



Identity Management

Using the Network to Enforce Identity Management

Kelly Kanellakis

Director of Technology, Office of the CTO

Enterasys Networks

kellyk@enterasys.com

Identity Management

- **What is Identity Management (IdM)?**
 - System is able to identify, with a level of certainty that a user, device or application are who they claim to be
 - Consists of user IDs, passwords and other mechanisms to verify identity
 - Identity is used to gain access to information or resources otherwise restricted
- **Why do we want Identity Management?**
 - Control of access to resources and assets
 - Security of information and infrastructure (regulatory compliance)
 - Convenience – Single Sign-On or Password Synchronization



Identity Management

- **What comprises Identity Management?**

- Identity (credential) Control system
- Identity Authentication system
- Password Synchronization system or Single Sign-On system
- Application Co-ordination Capability (linked to SSO)

- **Where do we want Identity Management?**

- Public Networks differ from Private Networks
- Public Sector differs from the Private Sector which differs from the Military



Identity Management:

Valuable to most organizations to allow them to know *WHO* is using the infrastructure and *HOW*

Identity Management and the Network

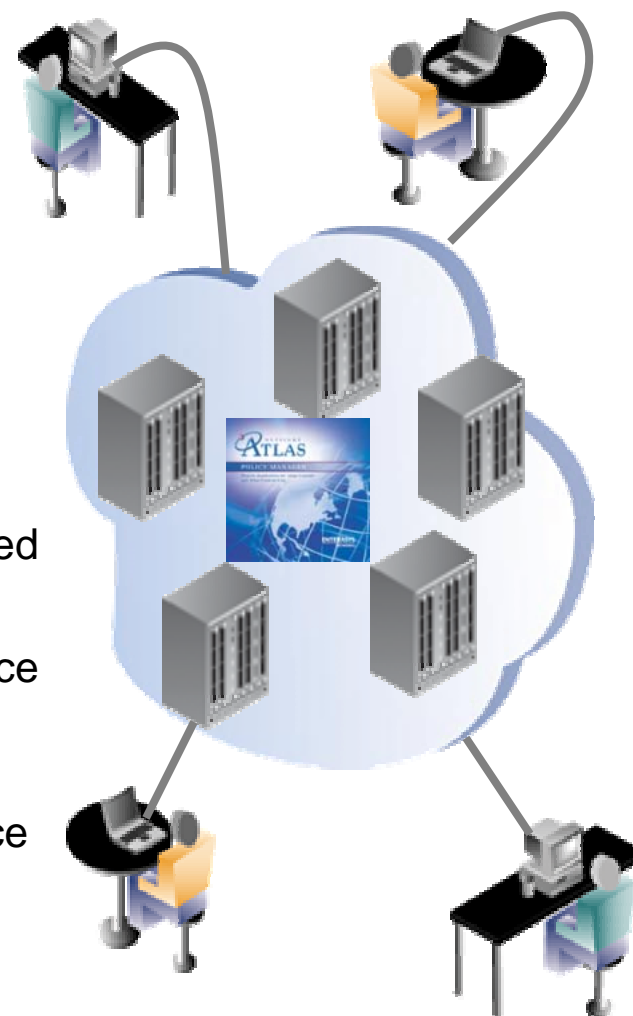
- **Networks are pervasive**

- Every device must touch the network to communicate
- Most organizations are fully networked
- Intercommunication between networks is now common

- **Networks are intelligent**

- Old goals of the network were simple connectivity, increased capacity and cost containment
- New goals are now Continuity, Context, Control, Compliance and Capacity – the 5Cs
- Flow-based network edge architectures classify communications sessions in real time with little performance impact

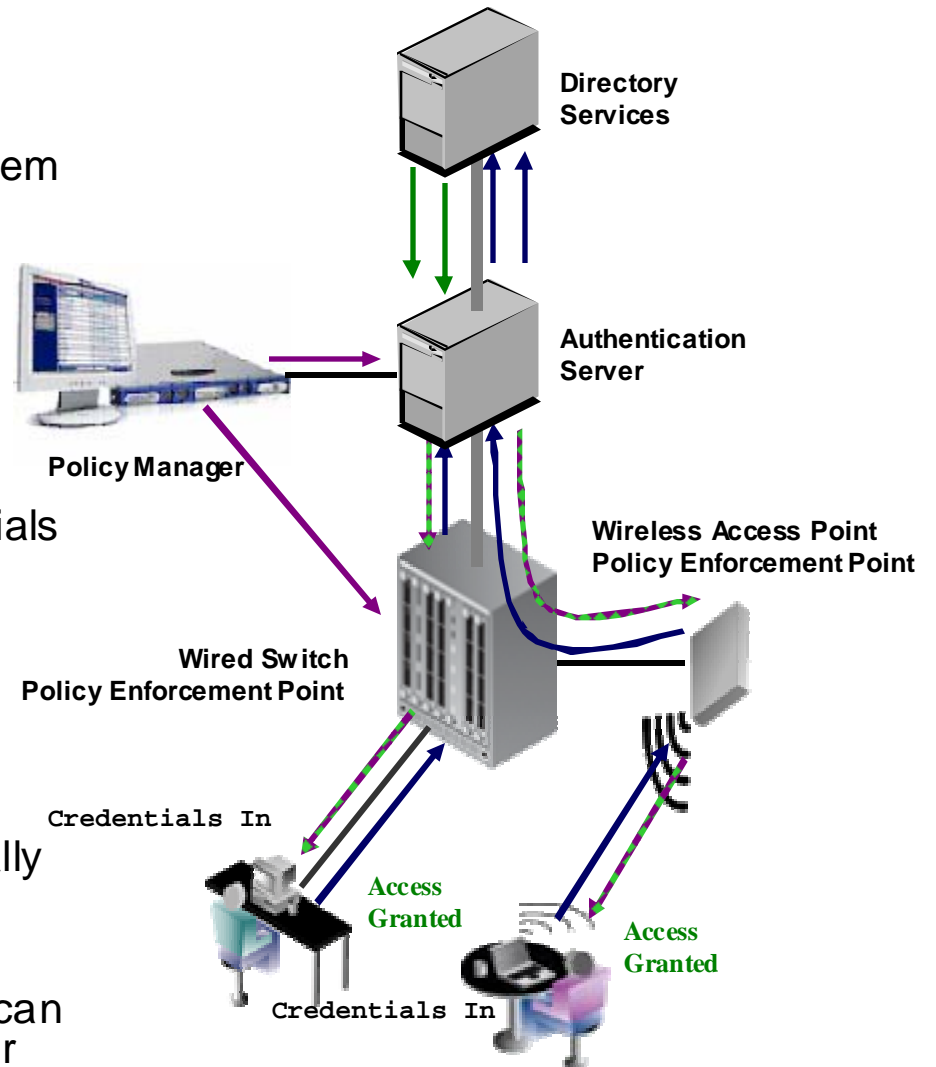
- **Networks are an ideal policy enforcement point for Identity Management**



