

Plug-in for Extending Microsoft NAP

UNETSHA

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.

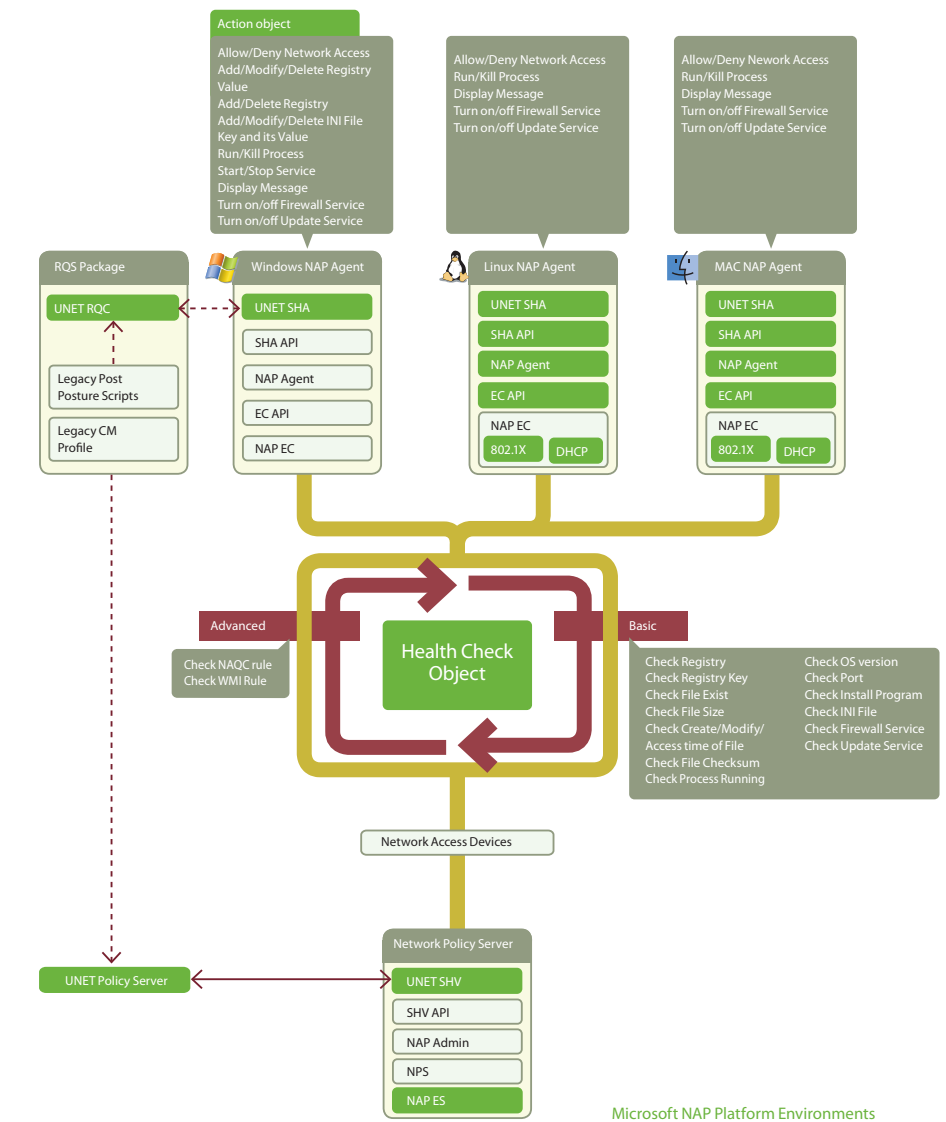
When terminals are accessed by your internal network, a process of authentication, detection, control and remediation through access policies can ensure that only safe and trusted terminals are accessible. Microsoft's Network Access Protection platform is one of the most effective methods for providing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

Quarantining user terminals that try to open specific ports used by worms, sending a warning message to the terminals that do not have required software or run prohibited program such as P2P, enforcing application patch, and more health check functions are supported by UNETSHA. More importantly, as it supports Windows Management Instrumentation (WMI) that used in managements of configuration, status, and operational aspects in hardware and software of Windows, so that administrators can use the managed objects as NAP policy objects. Using over than 7,000 managed objects, administrators can setup a thousand and hundreds of policy sets you can imagine. If you use this feature, terminals using mass storage devices such as external HDDs and CD writers, and/or unauthorized wireless network adapters would be quarantined from the corporate network.

