

Plug-in for Extending Microsoft NAP



Introduction

The changes taking place in the business world due to the spread of mobile devices and wireless networks have created a demand for fundamental changes in enterprise security strategy. When infected terminals on unsafe and untrusted networks are accessed, traditional perimeter security strategies are powerless to protect your network infrastructure. Internal network security strategies must evolve along with the changing business world, allowing successful enterprises to thrive now and in the future.

When terminals are accessed by your internal network, a process of authentication, detection, control and remediation through access policies can ensure that only safe and trusted terminals are accessible. Microsoft's Network Access Protection platform is one of the most effective methods for providing this kind of internal network security.

Microsoft proprietary Network Access Protection platform technology validates the security health state of network terminal so that it guarantees ongoing compliance by the network access control and system health policy. It provides a way of limiting the access of network clients until the health policy requirements have met.

UNETSHA is a plug-in for extending the security health check capability and interoperability with third-party endpoint security solutions in Microsoft NAP platform. It enables more granular network access control in enterprise-wide NAP implementation that includes heterogeneous network terminals such as Windows, Linux and Mac.

UNETSHA can perform a variety of health check functions including quarantining user terminals that try to open specific ports that are used by worms, enforcing application patches, and sending warning messages to the terminals that do not have required software or run prohibited software such as P2P programs. These actions are based on examining file sizes, installed programs, process monitoring status, registry keys, components in INI files, etc. UNETSHA also supports Windows Management Instrumentation (WMI) which is used to manage the configuration, status and operational aspects of hardware and software in Windows, and administrators can use these managed objects as NAP policy objects. Through the use of over 7,000 managed objects, administrators can set up a vast number of different policy sets. By utilizing this feature, terminals using mass storage devices such as external HDDs, CD writers or unauthorized wireless network adapters can be quarantined from the corporate network.

Features

| Extends Security Health Check Capabilities of Microsoft NAP

The default NAP policy is enforced on all PCs in the same domain. This policy may not support policies that are differentiated based on the actual user groups. UNETSHA supports login ID based policy enforcement for exceptional cases to make NAP policy enforcement more flexible.

| Supports Unlimited Policy Objects with WMI

With over 7,000 managed objects provided by Windows Management Instrumentation, administrators can use software and hardware objects to control the network access. For example, terminals using external mass storage devices or unauthorized wireless network adapters can be quarantined from the corporate network.

| Provides Windows, Linux and Mac NAP Agents

When implementing NAP on your network, you may have to deal with not only Windows terminals, but also Linux and Mac terminals. UNETSHA provides Windows, Linux and Mac agents for a seamless network access protection platform in a heterogeneous environment.

| Migrates NAQC to Microsoft NAP

Network Access Quarantine Control (NAQC) is a set of services and utilities available for Windows Server 2003 that lets you prevent remote users from connecting to your network with machines that are not up to date and quarantine those users in a secured area. The migration of compliance checks is critical in the transition from the NAQC environment to the NAP environment. UNETSHA supports migration from NAQC to NAP through script-level compatibility when you make a NAP policy.

| Easy Updates for NAP Agents

UNETSHA allows administrators to manage agent update packages from the main management console without the need for any additional applications. The NAP agents are updated automatically according to the operating system when the network is accessed.

| Enhances NAP Manageability

When you deploy multiple NPSEs with different policies in multiple domain environments, administrators have no choice but to perform management tasks for each one. For this scenario, UNETSHA supports the centralization or decentralization of NAP management tasks and provides a feature multiple domain support. Administrators can manage each domain's policy in a separate console or all the domains' policies in one management console.

| Supports Tailored Policy Enforcement

The default NAP policy enforces to all the PCs in the same domain. In real-world network environment, a domain might consist of many user groups and user types. The NAP policy needs to support this structural property for better security scheme. To support this, UNETSHA supports user and group based policy enforcement so that administrator can enforce tailored health check policy against respective user and user group. Furthermore, the policy enforcement cycle can be set by once or periodically depending on the characteristics of the policy.

| Supports Hierarchical Group and Policy Management

Enterprises usually configure and manage their departments hierarchically. In administrative point of view, enterprise-wide NAP policy need to support this hierarchical characteristic. UNETSHA supports hierarchical group and policy management so that administrator can manage NAP policies according to actual organizations. The precedence of NAP policy enforcement is in the following order; user - group - upper group - root group policies. The root group policy can be used as global policy.