Network Enforcement of IdM

How does Identity Management work with the Network?

- User identification is entered at the operating system level
 - User ID / Password, Tokens, Certificates
 - These become the credentials for IdM
- User attempts to access network resources
- Via IEEE 802.1X EAP first network ingress point challenges unknown user/device for their credentials using specific methods
- Credentials passed by OS or other 802.1X Supplicant back to network device
- Network passes credentials back to an authentication server (usually RADIUS)
- Authentication server can either authenticate locally or contact other back end services (usually a directory service) to authenticate the request
- Once credentials are verified, this user or device can be granted access and have policy applied to their communications



Advantages of Network Enforced IdM

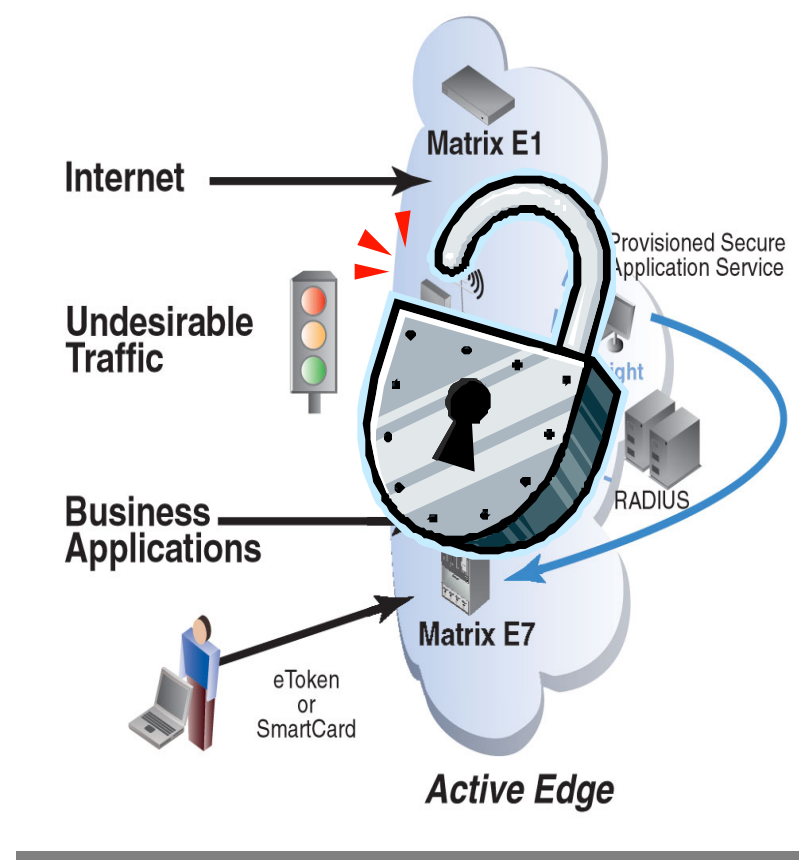
- Network becomes an enforcer for Identity Management processes
- Access to resources is very controlled
- Security and Identity become an integral part of the infrastructure
- The integration with back-end directory services serves as a foundation for single sign-on and Identity Management
- New solutions are made possible based on Identity Management enabled infrastructure
 - Acceptable use policy
 - Secure guest access
 - Secure wireless access
 - Tracking of anomalous behavior to a user



All this is possible with a Network Enabled IdM System!

Network Enabled IdM - Summary

- Identity Management is a requirement for any security conscious enterprise
- The networks of today are pervasive and intelligent
- The network becomes an ideal policy enforcement point for IdM
- With Network Enabled IdM, other more comprehensive solutions are possible for the business



Thank You!

