allows a server and domain to isolate computers to help make it possible to design a layer of security between computers or networks. Even if a hacker gains access to your network using an authorized username and password, the server and domain isolation can stop the attack because the computer is not an authorized domain computer.

Multiconfiguration System Health Validator This feature allows you to specify multiple configurations of a *system health validator (SHV)*. When an administrator configures a network policy for health evaluation, the administrator will select a specific health policy. Using this feature allows you to specify different network policies for different sets of health requirements based on a specific configuration of

the SHV. For example, an administrator can create a network policy that specifies th all internal computers must have antivirus software enabled and a different netwo policy that specifies that VPN-connected computers must have their antivir software enabled and signature files up-to-date.

NAP Monitoring

There may be many times when you will need to monitor how NAP is running a what NAP policies are being enforced. There are multiple ways that you can monit NAP. You can use the Network Access Protection MMC snap-in to look at how thin are running.

But there is another tool that you can use called Logman. Logman creates a manages Event Trace Session and Performance logs and allows an administrator monitor many different applications through the use of the command line. Table 14 shows some of the different Logman switches you can use.

TABLE 14.2 Logman switches

Switch	Description
Logman create	Creates a counter, trace, configuration data collector, or API
Logman query	Queries data collector properties
Logman start | stop	Starts or stops data collection
Logman delete	Deletes an existing data collector
Logman update	Updates the properties of an existing data collector
Logman import | export	Imports a data collector set from an XML file or exports a data collector set to an XML file