

Identity-Based Network Access Control

FEATURES

Comprehensive Access Control

- Control access to specific files and applications
- Security Zones based on location, device, and authentication

Transparent User Experience

- Integrated Windows Logon
- Single Sign On for Web and Files
- Supports all Windows, Mac, and Linux

Zero Network Disruption

- Works with all switching environments
- No client required
- High performance, Low latency

Authenticates Users

- Leverages existing identity stores
- Policy managed through directories

Checks Unmanaged Devices

- Authenticates, admits, quarantines
- Checks for all anti-virus, anti-spyware, personal firewalls
- Updates, OS, Service Pack, and Patch Level
- Processes, Ports, Registry entries, Files

Cleans Compromised Devices

- Terminates, blocks or remediates
- Self-remediation for non-compliant devices
- Flexible remediation for partial compliance

With more non-employees and third-parties accessing enterprise networks, Network Access Control (NAC) is emerging as a critical component to enterprise security. Threats to network security come in two basic types: first, from PCs that are corrupted, and second, from individual users with access to sensitive resources. To securely extend network access, threats from both devices and people need to be contained.

Caymas Identity-Driven Access Gateways provide the most comprehensive Network Access Control (NAC) solution available by protecting the network from misconfigured devices while providing granular access control to enterprise resources on a user by user basis. This allows enterprises to control not only who can connect to the network and from what type of device, but also where users can go once they're connected. With granular access control, network plug-and-play, and user transparency, Caymas offers the most secure, easy-to-deploy NAC solution available on the market.

GRANULAR ACCESS CONTROL

Once a user is on the network, Caymas gateways control access to networks, ports, protocols, and even as granular as specific files and applications. Caymas gateways support Security Zones based on four major components of Identity – user/role, device, location, and qualifiers – to dynamically determine the user's level of access, and then keep a detailed audit log of all user/resource activity on the network.

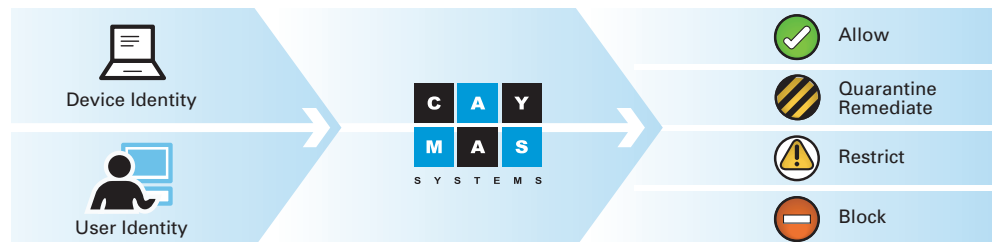
NETWORK PLUG AND PLAY

Many NAC solutions require extensive infrastructure upgrades/forklifts or control access

through VLANs – options that unnecessarily burden network engineering. Caymas gateways provide a simple overlay that is deployed without network upgrades or reconfiguration. Managing the Caymas gateway is simple given its tight integration with directories and permissions stores – Active Directory, LDAP, RADIUS, 2-factor, and PKI. And once the access policy is defined, change management is easily moved from networking engineering to the help desk, saving time and money.

USER TRANSPARENCY

Key to any NAC deployment is a transparent end-user experience, only requiring user attention if the PC fails to meet the security policy or the user attempts to access an unauthorized resource. Caymas gateways support Integrated Windows Logon, meaning users are automatically authenticated, scanned, and given access to a Security Zone without any user intervention. Users that fail the device check can self-remediate through simple, informative remediation screens, saving calls to the Help Desk. And all of this functionality can be clientless, allowing flexibility for both managed and unmanaged PCs.



BENEFITS

Protect Wireless LANs and Conference Rooms

Force user authentication and a device scan before allowing users onto shared networks, and then control where they can go once they're on. Optionally add strong encryption.

Control Guest / 3rd Party Access

Restrict guests, contractors, and consultants to Internet access only, or allow them access to specific data on the internal network.

Secure Remote Access

Use the full-featured SSL VPN capabilities of the Caymas gateway to apply the same policy to users whether they are on the internal LAN or remote.

Protect Critical Resources

Allow only authorized users access to sensitive data and applications, with a detailed audit trail of every access.

