



End-to-End Trust and Identity Platform™

White Paper

Extending Network Access Protection with Avenda's Products

November 9, 2007



<http://www.avendasys.com>
email: info@avendasys.com
email: sales@avendasys.com

Avenda Systems, Inc.
2855 Kifer Rd, Suite 102
Santa Clara, California 95051 USA
Tel: +1 408.748.1993
Fax: +1 408.748.1997

Avenda Systems India Pvt. Ltd.
#797, 3rd Floor, Annapoorna
10th Main, Jayanagar 4th Block
Bangalore 560011 India
Tel: +91 80.4153.0876/77/78
Fax: +91 80.4153.0879

Copyright © 2005-2007 Avenda Systems, Inc. All rights reserved. eTIPS™ and End-to-End Trust and Identity Platform™ are trademarks of Avenda Systems, Inc. All other brands or trademarks are the property of their respective holders. Contact Avenda Systems, Inc. for complete specifications and other product related information.

Introduction and the Need for Extending NAP Coverage

With Windows Server 2008 and Windows Vista, Microsoft introduces a new software infrastructure solution called Network Access Protection (NAP) for controlling access to the network and its resources. Network Access Protection does an excellent job of providing network access control of Windows Vista clients and soon thereafter Windows XP. There are, however, many other clients that are not supported by NAP and hence will not be able to reap the many benefits of NAP.

One approach is to deny access to any devices that are not supported by Microsoft altogether. While this may be acceptable in some situations, it is much more likely that an enterprise will have a plethora of devices that are either not supported by Microsoft, such as printers, or are not managed by the enterprise itself, such as clients belonging to guest users or contractors. While these devices may not themselves pose a security threat, the fact that they cannot be identified and have their health checked, means that the network would still be vulnerable to compromised or malicious end points. Thus, solutions are needed to provide the necessary access controls to those use cases that are not covered by the NAP solutions provided by Microsoft.

This white paper describes several use cases where Avenda Systems fills vulnerability gaps to enhance the benefits of Network Access Protection. For more details on Microsoft Network Access Protection, please go to <http://microsoft.com/nap>

Use Case 1: Extending NAP to Non-Windows Clients

Most enterprises have a mixture of Windows, Linux and Macintosh clients in their environment. This is particularly true for educational institutions. An easy way to cover these clients with NAP, and one that would fit within any deployment architecture, is to install a NAP agent onto these clients.

Avenda Systems, in partnership with Microsoft, has developed NAP agents for Linux and Macintosh clients. These agents bring Linux and Mac clients up to the same level of NAP support as Windows clients which include the Microsoft NAP agent for Windows. Included with each of these agents is a corresponding System Health Verifier (SHV) that installs on the Network Policy Server (NPS), a component of Windows Server 2008, for validating the health of these systems.

For more information please visit <http://www.avendasys.com/nap>.

Use Case 2: Comprehensive Assessment of Client Health

The Windows Vista NAP agent as well as the Avenda Linux and Macintosh NAP agents provide basic levels of client health checks. For more extensive checks, such as verifying the existence and status of third party anti-virus software, or the existence of various peer-to-peer applications, enterprises can install the Avenda Universal System Health Agent (USHA). This health agent, which installs directly into the NAP infrastructure

delivers ,comprehensive health and other client state to the policy server which can then be used to make flexible, sophisticated access control decisions.

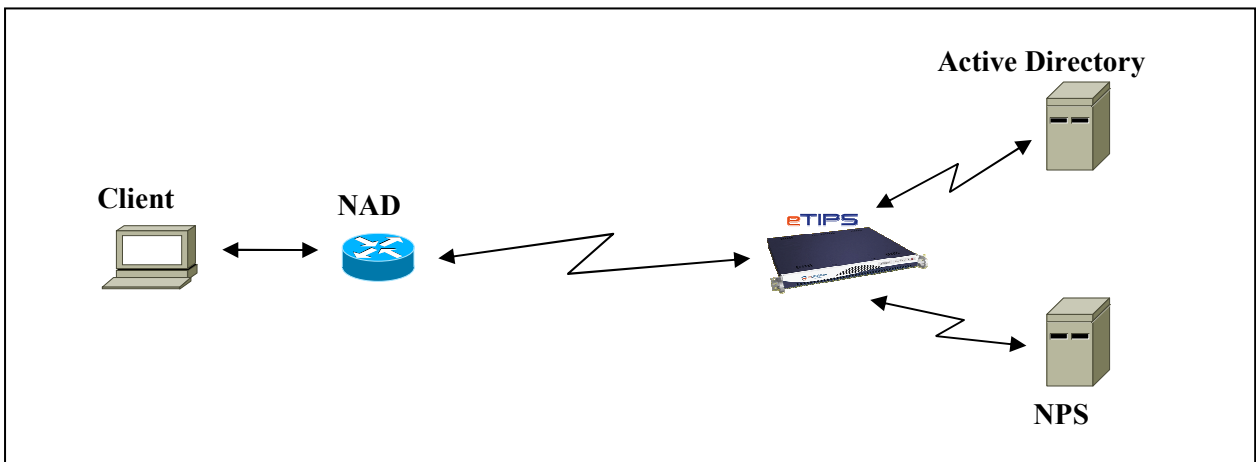
Please visit <http://www.avendasys.com/nap> for information on the specific health information that the USHA is able to ascertain.

