



End-to-End Trust and Identity Platform™

White Paper

Policy Management: The Avenda Approach To An Essential Network Service



<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

It may be hard to recall that, in the earliest days of the Internet, there was no built-in service for managing names and resolving names to addresses as there is today with the Domain Name Service (DNS). Before DNS, system administrators managed local “hosts files” which contained these name-to-address mappings and which had to be manually updated at each system as new hosts were added to the network. Some of this burden was later alleviated with scripts that would periodically distribute a master hosts file to a collection of hosts. Today, no one would consider running anything but a tiny network without a DNS and associated address management services as DHCP.

Avenda believes that policy management systems, which today are quite primitive and infantile, will mature and will become an essential service of a well-managed network, just as DNS has. Furthermore, just as the usefulness of DNS now extends far beyond its original scope of statically mapping names to addresses, the usefulness of policy systems will extend far beyond the scope they currently have.

Today, most policy systems are essentially RADIUS servers that are used to check users’ identity and to grant or deny access based on that identity. More recently, some more granular control has been implemented such as the ability to assign a user to a specific virtual LAN (VLAN), or to apply an access control list at the point of access based on the identity of the user.

However, policy needs to be applied at multiple points along the communication path including network elements, such as Ethernet switches, wireless access point and VPN gateways, and at multiple application servers such as file servers, Web servers and mail servers. Also, fine grain control over access, such as permission to access a file for read, write, or modify, is also required. While systems and applications provide such policy mechanisms each in its own way and each requiring its own configuration, what is needed is a ubiquitous, end-to-end policy management system that is integrated into and part of the network infrastructure.

Avenda was formed to address this need in the market. Our approach is to design and develop products to address immediate customer needs but with an architecture for evolving these products towards the vision of the end-to-end policy management solution.

The Immediate Need: Network Access Control

In the past couple of years, network access control (NAC) has been recognized to be an essential requirement for running any enterprise network. There have been two drivers for this. The first was the adoption of wireless networking. No longer could access be controlled by physical access to a building or computer room. Instead, the network is required to check the identity of who is connecting to the network. The second is the proliferation of worms, virus and system security breaches. What is needed is control

over what is connecting to the network and some level of trust that the system has not been compromised.

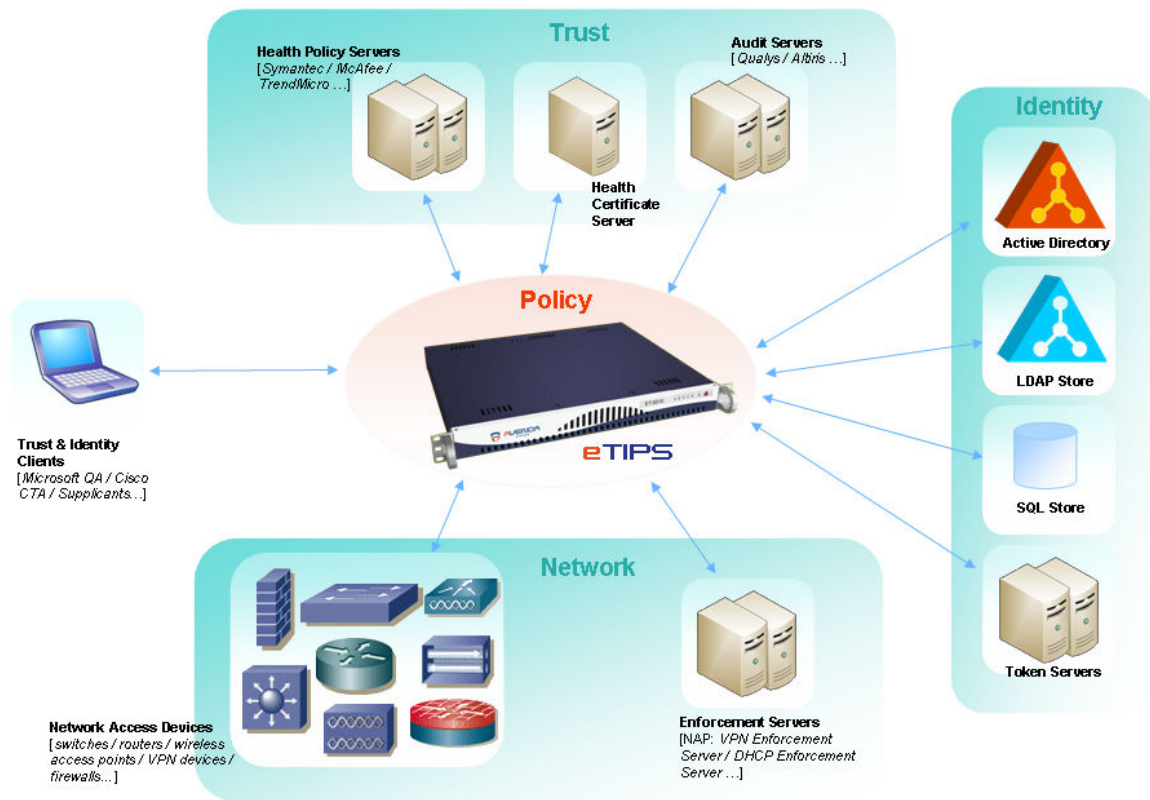
Succinctly said, network access control is the configuration of policies for, and enforcement of access to, the network and its services. Specifically, the purpose of NAC is to control who has access, under what conditions, what level of access should be granted, and to deny access, either proactively or reactively, to unauthorized or misbehaving clients. The purpose, of course, is to prevent unauthorized access to resources and theft of information and prevent malicious destructive activities such as DoS attacks and damaging viruses or worms.

Solution Architecture

Several NAC “frameworks” have been recently proposed and are under active development. These include Cisco’s Network Access Control (CNAC), Microsoft’s Network Access Protection (NAP), and The Trusted Computing Group’s Trusted Network Connect (TNC). Also, the IETF has created a working group chartered to address network endpoint assessment (NEA).

For each of these frameworks (to the extent they have been specified) the core component is the policy management system. This is the component the administrator interacts with to define network policies and where policy decisions are made. The policy management system then interacts with all the other components to ensure that the defined policies are enforced and to assist in any remediation activities. In order to minimize the administrative overhead and complexity (by avoiding deployment of multiple, disparate policy systems) and to ensure predictable behavior (by avoiding multiple, perhaps inconsistent, policy decisions) it is essential that there be a single, but highly scalable, comprehensive policy management system for the enterprise and one that can accommodate current and future needs of the enterprise. To address this requirement, Avenda has developed the Enterprise Trust and Identity Policy System (eTIPS) to provide this service for any of these NAC frameworks, and even for a deployment comprising multiple frameworks.

In keeping with the architecture of these emerging frameworks, eTIPS is designed to be embedded in an end-to-end solution as shown in the figure.



With this architecture, the policy system integrates with clients requesting access using standard protocols and various support services, such as identity stores and trust verification systems at the backend, also using standard protocols as well as emerging new ones. It works with individual frameworks or in an environment with multiple frameworks. Furthermore, it is a platform that is ready to deploy additional policy management services, such as policy management for applications.

The benefits of this solution are described in more detail below.

Policy Management and Enforcement With eTIPS

The functionality of eTIPS can be described by a workflow of five stages which provides a comprehensive model for policy management.



- **Define:** In the define stage, as its name suggests, the administrator defines the policies they want to apply to the network and its services. Arbitrary credentials (such as user identity and device state), attributes (such as location and time-of-day), and rules can be specified.
- **Detect:** Detection is invoked when some access request is made, such as when a client attempts to connect to the network. In this stage, eTIPS determines the access procedure and set of rules to apply to this client. For example, the procedure for a client requesting access from within the enterprise network may require a username and password for identity checks; the procedure for a client requesting access from an external hotspot may require two-factor identity checks. The results of detection also determine the protocol for the next stage, collection.
- **Collect:** Collection is the procedure for gathering all the data required to make a policy decision. This includes credentials and attributes such as identity, level of trust of the device, perhaps location.
- **Enforce:** In this stage, eTIPS makes a policy decision based on the gathered data and set of rules that were selected in the collection phase. The result of this

decision is a policy enforcement profile. This profile is then mapped to specific commands to be pushed to the enforcement devices.

- **Remediate:** In some cases, the decision is to deny, or limit access until some remediation action is taken. The eTIPS workflow includes a remediation stage which allows for this remediation to occur and then to be followed by a repeat of the workflow. The result of a remediation decision is to apply some remediation enforcement profile and some commands to the client to assist in its remediation. Depending on the remediation required, this might be automatic (requiring no action from the user) or manual (requiring explicit action from the user).

As described above, the eTIPS workflow applies *proactive* access control. That is, an access control decision is made *before* granting access. But this workflow is also applicable to *reactive* access control, that is, access control decisions made *after* a client has been granted access. In the case of reactive access control, eTIPS repeatedly invokes the workflow based either on a periodic timer or a network event. For each repetition of the workflow additional data may be include in the collection and enforcement stages, such as data obtained from an intrusion detection system.

It is useful to highlight some of the key benefits Avenda's solution architecture, specifically as it is implemented by eTIPS.