| Plug-ins for Diverse Client Health Check Programs

To support additional PC health check capabilities, UNETSHA allows plug-ins for a variety of health check programs independent of their type (VBS, EXE, BAT, etc.). This feature is included in the RQS Package to strengthen NAP policy enforcement through a diverse variety of PC health check programs.

| Including ECs: 802.1X Supplicant and DHCP Client

Linux and Mac versions include NAP agent with ECs for 802.1X authenticated connections and DHCP-based IPv4 address configuration. The supported EAPs in 802.1X are PEAP version 0/1/2, PEAP-MSCHAP v2, EAP-MD5, EAP-TLS, EAP-TTLS, EAP-GTC and LEAP.

FEATURE HIGHLIGHTS

Extends Microsoft NAP security health check capabilities

Migrate Network Access Quarantine Control in Windows Server 2003

Control network access for Windows, Linux, and MAC

Provides automatic agent updates in the unified console

Enhances NAP policy management with wizard-style interfaces

Specification

Health Check Object

Object	Description	Win	Linux	Mac
Registry	Check registry	o		
Registry Key	Check registry key	o		
	Exist	o	o	o
	Size	o	o	o
File	Version	o		
	Date	o	o	o
	Checksum	o	o	o
Default	Process	o	o	o
	Service	o		
	OS Version	o	o	o
	Port	o	o	o
	Install Program	o		
	INI File	o		
	Firewall	o	o	o
	Update	o	o	o
Extended	NAQC Script	o		
	WMI	o		

Action Object

Action	Description	Win	Linux	Mac
Allow	Allow network access	o	o	o
Deny	Deny network access	o	o	o
Registry Action	Add/Modify/Delete registry value	o		
Registry Key Action	Add/Delete registry key	o		
INI File Action	Add/Modify/Delete a key and/or its value	o		
Process Run/Kill Action	Run/Kill process	o	o	o
Service Start/Stop Action	Start/Stop service	o		
Message	Display a message with URL link	o	o	o
Firewall Action	Turn ON/OFF firewall service	o	o	o
Update Action	Turn ON/OFF update service	o	o	o

Operation Environments

Component	Description
UNET NAP Manager	Microsoft Windows Server 2008 (x86/x64)
Database	Microsoft SQL Server 2005/2008 or Express (x86/x64)
	Windows: 7, Vista and XP Service Pack 3 (x86/x64)
NAP Agent	Linux: Fedora 6/7/8/9/10/11, Ubuntu 7.x/8.x/9.x (x86/x64)
	Mac: OS X 10.5 Leopard

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH UNETSYSTEM PRODUCTS. EXCEPT AS PROVIDED IN UNETSYSTEM'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, UNETSYSTEM ASSUMES NO LIABILITY WHATSOEVER, AND UNETSYSTEM DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY RELATING TO SALE AND/OR USE OF UNETSYSTEM PRODUCTS, INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT, OR OTHER INTELLECTUAL PROPERTY RIGHT. UNETSYSTEM MAY MAKE CHANGES TO SPECIFICATIONS, PRODUCT DESCRIPTIONS, AND PLANS AT ANY TIME, WITHOUT NOTICE.

UNETSystem Corporation may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights that relate to the presented subject matter.

Anyclick, UNETSHA, Anymon, Netprism, TrustNET, ubiONE and their logo are trademarks or registered trademarks of UNETSystem Corporation or in Korea. Other names and brands may be claimed as the property of others.

Copyright (c) 2007-2009 UNETSystem Inc. All rights reserved.



7th Fl., Lotte Center 533-2 Gasan-dong, Geumcheon-gu Seoul, Korea 153-803
TEL.82-2-2028-9000 FAX.82-2-2028-9099 E-mail.sales@unet.kr URL.www.unet.kr/nap

To purchase UNETSHA solutions, please visit at www.unetsha.com or following authorized reseller.

Authorized Reseller | North America & Canada: SJ NAMO Inc.

2005 De La Cruz Blvd. Suite 245 Santa Clara, CA 95050 USA
TEL. +1(408)-567-9005 | FAX. 1(408)-567-9014 | E-mail. namous@namo.com

Screen Shot