Use Case 3: 802.1X Clients without NAP Agents

This use case addresses clients that support the 802.1X protocol and common EAP methods for authentication but do not support NAP. Many such clients are already deployed since 802.1X pre-dates NAP. Examples include clients with 802.11 (WiFi) interfaces and Voice-over-IP (VoIP) phones with 802.1 supplicants which have been introduced into the market more recently. Common EAP methods in use are EAP-FAST and EAP-TTLS.

One obvious and conceptually simple solution to supporting these clients is to install a NAP-compliant agent onto these devices. But this requires that a software upgrade for these clients be available. Even if this were available, a software upgrade is often a difficult logistic operation.

Alternatively, NAP access controls can be extended to these clients by introducing a RADIUS server that supports other EAP methods (such as EAP-FAST and EAP-TTLS). This RADIUS server sits in the communication path between the Network Access Device (NAD) and NPS and terminates the EAP tunnel on behalf of NPS. PEAP (the NAP EAP method) would still be terminated by NPS by having the intermediate RADIUS server proxy those sessions to NPS. If the intermediate server were eTIPS, which also supports PEAP, then it could terminate all EAP methods, thereby avoiding the communications overhead, and inherent network degradation, of the proxy function. This complete solution is shown in the figure below with eTIPS terminating all EAP tunnels, accessing Active Directory directly for verifying identity. NPS would be queried for health checks. (Note: The communication paths shown in the figure represent the control plane communication paths. eTIPS is not in the data path.)



Use Case 4: Printers, VoIP Phones and Other Agent-less Assets

Many end points do not have any agent installed at all. That is, they are incapable of running any EAP authentication method or even the 802.1X protocol itself. With Avenda's eTIPS policy system there are two approaches to handle this use case. For both of these, eTIPS is installed as the primary policy manager as shown in the figure above.

MAC Bypass

This solution requires some support from the NAD. When a client connects but fails to respond to 802.1X identity request messages, the NAD makes a RADIUS access request using the MAC address of the client as the identity. When the request is received by eTIPS, a policy decision is made using this MAC address as the client identity. No EAP method is executed in this case and no health information is (or can be) collected. While it might seem limited to make an access control decision based only on MAC address, the rich policy definition language that eTIPS provides makes this a surprisingly effective solution. Some specific capabilities are the following:

- The policy can be MAC-specific. For example, if the MAC address corresponds to a printer, the access rules can limit access to receiving only printer protocols and nothing else. If the MAC address corresponds to a scanner with email capability, the access rules can limit the device to initiating SMTP connections and nothing else. If the address corresponds to a VoIP phone, then the access rules can limit the device to VoIP protocols.
- A MAC address can be bound to a port so eTIPS can ensure that the expected device is connecting to the expected port and it is not some other device connecting.

The problem with this solution is that it requires that MAC addresses be known and entered into the directory (either the enterprise's user directory or the eTIPS internal directory) as identities. An alternative is to discover the type of device automatically with a device audit.

Device Audit

With this solution, eTIPS is configured to automatically discover information about the device, including some health information (such as which network protocols are open on the device). Then, using this information a policy decision is made and the appropriate access control decision is downloaded to the NAD.

Operationally, this is a two-stage process. First, when the device connects to the network and is found to be unresponsive to the 802.1X protocol messages, it is put in a highly restricted VLAN allowing no access to the network. Second, eTIPS triggers an audit of the device. The audit process is essentially a probe of the device across the network and gathers as much information as possible from this network probe. This information is returned to eTIPS which can then make a more informed policy decision. Based on this new decision, new enforcement rules are sent to the NAD, thereby granting the device

access to the network but with appropriate access controls based on the information that can be ascertained about the device.

Use Case 5: Access Control of Guests and Other Non-Enterprise Clients

Many enterprises allow guests, or other non-employee users such as contractors to access the enterprise network with their private client machines. In such scenarios, guest users must be identified so that the appropriate access controls can be enforced for them. In addition, it may be desirable to evaluate the health of these clients as this may affect the level of access granted.

In many cases, such as with clients running Windows Vista or XP with SP3, these clients may support NAP. In this case access control policies can be applied without any additional NAP capabilities beyond what is already provided except for the ability to easily register guest users, perhaps even temporarily. All that is needed is to create access control policies for these users in the policy system. However, for clients that do not support NAP, or who have disabled NAP, other mechanisms for making access control policy decisions are required.

eTIPS provides an alternative mechanism for these clients that includes both authentication and health verification so that the same level of compliance and trust can be applied to these non-enterprise clients as with enterprise clients. This mechanism is based on the familiar “hotspot model” of network access whereby the user must first launch a browser which forces a login before network access is granted.

When the browser is launched, the NAD captures the HTTP request and passes it on to eTIPS. eTIPS then does two things. First, it returns a login page requiring the user to enter an identity and some credentials to verify the identity (such as a password or a security token). Second, it downloads a Java applet to the browser which gathers health information about the client (such as some registry settings, the status of the personal firewall and the status of any virus checking software) and returns this information to eTIPS. Using this identity and trust information, eTIPS makes an access control decision and sends enforcement rules to the NAD.

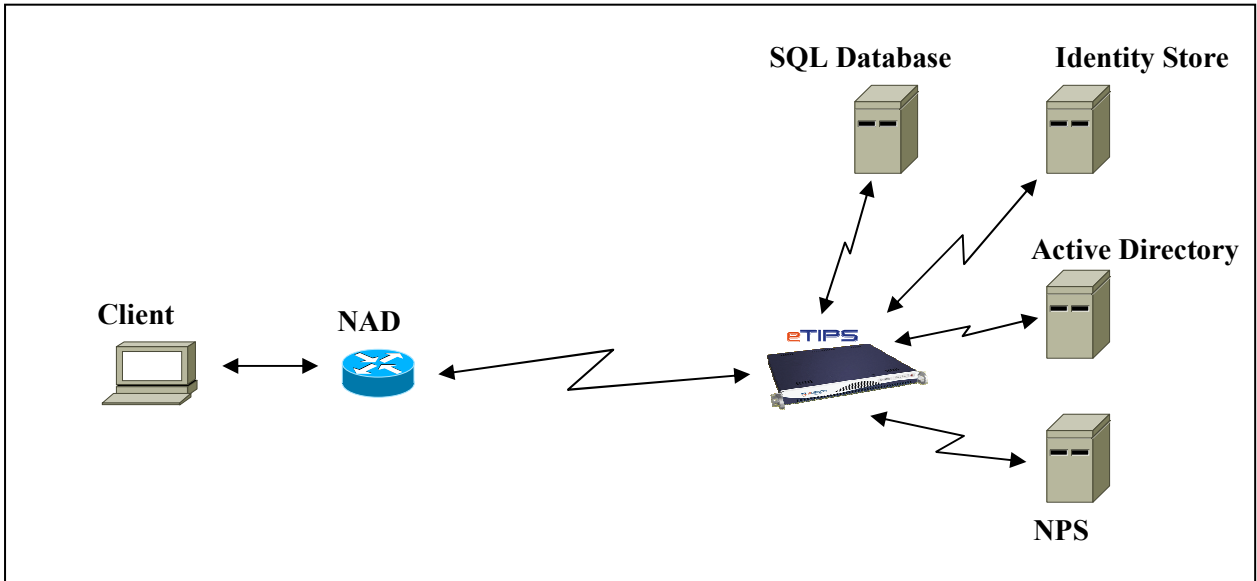
Use Case 6: Using Third Party Identity and Data Stores

In many enterprises some identity information is stored in third party identity stores such as identity token servers. Also, many enterprises have data stored in enterprise-specific databases using home-grown data schema. Often these third party identity stores and home-grown data stores contain information valuable for making an access control decision.

Because it has extensive support for accessing external backend servers, eTIPS makes it possible to integrate these systems, and the information they contain into the NAP

environment. More specifically, eTIPS can query any number of identity systems and SQL databases as a function of the decision making process and use the results of these queries in the policy rules as they are evaluated. As in the other use cases described in this white paper, eTIPS continues to query NPS for evaluating the health of a client as needed.

The figure below shows conceptually the interactions between these systems. (As with the previous figure, the communication paths shown represent the control plane communication paths. eTIPS is not in the data path.)



Summary

This white paper outlines several network access control uses cases for a NAP deployment. It describes how Avenda products, the Linux and Macintosh agents, the Avenda Universal SHA, and the Avenda Policy Management System eTIPS ensure that appropriate enterprise-specific, access control policies can be enforced for these use cases. Thus, with Avenda products, Microsoft's Network Access Protection becomes a compelling access control solution for a wide range of environments, especially those with non-Windows clients.