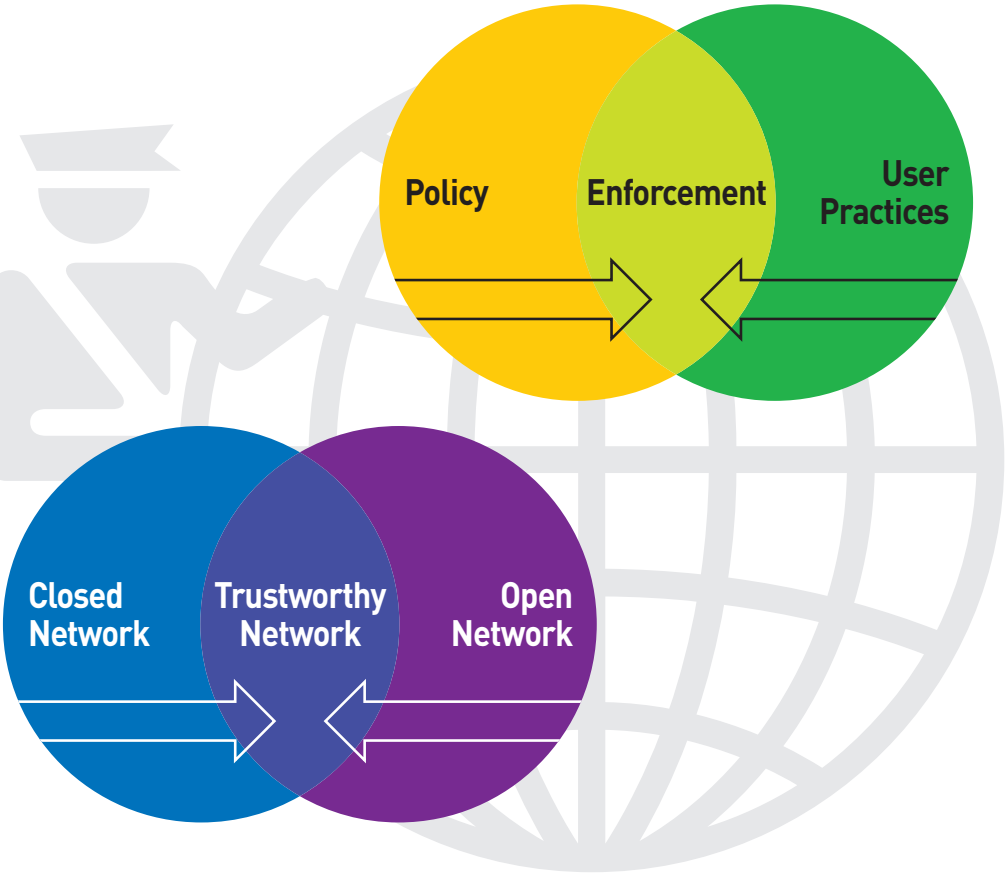


Sygate Secure Enterprise:
Making Open Networks Trustworthy

The Open Network Problem

Since the introduction of the Internet, enterprise networks have evolved from a closed to an open environment. As it became clear that information technology—in the form of the Internet, wireless, remote connectivity, and network-enabled applications—would increase the productivity of workforces, streamline business processes, and open new markets, enterprises began to open their networks to the outside world. An unfortunate byproduct of this evolution to open networks was the fact that enterprise assets (including intellectual property, brand, computing resources, and sensitive data) are exposed to unprecedented risk, resulting in significant financial losses. Despite these consequences, networks remained open simply because the benefits of open networks were greater than the associated risks.

Benefits

- Secure enterprise networks against intrusion
- Enable the secure deployment of productivity-enhancing technologies, such as VPN, Wireless LAN, and collaboration applications
- Enforce the presence and effectiveness of security applications, such as anti-virus, firewalls, IDS, and other third-party security software when connected to the Virtual Trusted Network
- Gain visibility and control of network-enabled devices when they travel outside your network
- Achieve compliance with enterprise security policy and regulatory requirements

Features

Application-Centric Firewall

Sygate Security Agent incorporates an application-centric firewall that stealths host systems, provides stateful firewalling, applies rule-based security policy, and controls application usage.

Application-Based Intrusion Prevention Engine

Sygate Security Agent's intrusion prevention engines applies patterns of known attacks to all incoming and outgoing traffic as a second layer of defense. Sygate's unique application-based approach to intrusion prevention uses application layer information to more effectively identify and block known attacks.

Host Integrity Enforcement

Host Integrity Enforcement enables enterprises to enforce security policy at all endpoints and network access points to the enterprise network including VPN, Wireless, and RAS dial-up servers. Host Integrity includes the ability to check for the presence and update status of firewalls, intrusion prevention, anti-virus, and other third-party applications prior to granting access to the enterprise network.

User, Application & Network Behavior Learning

The Sygate Secure Enterprise suite has the ability to learn the behavior of users, applications, and networks for the purpose of automating the policy creation and enforcement process. Sygate Security Agent learns which users communicate with which applications and how. Sygate Enforcers learn what security measures are in place for each user and provides a comprehensive view of policy compliance. Sygate Management Server correlates information from Sygate Security Agents and Enforcers to reconcile policy with practice.

Dynamic User, Location & Adapter Policies

Sygate Secure Enterprise dynamically adapts security policies based on the user, the hostility of the network environment, and the access technology that is being used. Dynamic security policies provide the appropriate security for each network environment without impacting the productivity of the user.

Highly Scalable Multi-Server Architecture

Sygate Secure Enterprise is designed to be deployed in large and distributed enterprise networks. Sygate's multi-server architecture provides unlimited scalability, fault-tolerance, performance optimization, and policy uniformity across global enterprise networks.

Security technologies, such as perimeter firewalls, anti-virus, intrusion prevention, and authentication, have evolved to address specific holes in the open network. The proliferation of the Internet on every network device, the increased mobility of those devices, and the introduction of network-enabled applications have rendered traditional network-based security infrastructures vulnerable to a new generation of attacks. Vulnerabilities in VPNs, wireless LANs, operating systems, and network-enabled applications result in the breakdown of enterprise security architectures. Despite the advances in security technology, enterprise networks have never been more vulnerable.

The vulnerability of enterprise networks lies in the gap between security policy and practice. Parallel to the implementation of security technologies, enterprises have developed extensive security policies designed to mitigate the risks of open networks. These policies have been developed to govern the use of applications, the implementation of security measures, remote access to enterprise resources, the use of wireless devices, and countless other security issues.

However, a gap has developed between security policy and the ability of enterprises to implement those policies. Existing security technologies have addressed specific problems but none have built the foundation to solve the open network problem. Today's enterprise requires the ability to understand the communications behavior of their network, reconcile written security policy with that behavior, and then enforce that policy across the entire network.

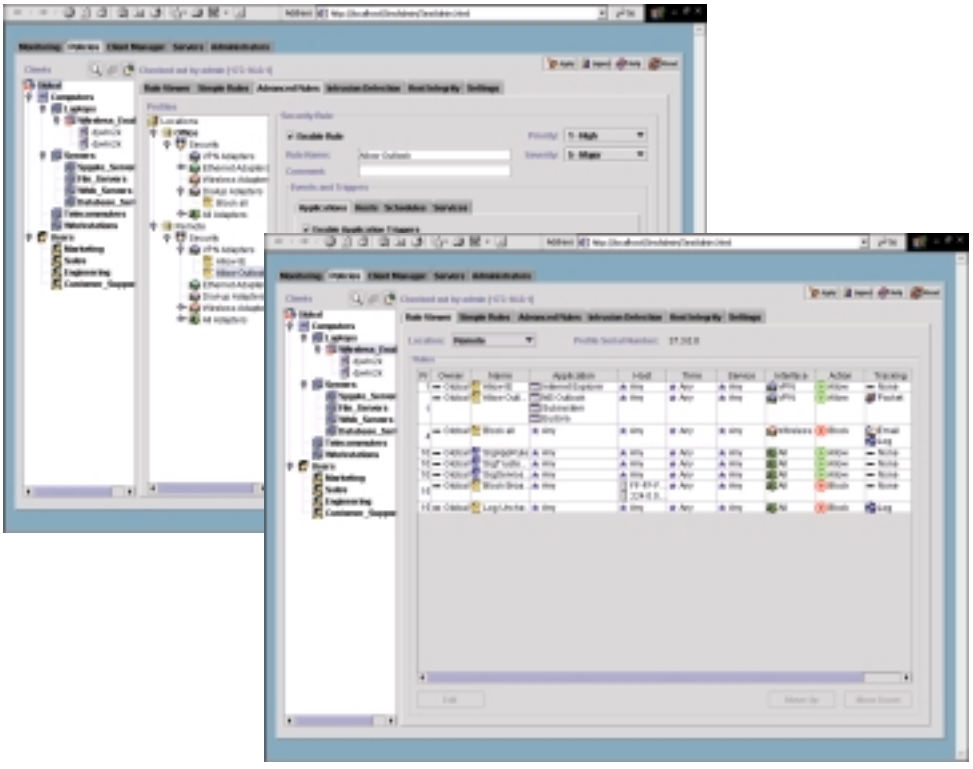
The Sygate Solution

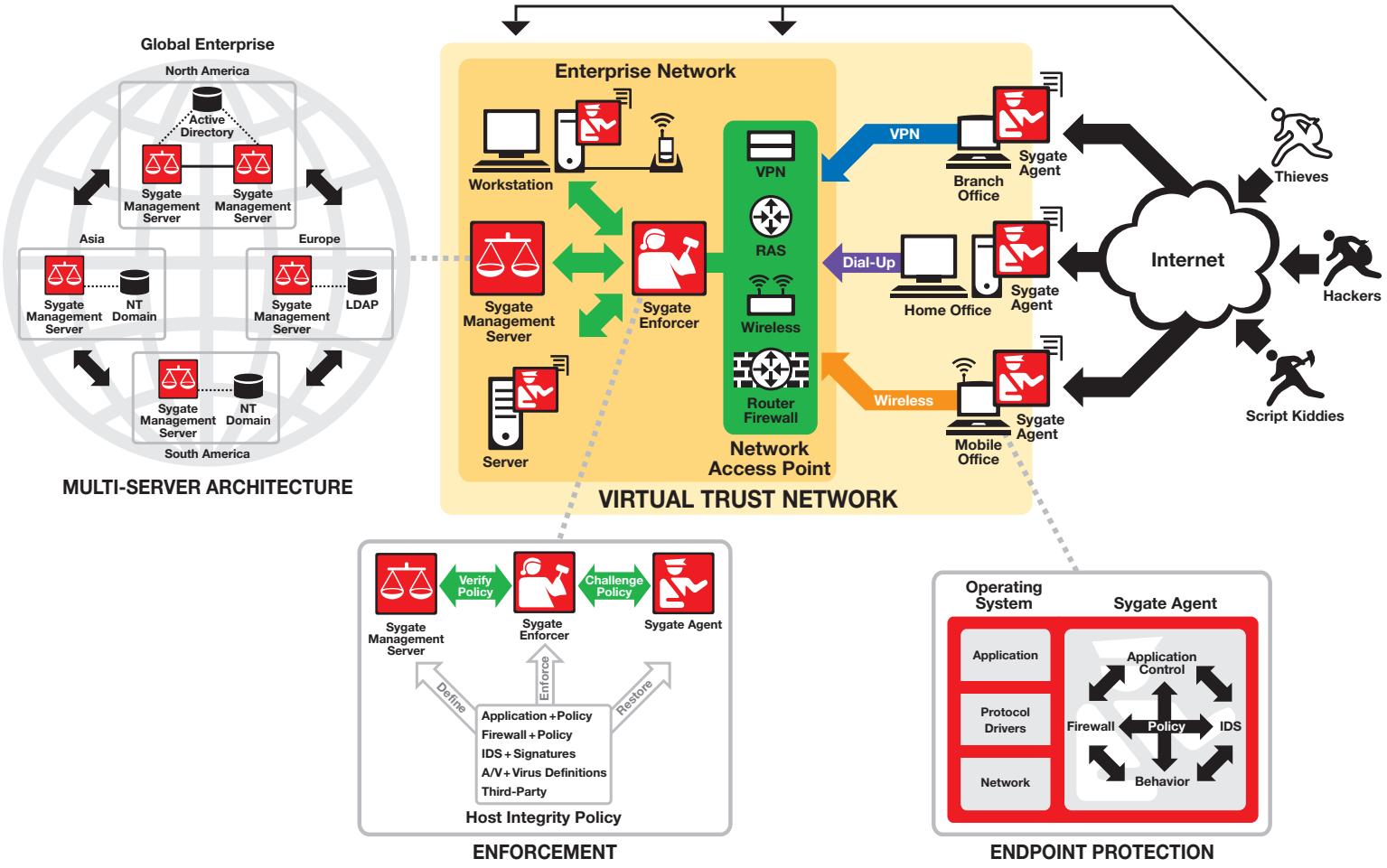
The Sygate Solution to the open network problem provides a foundation that enables enterprises to:

- Learn user, application and network-behavior
- Define policies for correct and safe behavior based on that knowledge
- Enforce policies at the endpoints and network access points of the enterprise

Achieve Trust in Open Networks

The Sygate solution creates what we call Virtual Trust Networks™ (VTN) designed specifically to enforce security policies on every endpoint and network access point. VTNs extend protection to every





point in your organization, establishing a trust in the enterprise network. This trust enables enterprises to continue to deploy productivity-enhancing applications such as Internet connectivity, wireless LANs, remote access, and collaboration applications, while at the same time making their open networks trustworthy.