Single Access Control Solution

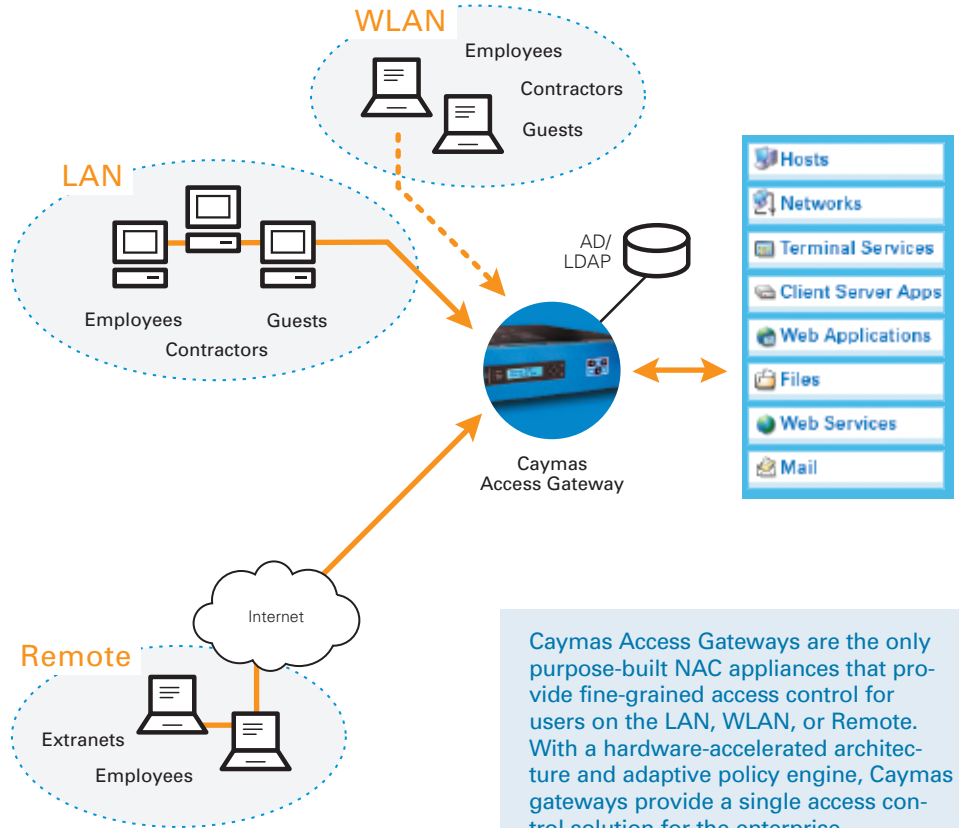
Manage a single access control policy for users whether they are wired, wireless, or remote.

Identity-Based Audit Trail

Know who is doing what on your network through a consolidated set of Audit logs that tracks access based on user identity, not IP address.

On-Demand Reporting

Generate user- and resource-based usage reports that can be exported for presentations to senior management or auditors.



Caymas Access Gateways are the only purpose-built NAC appliances that provide fine-grained access control for users on the LAN, WLAN, or Remote. With a hardware-accelerated architecture and adaptive policy engine, Caymas gateways provide a single access control solution for the enterprise.



SPECIFICATIONS

<p>SUPPORTED CLIENT PLATFORMS</p> <p>Windows, Mac, Linux</p>	<p>HOST INTEGRITY CHECK</p> <p>OS and Patch Level, Registry Keys, Ports, Processes, Files, Anti-virus with Last Update, Personal Firewall, Anti-spyware</p>	<p>FAULT TOLERANT</p> <p>Caymas 525: LAN Failover Dedicated High Availability ports Redundant power supplies Redundant power inputs</p> <p>Caymas 318: Dedicated High Availability ports</p>
<p>AUTHENTICATION</p> <p>Local, LDAP, Active Directory, RADIUS, X.509 Certificates, RSA SecurID, Safeword</p>	<p>PHYSICAL DIMENSIONS</p> <p>Caymas 525: 2RU Caymas 318: 1RU Caymas 220: 1RU</p>	<p>MULTI-NODE DEPLOYMENTS</p> <p>Caymas 525: Hub or Spoke Caymas 318: Hub or Spoke Caymas 220: Spoke only</p>
<p>AUTHORIZATION</p> <p>Local, LDAP, Active Directory and RADIUS Groups</p>	<p>PHYSICAL INTERFACES</p> <p>Caymas 525: 4 x 10/100/1000baseT, Dedicated management port, Console Caymas 318: 2 x 10/100/1000baseT, Console Caymas 220: 2 x 10/100baseT, Console</p>	<p>PERFORMANCE</p> <p>Caymas 525: 2.0 Gbps, 600 Mbps encrypted Caymas 318: 380 Mbps, 300 Mbps encrypted Caymas 220: 100 Mbps, 100 Mbps encrypted</p>
<p>AUDIT AND ALARMS</p> <p>Syslog, FTP and SCP for log transfer SNMP traps On box reporting</p>	<p>ENCRYPTION</p> <p>RSA, RC4, DES, 3DES, AES, MD5, SHA-1, IKE, TLS, IPSec</p>	<p>CERTIFICATION</p> <p>Caymas 318 and 525 FIPS 140-2 Validated</p>



Caymas Systems, Inc.
Phone: 408.985.9000
Fax: 408.985.9001
www.caymassystems.com

Contact a Sales Representative: sales@caymassystems.com

© 2006 Caymas Systems, Inc. All rights reserved. Caymas Systems, the Caymas logo, Caymas 220, Caymas 318, Caymas 525 and CaymOS are trademarks of Caymas Systems, Inc. All other trademarks are the property of their respective owners. DS-NAC 7/06 v1