Conceptual Architecture



| Component | Description |
|--------------------|---|
| UNET Policy Server | A plug-in module for user and policy management in the Microsoft Management Console (MMC) of Microsoft Windows Server 2008. It defines relationships between rules, policies, users and groups. |
| UNET SHV | A server module installed on the NPS which supports interoperability with NAP administration server through the UNET Policy Server and NAP SHV API. |
| UNET SHA | A module to extend NAP functions and link with NAP clients through the NAP SHA API. NAP policies coming from UNET Policy Server are enforced on user terminals according to individual login IDs. |
| NAQC Package | A NAP execution package for Network Access Quarantine Control by Connection Manager (CM) Profile. (Windows version only) |
| EC API | This allows other third-party endpoint security vendors to create and install additional NAP ECs. It supports fast and easy development of additional ECs in Linux and Mac environments. |
| NAP EC | This requests a level of access to the network, passes the computer's health status to the NAP enforcement point that is providing network access and indicates to other components in the NAP client has limited or unlimited network access status. Linux and Mac versions include ECs for 802.1X-authenticated connections and DHCP-based IPv4 address configuration |

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

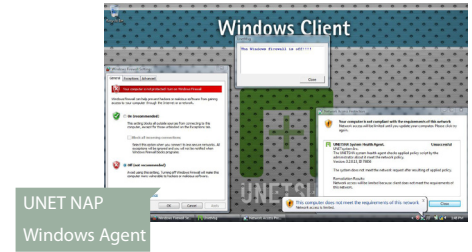
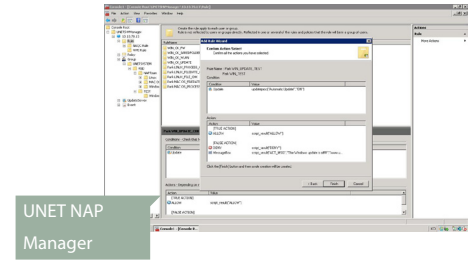
Provides automatic agent updates in the unified console

Enhances NAP policy management with wizard-style interfaces

Benefit

| Benefit | Description |
|--------------------------|--|
| Operation Consolidation | <p>PC health check policies that were used in Microsoft Windows 2003 can be easily migrated to Windows 2008 either manually or automatically so that you can consolidate your management environment for added efficiency.</p> <p>Administrators can consolidate PC health check policies for Windows-based terminals as well as Linux and Mac-based terminals for increased operational efficiency in a heterogeneous environment.</p> <p>The UNETSHA consolidated update service allows you to update agents easily. An update package is imported on the policy server, and then users are shown an update message when connecting to the network in accordance with the update settings. The update package is provided by the operating system.</p> |
| Seamless Security Policy | <p>With Windows Management Instrumentation (WMI), UNETSHA includes all the managed items that are used in the management of hardware/software components in the operating system. Administrators can use these objects to create more flexible security policies catering to their individual company's security goals.</p> <p>NAP management capabilities that are based on the actual organizational structure allow for intuitive management, helping to eliminate mistakes when setting security policies.</p> <p>Scripts written in an IF (Condition) THEN (Action) ELSE (Action) format enable flexible rule editing to support administrative diversity and better compliance with laws and regulations.</p> |
| Expandability | <p>Plug-in capabilities for other endpoint security technologies in the RQS package allow administrators to integrate current and future endpoint security technologies into their own NAP platform infrastructure.</p> |

Screen Shot



Operation Environment

UNET Policy Server

Microsoft Windows Server 2008 (x86/x64)

Database

Microsoft SQL Server 2005/2008 or Express (x86/x64)

NAP Client

Microsoft Windows XP with Service Pack 3 (x86/x64)

Microsoft Windows Vista (x86/x64)

Microsoft Windows 7 (x86/x64)

Linux Fedora 6/7/8/9/10/11 (x86/x64)

Linux Ubuntu 7.x/8.x/9.x (x86/x64)

Apple 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