- **Flexible, extensible policy definition:** The administrator can configure attribute-based service, role-mapping, health and enforcement policies in a streamlined and uniform manner. Rule definitions can be based on roles, health, time, date, location, access and authentication protocol attributes, identity store attributes, connection method, white and black lists, MAC & IP address lists. The policy definition sub-system can be extended in a running system to add new policy attributes and rules.
- **Powerful rules engine:** Behind the workflow is a powerful rules engine designed to act on the extensible policies and rules of the policy definition sub-system. Based on these inputs, the engine determines and abstract "enforcement profiles" and then converts this to specific enforcement rules. eTIPS supports the ability to simulate policies and place the system in monitor-only mode. This enables the administrator to experiment with complex policies before deploying them in the network.
- **Out-of-band deployment:** eTIPS platform sits outside the regular traffic path and makes use of RADIUS and TACACS+ based enforcement as specified by the supported NAC frameworks. Most network devices support these protocols. Network performance and scalability are not impacted, unlike with in-band-based enforcement technologies. In addition, the enforcement of the policy decision is synchronized with the granting of access, unlike with non-integrated protocols such as SNMP.
- **Enforcement with existing infrastructure:** Rather than deploying enforcement devices and thereby duplicating the network infrastructure, eTIPS controls enforcement using the capabilities of the existing infrastructure. The abstraction of enforcement attributes enables eTIPS to apply enforcement in a multi-vendor

- network infrastructure and to easily integrate new devices as they are added to the network.
- **Multi-vendor device support:** eTIPS can push enforcement commands to any vendor's switches, routers, wireless access points, firewalls and VPN devices using both standard and vendor-specific RADIUS attributes such as VLAN, filter ID for ACLs, Downloadable ACLs, policy based ACLs and others. Enforcement profile abstraction enables administrator to use the same set of rules to enforce access control on different types of devices.
 - **Multiple NAC framework support:** With its extensible architecture eTIPS natively supports both Cisco NAC and Microsoft NAP frameworks and acts as a unified policy decision point for both frameworks. The enterprise can use best-of-breed capabilities of either framework and define a single set of policies to control access to network and server elements. The extensible architecture also makes it possible for the eTIPS platform to support standard frameworks, such as TNC, as they evolve.
 - **Rich APIs:** eTIPS supports a rich set of APIs for configuration and monitoring. This allows third-party applications to interface to the eTIPS policy subsystem. It also makes it possible to configure eTIPS with external scripts, thereby easing the administration overhead.
 - **Integrated Remediation:** With eTIPS, remediation is fully integrated into the workflow from the definition phased through the decision and enforcement phases.
 - **Enterprise-class management and deployment scalability:** The platform supports a fully replicated cluster of eTIPS appliances for high availability and load balancing. All members of the cluster can be centrally managed, with support for consolidated dashboard view of all session activities. All configuration changes are replicated throughout the cluster without need for a system restart.
 - **Cost-effectiveness:** eTIPS uses existing identity stores, network infrastructure and posture validation and audit servers, thus increasing return on existing investment and reducing total cost of ownership.

Beyond Network Access Control

As stated in the introduction, Avenda believes that policy management services will play an ever increasing role in the day-to-day operations of enterprise networks. Consequently, flexibility and expandability have been primary factors in the design of the eTIPS architecture.

From discussions with customers and partners, some additional policy management needs have already been identified.

- **Device Identity:** In several situations the devices themselves need to be identified. Policies can then be specified based on device identity as well as user identity.
- **Client provisioning:** eTIPS can push policy decisions to the clients themselves allowing the client itself to enforce some of the policies. This might be to

optimize the device behavior to match the services of the network (such as for quality of service parameters) or for a virtual machine monitor to enforce policies for virtual machines.

- **Application access control:** Policies can be specified based on specific application requirements and then applied to the access of those applications. Specifically, different policies might apply for Web access, file access, mail access. In the future, applications will integrate with the policy management system in order to determine application access control
- **Fine-grain control:** Within an application, the policy rules and decision might need fine-grain control. For example, read access and write access are likely to have different policies (as is already the case in file systems). Different policies might be applied to different data within the application.
- **Reactive policy definition and enforcement:** Various intrusion detection and attack mitigation systems have been deployed and are becoming more prevalent. In the future these will integrate with the policy subsystem sharing the same policy definitions and leveraging the enforcement and logging mechanisms of the policy management system.

Summary

Network access control has created a demand for improved, more powerful policy management solutions. Avenda has addressed this emerging market with the Enterprise Trust and Identity Policy Management System (eTIPS).

Recognizing that access control is a multi-vendor, multi-component solution, eTIPS has been designed to integrate with existing infrastructure and emerging NAC frameworks so as to take advantage of capabilities already embedded in the network. The eTIPS architecture is also well suited to solve future requirements that IT managers will demand as their policy management requirements grow and mature.