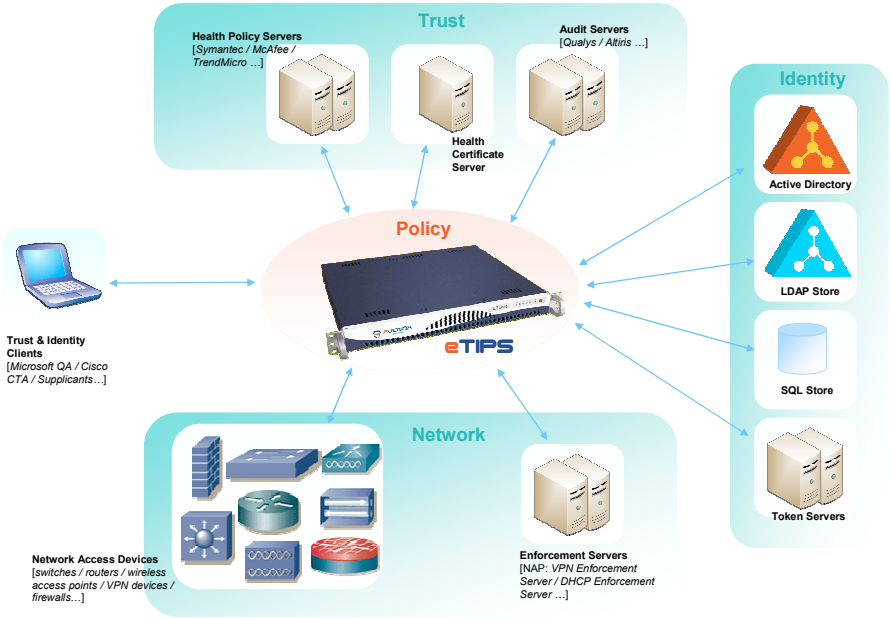
Enterprise Trust and Identity Policy System - eTIPS

Overview

There is a critical need in the enterprise to control employee, guest and partner access to network and server resources in order to prevent unauthorized access and theft of information and to prevent malicious, destructive activities in the form of denial- of-service attacks and damaging viruses and worms. The network administrator needs the flexibility to configure and manage who has access, under what conditions, and the level of access to network and server resources. The administrator also needs the ability to deny access, either proactively or reactively, to unauthorized or misbehaving clients. Current compliance laws also require accurate reporting and monitoring of all activities related to access to critical resources. What is available today is a mishmash of access control architectures and access enforcement technologies.



eTIPS is a comprehensive, highly scalable and high-performance trust and identity policy system that uses existing enterprise identity stores and network infrastructure to provide a unified network access control solution spanning different client operating systems and agent technologies, network access technologies and protocols, and enforcement and remediation mechanisms. eTIPS enables the enterprise to:

- ✓ Define flexible policies for access control decisions and trust determination
- ✓ Identify and authorize the users and devices that access the network using existing enterprise identity stores or local store
- ✓ Evaluate the posture or health of the devices that access the network using existing network access client technologies and posture validation systems
- ✓ Enforce network access rights by downloading enforcement decisions based on flexible policy definitions to existing network and system infrastructure elements from a variety of vendors
- ✓ Quarantine and provide automatic or manual remediation services for non-compliant devices using the capabilities of existing network infrastructure and client agent
- ✓ Audit and enforce policies on agent-less devices using existing audit servers
- ✓ Centrally monitor all user and device sessions and network policies applied to those sessions through the built-in activity dashboard
- ✓ Simplify and consolidate guest access by means of the built-in guest portal and existing network infrastructure support for captive portals
- ✓ Authenticate administrative access to devices and systems and authorize commands that can be executed on them

eTIPS reduces operational complexity and cost by consolidating user and device authentication, authorization, access control, trust determination and monitoring under a single policy management system. It integrates with existing identity stores, network infrastructure, posture validation servers, audit servers and logging systems through well defined protocols, APIs and standards.

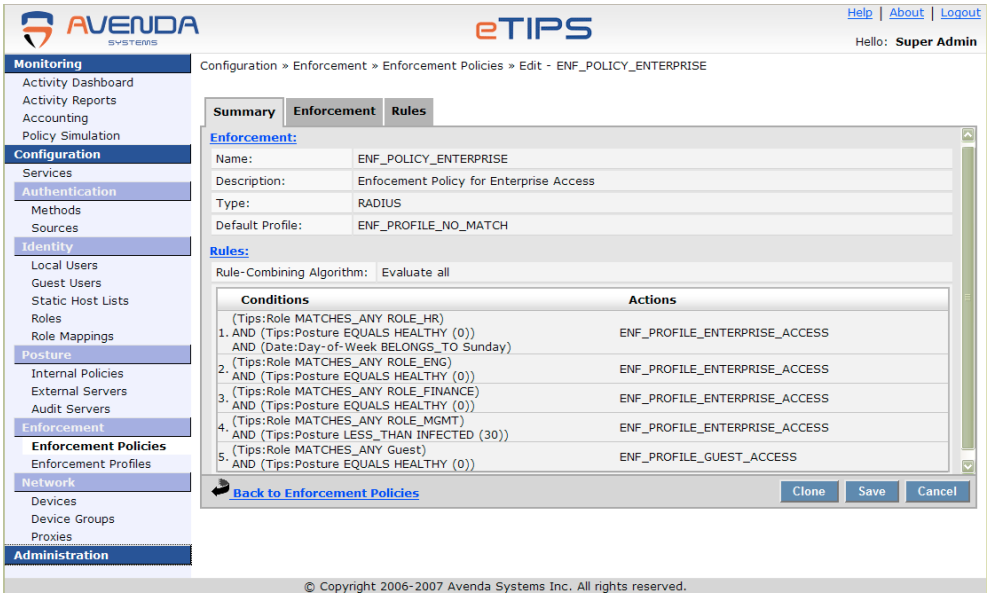
Benefits

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.

Out-of-band deployment: eTIPS platform sits outside the regular traffic path and makes use of RADIUS and TACACS+ based enforcement, which is available on most managed network devices. Network performance and scalability are not impacted, unlike in-band and SNMP-based enforcement technologies.

Rich APIs: Rich set of APIs for configuration interface eases configuration burden. Policy server APIs allows third-party interfacing with the eTIPS policy subsystem.

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.



Flexible policy definition: Powerful rules engine and rules editing interface built using latest Web 2.0 technologies allows browser based access from anywhere. 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 abstraction of enforcement attributes enables enterprises to continue to use a multi-vendor network infrastructure. The ability to simulate policies and place the system in monitor-only mode enables the administrator to experiment with complex policies before deploying in the network.

Multi-vendor device support: eTIPS can push enforcement commands to any vendor's switches, routers, wireless access points, firewalls and VPN devices that support standard and vendor-specific RADIUS attributes such as VLAN, filter ID for ACLs, Downloadable ACLs, policy based ACLs, private VLANs and others. Enforcement profile abstraction enables administrator to use the same set of rules to enforce access control on different types of devices.

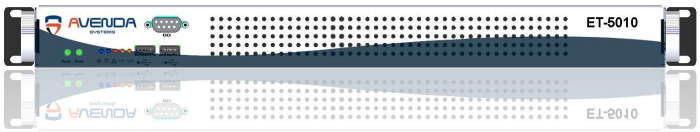
Cost-effectiveness: eTIPS uses existing identity stores, network infrastructure and posture validation and audit servers, thus increasing return on investment and reducing total cost of ownership.

