



Aruba Networks Secure Mobility and Avenda Systems Policy Management

Deploying Automated User Access Control

Target Markets

Organizations that understand the advantages of enterprise class network security, scalability and compliance administration. From the most demanding of Enterprises, financial institutions, government agencies, universities, healthcare organizations to small businesses.

Introduction

The growing need to offer broader employee, guest and partner access within organizations has created greater and often times unwarranted access to network and server resources than ever before. With this freedom and mobility has come a need to better protect against unintentional and possibly malicious attacks on intellectual property and resources. Furthermore, wired, wireless and VPN access methods for these same users has forced organizations to create silos of policy systems and authentication stores that may or may not interoperate with each other.

The Challenge

IT organizations tasked with preventing unauthorized wireless access, theft of information and malicious, destructive activities, must identify and authenticate all users and endpoints in order to minimize risk. In addition, government compliance initiatives are forcing organizations to proactively deploy stronger identity and reporting mechanisms.

It is no longer prudent to just deploy basic wireless authentication methods and install silos of policy infrastructure in hopes that all users abide by the rules. The alternative is to deploy a solution that unifies policies and enforcement, where a single policy platform helps eliminate unnecessary infrastructure and streamlines associated management functions for wired, wireless and VPN access.

The Aruba and Avenda Solution

Aruba's wireless solutions' support for 802.11i and Avenda's eTIPS policy platform combine to provide a standards based, secure infrastructure that addresses the above challenges and more.

The Aruba Mobility Controllers offer a wide range of wireless and wired network mobility, security, and remote access requirements for enterprises of any size. And the Avenda eTIPS platform delivers an advanced level of network access security and policy management.

Aruba Multi-Service Mobility Controllers

The Aruba line of mobility controllers includes multiple models, sized and priced to support the varying requirements of different sized mobile networks

Available Models

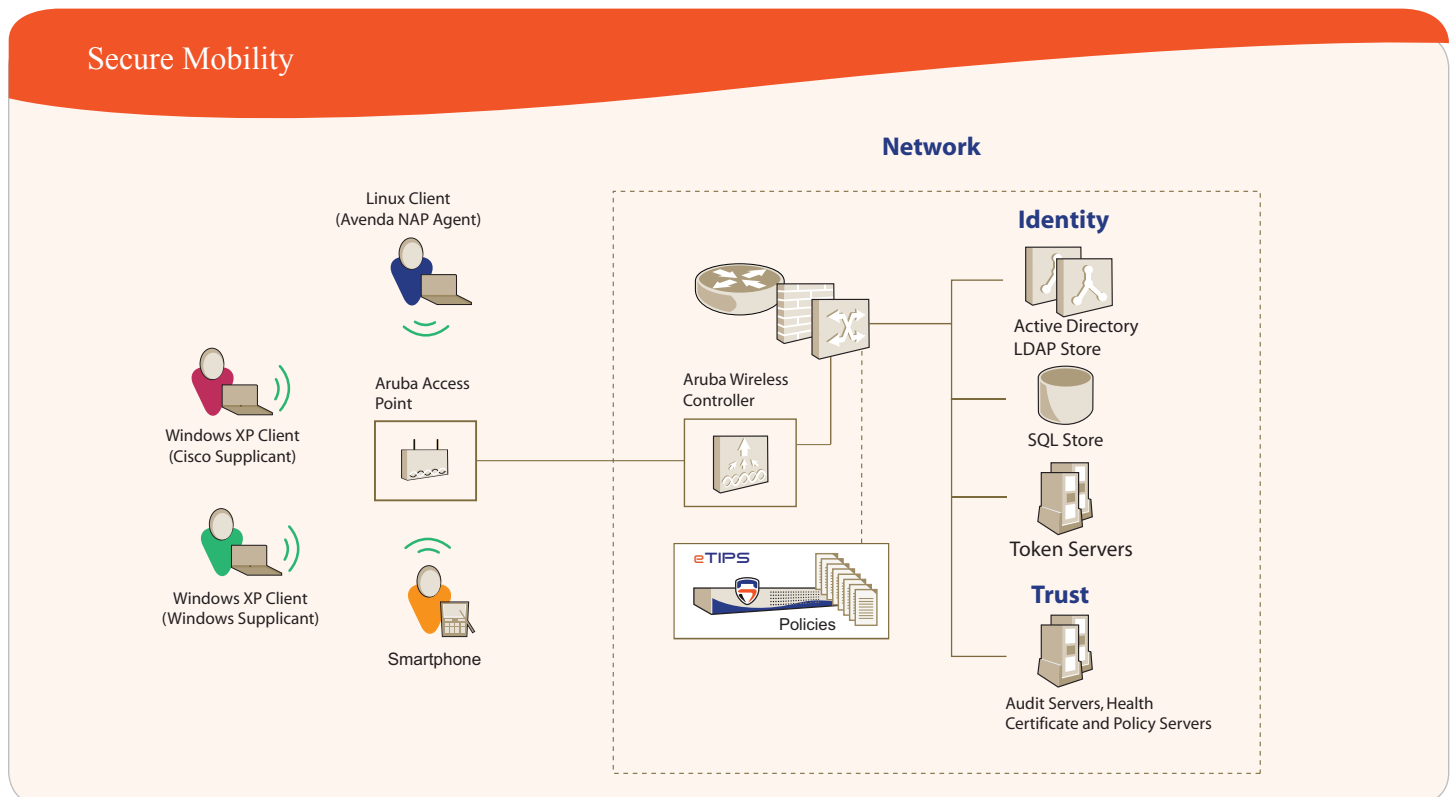
- MMC-6000
- MMC-3000 Series
- MMC-2400
- MMC-800
- MMC-200

Benefits

- Role-based network access and privileges
- Consistent policy enforcement regardless of device or location (managed and unmanaged end-points such as laptops, handhelds, printers, and ad hoc wireless access points)
- Microsoft NAP posture and health checks with the ability to mitigate end-point compliance
- Improved security, reporting and regulatory compliance
- Same policy platform for wired and VPN access needs, as well

Secure Network Mobility

The Mobility Controller is the primary integration component in the Aruba wireless solution, designed to address a wide range of wireless and wired network mobility, security, and remote access requirements for enterprises of any size. The Aruba Mobility Controller is an ICSA certified stateful firewall that provides centralized encryption delivering all traffic to the firewall, which in turn enforces policy and enables advanced traffic aware functionality. Per-user authentication, identity and posture checks, and policy enforcement is performed with a combination of Avenda's standards based eTIPS platform and the Aruba Mobility Controller. The combined products create an enterprise-class, scalable solution that allows the combined solution to work in mixed networking and authentication store environments.



Role-based User Authentication

The combined solution also supports mixed NAC, NAP or TCG-TNC framework deployments from a single infrastructure system and policy model, operating systems, managed and unmanaged endpoints, agents and existing identity stores. For example, whether an employee accesses the network via wireless, wired or VPN connection, or connects using a laptop, handheld or other type of device, appropriate access is granted. Additional enforcements can also be applied that will limit access rights depending on whether the employee is using an approved computer, handheld device or Smartphone.

Visitors and partners are only given access to specific areas of the network for set periods of time; regardless of how they have connected to the network, which strengthens security and minimizes loss of intellectual property.

Unified Policy Enforcement

In order to provide a consistent level of access control, the solution uses eTIPS to provide a clustering capability that allows a single appliance platform to be deployed throughout an organization regardless of location. What this also means is that siloed policy platforms for wireless, wired and VPN are no longer required and we form a unified method for policy administration, updates and enforcement across deployments. The ability to manage a single platform also ensures that policy updates are propagated efficiently and in a timely manner, and consistent enforcement is applied to all forms of access types, i.e. 802.1X with and without Posture, Web Authentication, MAC Authentication Bypass (whitelists/blacklists), etc.

Microsoft Network Access Protection

The Aruba and Avenda solution provides advanced support of Microsoft's Network Access Protection (NAP) framework in Windows Server 2008, Windows Vista, and Windows XP Service Pack 3 environments. Agents can also be used to extend Posture and health check features to all major Linux releases. Once identity is established through authentication, administrators can define granular control based on whether a client/endpoint is compliant with corporate governance policies. In the event the endpoint is not compliant or healthy, the eTIPS platform natively interacts with the Aruba Controller and NAP components to bring the client into compliance. A pre-connect check can compare endpoint security settings against enterprise security policies such as anti-virus version, firewall settings or operating system patches. To provide additional protection the Aruba/Avenda solution can also interact with networking infrastructure to assign them to a QUARANTINE VLAN so that remediation can be performed if needed.

Avenda eTIPS Trust and Identity

eTIPS enables organizations to securely manage the access and visibility privileges of all users and endpoints on their networks.

Analyst Insight

Microsoft's Network Access Protection (NAP) solution was cited as a leader (the top category) in a recent independent report, "The Forrester Wave: Network Access Control, Q3 2008."

Compliance and Reporting Tools

As customers implement new wireless networks with richer authentication methods, built-in policy monitoring allows IT administrators to generate detailed reports regarding the health of the policies, and endpoints in their network before enforcing network access control. A policy simulation utility allows administrators to determine if VLAN, or ACL assignments have been properly assigned within new policies to ensure successful deployments. A built-in audit server can also be used to assess threats/vulnerabilities, and hence determine the posture of managed and unmanaged devices. The eTIPS Policy Manager also includes:

- Activity Dashboard for all sessions with detailed information per user
- Canned and custom filters for monitoring and report generation based on correlated session and accounting data
- Consolidated cluster view for monitoring, reporting and accounting records

Conclusion

In today's business-critical environments, 24/7 uptime is not an option but a strategic imperative. The Aruba Mobility Controller combined with the eTIPS platform can be quickly and confidently deployed to provide a new level of user, endpoint and network security. The integrated solution also provides the ability to consistently apply role-based authentication and authorization across any sized organization, regardless of location.

Standards based protocol and framework support ensure that organizations can leverage existing identity stores and networking equipment to extend role-based access policies to wired and VPN installations. Rich reporting and troubleshooting tools make compliance efforts easy and accurate. Benefits include:

- Improved return on investment (ROI)
- Consistent policy enforcement
- Unified management and control

To learn more about user and endpoint wireless edge security:

info@avendasys.com



Avenda Systems, Inc.
3255 Scott Blvd., Bldg. 2, Suite 102
Santa Clara, California 95054
408.748.0902
www.avendasys.com