At the core of Sygate's ability to make open networks trustworthy is the concept of Host Integrity. The Sygate solution incorporates the unique ability to define, enforce, and restore the host integrity for the purpose of securing enterprise networks and valuable data. Defining host integrity involves creating a profile of security applications, data, and policies that must be in place for secure communication. Enforcing host integrity is accomplished by checking the integrity of each host system every time they connect to the enterprise network, and allowing or denying access based on the integrity of the host. Restoring host integrity is accomplished through an access control methodology that allows users who connect to the enterprise network, but are denied access because of integrity loss, to restore their integrity by connecting to the anti-virus, host-based firewall, intrusion prevention and/or other third-party update servers. The Sygate Secure Enterprise suite bridges the enforcement gap that exists today in the enterprise, by ensuring that all devices that connect to the enterprise network are running the correct security application, with the policy and data that is mandated by information security organizations.

Building a Foundation

The challenge is to build a security architecture that allows enterprises to continue realizing the benefits of open networks, while protecting enterprise assets from loss and damage.

Sygate Secure Enterprise combines a sophisticated security agent that runs on each client, one or more policy management servers distributed across the enterprise, and enforcement servers at network access points. Sygate's is the first architecture to enable dynamic security policies that can be tied to individual users, following them as they change location (for example, home to office to hotel) or method of connection (from switched Ethernet to VPN over DSL to wireless LAN). Sygate countermeasures automatically adapt to the changing risks of each environment, ensuring business continuity and appropriate security policy in a distributed and mobile enterprise.

Supported Platforms

SYGATE MANAGEMENT SERVER

Operating Systems

Windows 2000 Server

Solaris 8 or greater

Web Servers

iPlanet Web Server

Internet Information Systems

Database

Oracle

Microsoft SQL

SYGATE SECURING AGENT

Operating System

All Microsoft Windows platforms

SYGATE ENFORCERS

Operating System

Windows 2000 platform

Enforcement Scope

Sygate Enforcers are vendor independent and will interoperate with any standards based networking technology including VPN, WLAN, and RAS.

Sygate Security Agents

Sygate Security Agents are installed on all network-enabled endpoints within an enterprise to provide host-based security, including an application-centric firewall and intrusion prevention engine. The security agent also gathers information for Sygate Management Server and Sygate Enforcers to automate the policy creation and enforcement process.

Sygate Management Server

Sygate Management Server learns communications behavior, creates and deploys security and enforcement policies, manages user and computer group structures, and communicates with other Sygate management and enforcement servers. Through Sygate Secure Enterprise's heartbeat communication protocol, Sygate Management Server learns user, application, and network behavior from Sygate Security Agents and Enforcers to provide enterprises with an up-to-the-minute view of their security posture. With the information that is learned by Sygate Management Server, enterprises can automatically create security policies that link users, connectivity technology, applications, and network communication to security policy. Sygate policies are managed and inherited through group structures of users, workstations, and servers that can be imported and synchronized with NT Domain, Active Directory, and/or LDAP. Sygate Management Servers can be centralized or distributed in a global enterprise to provide scalability, fault tolerance, load balancing, and policy replication.

Sygate Enforcers (VPN, Wireless, RAS)

Sygate Enforcers are network gateway devices that enforce host integrity at network access points to the enterprise network such as VPN, wireless access points, and RAS dial-up servers. Sygate Enforcers communicate with Sygate Management Server to obtain enforcement policy and agent authentication information. When a Sygate Security Agent connects to the enterprise, Sygate Enforcers initiate a challenge response session that determines the authenticity of the agent, the status of the firewall, intrusion prevention, anti-virus, other security applications, and the adherence of policy, signatures, and virus definitions to corporate policy.

SYGATE

Sygate Technologies, Inc.

6595 Dumbarton Circle, Fremont, CA 94555

Tel: 510.742.2600 • Fax: 510.742.2699 • www.sygate.com