Features & Specifications

Network access control framework native support • Cisco NAC Framework • Microsoft NAP Framework • Extensible architecture to support other frameworks	**Scalability** • Redundancy support with eTIPS cluster nodes • Automatic replication to slave nodes • Centralized management of all cluster nodes	**Administration** • HTTPS – secure browser access to administration console • CLI (ssh or serial port) • Centralized management of cluster nodes • Multi-level administration
Policies • Powerful rules engine, with extensible attribute dictionary based rules definitions. Rule definitions based on roles, health, time, date, location, protocol attributes, white and black lists, MAC & IP address lists	**Access type and authentication methods** • Wireless 802.1x (EAP-FAST, EAP-TLS, EAP-TTLS, PEAP) • Wired 802.1x (EAP-FAST [EAP-GTC, EAP-MSCHAPv2, EAP-TLS], EAP-TLS, EAP-TTLS, PEAP [EAP-GTC, EAP-MSCHAPv2, EAP-TLS]) • EAPoUDP (Cisco L2IP & L3IP) – EAP-PEAP, EAP-FAST	**Identity Stores** • Active Directory • Any LDAP-compliant directory service • ODBC-compliant SQL store (Oracle, MS-SQL, mySQL …) • Token Servers (RSA SecurID, …)
Posture / health validation & supplicant (client technology) • Cisco Trust Agent and associated posture plugins • Microsoft Quarantine Agent and associated system health agents • Cisco Secure Services Client, Funk Odyssey, Microsoft, …	**Posture/health validation (server)** • Internal posture validation (OS version, Firewall, Anti-spyware, HIPS and others) • External posture validation with Symantec, McAfee, TrendMicro and other posture validation servers	**Client OS support for identity and posture** • Windows XP, Windows Vista, Windows NT 4.0, Windows 2000, Red Hat Linux
Audit • Triggered audits with Qualys, Altiris and other audit servers	**Agent-less hosts** • MAC authentication bypass • Non-responsive host with triggered audits	**Remediation** • Auto remediation • Remediation portal using HTTP redirect URL support in network devices • Manual remediation with remediation URL notification on the client agent
Enforcement • VLAN • Downloadable ACLs • Policy-based ACLs • Filter-ID based ACLs • Private VLAN • Other enforcements	**Policy simulation** • Simulate policies on the administrative console before deployment • Service categorization, role mapping, posture validation, audit, enforcement policy and chained simulation	**Monitor mode** • Track and generate inventory reports for system assets and health state of the systems in your network before enforcing any network access control
Guest access • Receptionist console for guest handling • Guest portal for authentication • Uses existing support in devices – Web-auth and authentication proxy	**Reporting, Monitoring and Accounting** • Activity Dashboard for all session activities with detailed session information • Canned and custom filters for monitoring and report generation based on correlated session and accounting data • Consolidated cluster view for monitoring, reporting and accounting	**Device administrator authentication and authorization** • Industry-standard TACACS+ implementation for administrative access to network devices and management systems • TACACS+ accounting • Support for command authorization
APIs • Configuration SOAP API to configure all aspects of the eTIPS system • Policy server SOAP API for third-party interfacing to the policy system	**Logging & Troubleshooting** • Consistent logging for all modules, including standard syslog support • Control cluster-wide logging from the administration interface	**RFC & standards compliance** • RFC – 2246, 2548, 2716, 2759, 2865, 2866, 2869, 2882, 3079, 3579, 3580, 3748, 4017 • Internet Drafts: PEAPv0, PEAPv2, EAP-FAST, EAP-FAST dynamic provisioning, EAP-TTLS, Microsoft CHAP Extensions

Avenda ET-5005, ET-5010, ET-5020, ET-5040 Hardware Specifications

Processor	Single or multi-processor, dual core 64-bit processor, with different speeds based on model number
Ports	2 Gigabit Ethernet ports, 1 serial port
Form factor	Mini 1U; rack-mountable chassis
Dimensions & Weight	16.7"W x 1.7"H x 16"D 20 lb
Storage	~200 GB
Power Supply	Thermal control 275W AC power supply with PFC UL approved; FCC compliant
Assembly	Custom cabling for optimal chassis cooling Rigorous system-specific quality control



AVENDA SYSTEMS
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

Document version 7.0