5.9.3 NAP Facts

Network Access Protection (NAP), also referred to as Network Access Control (NAC), is a collection of components that allow administrators to regulate network access or communication based on a computer's compliance with health requirement policies. For example, you can allow network access only to clients that have antivirus software, that have the firewall enabled, or that have the latest patches installed. NAP can also ensure ongoing compliance by requiring that a computer maintain adherence to health requirements.

NAP uses the following components:

Component	Description

NAP Client	Client computers must have NAP-aware software, either through the operating system or other components.
	▪ Client software generates a statement of health (SoH) that reports the client configuration for health requirements.
	▪ The client software prevents the system from accessing the network if the system is not in compliance with health requirements.
	▪ Client computers have a component called the enforcement client.
	  ▪ Clients run the enforcement client type that corresponds to the enforcement server type to which they are connecting.
	  ▪ To prevent users from disabling NAP on the client computer, enable the Network Access Protection agent and the corresponding enforcement client through Group Policy.

NAP Server	The NAP server is responsible for keeping track of health requirements and verifying that clients meet those requirements before gaining access. A Windows server running the Network Protection Service role is a NAP server. ▪ The System Health Validator (SHV) runs on the NAP server and identifies the client health requirements. The SHV compares the statement of health submitted by the client to the health requirements. ▪ Health policies on the NAP server identify the action to take in response to compliant or non-compliant clients: allow access, deny access, or allow access to the quarantine or limited access network. Multi-configuration SHVs are available beginning with Windows Server 2008 R2, allowing different network policies to specify different health requirements. For example, computers on the intranet can have a different health policy than computers connected to the network through a VPN.
Enforcement Server (ES)	An *Enforcement Server* (ES), also called an enforcement point, is the connection point for clients to the network. Clients connect to the ES, submitting the SoH for validation. The ES forwards the SoH to the NAP server for validation. Once the response from the NAP server is received, the enforcement point allows or denies network access.
Remediation Server	Remediation servers are a set of resources that a non-compliant computer can access on the limited-access network. The purpose of a remediation server is to provide the resources necessary to help non-compliant clients become compliant. For example, you might identify servers that hold operating system patches or anti-virus definition files as remediation servers.

The following table identifies five different enforcement point types. Each type identifies a method for controlling client access to the network:

Type	Description
DHCP	The DHCP enforcement server controls access by leasing addresses only to computers that meet the health requirements. DHCP enforcement is the easiest method to implement. When using DHCP enforcement: ▪ Enable NAP on the DHCP scope. ▪ Configure new DHCP options to deliver IP configuration values to non-compliant computers. For example, you can define options that identify the remediation servers. DHCP enforcement is the easiest method to bypass, since clients can assign themselves a static IP address.
Remote Desktop (RD) Gateway	A Remote Desktop (RD) Gateway server can be combined with NAP to allow or deny access based on health compliance. When using RD Gateway: ▪ Enable NAP enforcement by editing the properties for the server and selecting **Request clients to send a statement of health**. ▪ The remote desktop server uses the Remote Desktop Protocol (RDP) over port 80 or 443. ▪ Configure RD CAPs (Connection Authorization Policies) and RD RAPs (Resource Authorization Policies) on the RD Gateway server.
VPN	

	A remote access server configured for VPN access can integrate with NAP. When using NAP with a VPN: ▪ You can define IP filters in network access policies to limit resource access for non-compliant computers. ▪ You can create a connection request policy on the NAP server that uses PEAP and enables quarantine checks.
802.1x	Use 802.1x as an enforcement point for both wireless and wired clients. When configuring 802.1x: ▪ Configure the enforcement point as a RADIUS client to the NAP server. ▪ On an 802.1x switch, define VLANs to create compliant and non-compliant networks. Client computers are assigned to the appropriate VLAN based on health compliance. ▪ In the network access policies on the NAP server, identify the VLAN that corresponds to the compliant and non-compliant networks. The switch must have 802.1 enabled and properly configured.

IPsec	IPsec enforcement requires the use of IPsec for clients to connect to and communicate on the private network. IPsec setup is complex, but it is also the most secure NAP type. For IPsec enforcement:
	▪ IPsec uses client certificates; clients must be issued a valid certificate before a connection to the private network is allowed.
	▪ IPsec provides domain and server isolation. When combined with NAP, three to four logical networks are established.
	▪ Add the Health Registration Authority (HRA) role service to the NAP server and configure the server as a subordinate CA so that it can issue certificates to compliant computers.
	▪ Active Directory Domain Services (AD DS) is required. Configure Group Policy to allow certificate auto-enrollment and identify a security group for computers that are exempt from health checks.
	When implementing NAP with IPsec:
	▪ A client untrusted by the system is restricted to the boundary or untrusted network.
	▪ An untrusted client can initiate communication with a resource in the restricted network using cleartext.
	  ▪ The restricted network can contain NAP enforcement servers and remediation servers.
	  ▪ Clients in the restricted network will have the IPsec policy, meaning they will use IPsec when communicating with IPsec-enabled computers. They will default to clear text communication, if necessary, to communicate with computers in the boundary.
	▪ Clients in the secure network require IPsec.
	  ▪ The NAP server (NPS) resides in the secure network.
	  ▪ NAP-compliant clients also reside in the secure network.
	  ▪ Clients in the secure network will have the secure server IPsec policy.
	▪ Domain isolation combines IPsec with Active Directory.
	▪ Server isolation can be implemented as an additional layer of security.
	▪ IPsec can also be used by itself, without NAP, to establish the three network security tiers.

Agents are pieces of code that authenticates a user or device on the network. Network authentication methods using agents are listed in the table below:

Type	Description
Permanent	The agent resides on a device permanently. This is the most convenient agent since it does not have to be renewed and can always run on the device. It is also known as a persistent agent.
Dissolvable	The agent is downloaded or a temporary connection is established. It is removed once the user is done with it. The user will have to download or connect to the agent again if needed.
Agentless	The agent is on the domain controller. When the user logs into the domain, it then authenticates with the network.

TestOut Corporation All rights reserved.