

Secure Networks™: Acceptable Use Policy Solution

Secure Networks Benefits

- **Reduces complexity and risk** by embedding active, automated security into the network fabric
- Maps **business policy to network implementation**
- **Improves visibility** into the network as a single entity for faster trouble resolution
- **Provides secure/reliable access to internal and external users** based on their roles within the organization
- **Delivers automation and system-level control** to lower the cost of administration, implementation and troubleshooting
- Enables **application growth** and expansion
- **Increases productivity** through improved access to data/applications

Secure the Network through the Use of Access Policy

Enterasys Acceptable Use Policy Solution is a unique, policy-based system that allows the network to provision required business services to users automatically, while preventing undesirable and malicious traffic from entering the infrastructure. As a key component of a Secure Network, an enforceable Acceptable Use Policy can:

- Secure the enterprise network from undesirable applications and protocols
- Respond quickly and effectively to changes in the environment
- Ensure reliable access to business-critical services by enforcing an application prioritization scheme
- Enable automation and system-level control to lower the cost of administration, implementation, and troubleshooting

Ensuring Security and Productivity through “Acceptable Use”

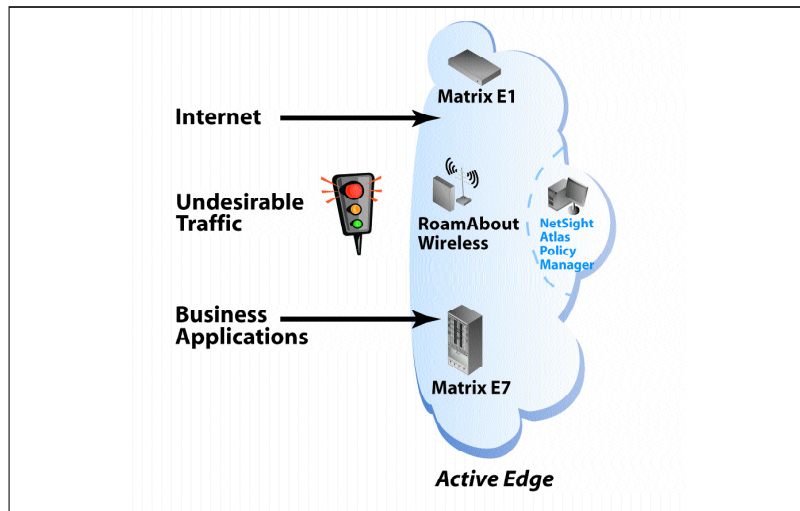
Most organizations have a set of rules and guidelines that dictate how the network should be used. The Secure Networks Acceptable Use Policy provides a foundation for aligning actual network user and application behavior with these business objectives. Typically, an Acceptable Use Policy is formulated with input from a

number of different business policies. The organization’s security policy, for example, may specify network traffic and services that should be eliminated from some or all usability points on the network. Other business policies may highlight how specific network services may be used or which services are mission critical to the business.

Secure Networks Acceptable Use Policy Solution enables organizations to enforce their Acceptable Use Policy proactively and effectively. To do this, a policy architecture is developed that maps the “Roles” of your organization, the “Services” available from the network infrastructure, and the “Rules” that enforce the defined services.

Once identified, Roles, Services, and Rules are leveraged to build the appropriate configuration in NetSight™ Atlas Policy Manager, Enterasys’ graphical, easy-to-use, policy-management tool. In NetSight Atlas Policy Manager, Acceptable Use Policy guidelines are constructed into a policy profile, which is distributed to the network infrastructure. This policy allows appropriate business-service access, but filters out undesirable traffic.

Ensuring the security of technology assets and intellectual property is a primary goal of most Acceptable Use Policies, so the ability to eliminate known threats, such as



rogue applications and protocols, worms and viruses, or Denial of Service attacks is essential. With an Acceptable Use Policy Solution, organizations can benefit from a network architecture that permits required business resources, yet prevents access to resources that are undesirable or prohibited. And, as new security threats emerge, the Acceptable Use Policy Solution allows an organization to respond quickly and effectively, by modifying the network to mitigate the impact of these threats.

With the Acceptable Use Policy Solution, the organization can work more securely and efficiently. As access to undesirable applications and resources is minimized, the bandwidth they have been consuming can be used by business-critical applications and resources. This, in turn, leads to enhancements of in network infrastructure performance, viability and lifecycle.

Secure Networks Acceptable Use Policy Solution:

- Provides increased security
 - Protection from Denial of Service (DoS) attacks at each point of ingress

- Elimination of port scan events
- Prevention of the use of administrative protocols by unauthorized network users
- Rate limiting for non-essential applications
- Enables centrally administered policy for entire enterprise to act as a “distributed firewall”
- Protects the performance of required services
- Deploys in minutes and enforces parameter changes in seconds

The result is an enterprise that is protected from misuse, technology resources that are aligned with business requirements and a more productive workforce.

To Learn More

To find out how Enterasys’ Secure Networks and the Acceptable Use Policy Solution can help you ensure the security, accessibility, and control of your enterprise network, call your Enterasys sales representative or an authorized Enterasys partner, or visit enterasys.com/secure-networks

Secure Networks is a registered trademark of Enterasys Networks. All other products or services mentioned are identified by the trademarks or service marks of their respective companies or organizations. NOTE: Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications.