



## Caymas 220, Caymas 318 and Caymas 525 Award Winning Identity-Driven Access Gateways



### Control Access Based on Identity

#### Control Remote Access

- Award Winning SSL VPN
- Business Partner Extranets

#### Control LAN Access

- Award Winning Network Admission Control
- WLAN Security
- Contractor and Guest Access

#### Control Data Center Access

- Regulatory Compliance
- Security Zones for Sensitive Data
- PKI Enable Applications
- Reduced and Single Sign On

### Identity-Driven Access Gateways: The Only NAC and SSL VPN Appliance

Award winning Caymas 220, 318, and 525 Identity-Driven Access Gateways deliver identity-based SSL VPN remote access and Network Access Control (including endpoint security) in a single platform. Caymas Access Gateways feature the most advanced policy engine, accepting inputs based on the identities of users, devices, locations, applications, and the results of host integrity checks, to provide a single point of policy enforcement for enterprises and government organizations. The result is unprecedented visibility and control for access to networks, applications, files and information by internal and remote users. Only Caymas Access Gateways are fully FIPS 140-2 Validated by the US Government, and award winners for both network access control and SSL VPN remote access. Caymas Access Gateways are used by hundreds of commercial and government organizations to control access and control their business.

Caymas Access Gateways are ideal for the following applications:

- **Network Access Control.** Caymas Access Gateways provide real-time Network Access Control, including positive Layer 3 - 7 permit/deny capability to network resources. Moreover, Caymas' Host Integrity Checker, Security Zones and policy synchronization capabilities allows security administrators to tune access rights to meet specific policy requirements.
- **SSL VPN Remote Access.** Caymas Access Gateways include a full featured SSL VPN that supports all application, access and security controls. Policy is defined once for both Network Access Control and Remote Access.

The Caymas 220, Caymas 318 and Caymas 525 are ideal for enterprises that want to simplify access without compromising security. All are drop in appliances that support hundreds to thousands of simultaneous users, providing ultra secure access to remote employees, business partners, and internal users through a single platform via a browser-based user interface. The Caymas 220 is designed for small, single site businesses and supports up to 100 concurrent users. The Caymas 318 is designed for smaller enterprises and remote sites and supports up to 500 concurrent users. The Caymas 525 is designed for medium to large organizations and supports up to 2,500 concurrent users. Caymas appliances provide constant user identity-awareness, thorough access control, integrated transport security and data integrity, and full audit and logging capabilities. With Caymas Access Gateways, enterprises can quickly and securely connect users to required corporate applications.

### Identity-Driven Access

Identity-Driven Access is based on positively identifying and authenticating user, devices, locations, resources and a host of other variables, and then uniquely tagging all communications associated with each user. By building access policy around Identity, it is possible to tightly control and monitor what specific users are allowed to access when connected to a network. Employees, third parties, and ad hoc guests can all be granted fine grained access to just the resources they are entitled to use when permission is based on who they are, where they are, what device they are using, and more.

Caymas Access Gateways also support PKI authentication for government networks, single and reduced sign-on, and detailed, identity-based, logging and auditing for compliance.

**Caymas 220, Caymas 318 and Caymas 525 Specifications**

<b>DEPLOYMENT OPTIONS</b>
Remote Access SSL VPN
Remote Extranet
Guest Network Access Control
Network Admission
Departmental Firewall
IPSec VPN
<b>SUPPORTED PLATFORMS</b>
Windows XP (Home and Pro), Windows 2000, NT (SP 6)
Apple OSX (10.2, 10.3)
SUSE Linux 8.2
<b>SUPPORTED BROWSERS</b>
Microsoft Internet Explorer
Netscape
Mozilla Firefox
Apple Safari
<b>AUTHENTICATION</b>
Local, LDAP, Active Directory, RADIUS, X.509 Certificates with CRL support, RSA SecurID (Ace or RADIUS), User Defined Authentication methods can be combined for graded authentication
<b>AUTHORIZATION</b>
Local, LDAP and Active Directory
Security Zones adjusts authorizations based on authentication method, location and Host Integrity Checker scan result
<b>ENCRYPTION</b>
RSA, RC4, DES, 3DES, AES
MD5, SHA-1, IKE, TLS, IPSec
<b>RESOURCES PROTECTED</b>
<b>Web:</b> HTTP, Javascript, WebDAV, ActiveX
<b>File:</b> CIFS, NFS, DFS
<b>Mail:</b> IMAP, POP, SMTP, MAPI (Microsoft Exchange)
<b>Terminal Services:</b> Citrix, Windows Terminal Services, VNC
<b>Host Access:</b> Telnet, SSH (Internal and External), Mainframe Access (3270 and 5280)
<b>Client/Server:</b> All client/server applications, TCP/UDP static port and TCP/UDP dynamic port
<b>NETWORK PROTECTION</b>
Stateful layer 3/4 firewall
Network admission control
Trusted/Untrusted WLAN security

<b>ACCESS METHODS</b>
<b>Clientless</b>
<b>Secure Proxy:</b> HTTP, HTTPS, NFS, CIFS, DFS
<b>Thin Client</b>
<b>Web Relay:</b> Local proxy for Web applications - Java and VBScript compatibility
<b>WebDAV:</b> CIFS, DFS
<b>Secure Tunnel:</b> Thin client Java and ActiveX for client server applications
<b>Full Client</b>
<b>Secure Connect:</b> Network client for layer 3 access over SSL (Split Tunnel Control)
<b>IPSec:</b> Network Layer Access, Site to Site, Client to Site,
Unencrypted for internal LAN access
<b>THREAT PROTECTION</b>
Cookie Tampering, URL Tampering, Repeat Attacks (Password Cracking), SQL Injection/OS Command Injection, Web Attacks (SNORT Signatures), DoS Attacks, Protocol Anomaly Detection
<b>SINGLE SIGN-ON</b>
HTTP Basic authentication, Forms-based Web SSO, NTLM authentication, CIFS, DFS, NFS
<b>ADDITIONAL PROTECTION</b>
File Extension Restriction, HTTP Method Restriction, URL Canonicalization
<b>HOST INTEGRITY CHECKER</b>
AV engine, AV definitions, personal firewall, OS patches, registry entries, processes, open ports, file resent/absent with MD5 trojan horses, keystroke loggers
<b>INTEGRATED CACHE CLEANER</b>
Caymas 525/318/220
<b>LOGGING/REPORTING</b>
<b>Audit:</b> Source IP, userID, Group, Timestamp, Resource accessed (URL, Destination IP, Ports, Files accessed), Status, Bytes, Referrer, Authentication method, Logins/logouts
<b>Events:</b> Intrusion, Denied Resource Attempts, Security Alerts with SNMP Traps, Syslog, FTP or SCP Log Transfer, Custom Reporting
<b>NETWORK MANAGEMENT</b>
Caymas Management System (CMS), Command Line Interface, SNMP
<b>HARDWARE</b>
<b>Caymas 525</b>
4x10/100/1000bT LAN Ports
10/100bT Management Port
RJ-45 Serial Port for Direct Connectivity

Redundant Power Supplies	
<b>Caymas 318</b>	
2x10/100/1000bT LAN Ports	
RJ-45 Serial Port for Direct Connectivity	
<b>Caymas 220</b>	
2x10/100bT LAN Ports	
DB-9 Serial Port for Direct Connectivity	
<b>HIGH AVAILABILITY</b>	
<b>Caymas 525/318</b>	
Active/Standby Configuration	
<b>ENVIRONMENTAL</b>	
Input Voltage:	90-260VAC
Temperature (Operating):	0C to 50C
Temperature:	-30C to 60C
Humidity (Operating):	5% to 95% non-condensing
Humidity (Storage):	5% to 95% non-condensing
<b>CERTIFICATIONS</b>	
Safety	UL, CSA, EN60950
Emissions	FCC Class A
<b>PERFORMANCE</b>	
<b>Caymas 525</b>	
Concurrent Users	2,500
Overall Throughput	1 Gbps
Encrypted Throughput	1 Gbps
Deep Packet Inspection	10,000 ops/sec
IPSec Tunnels	2,500
SSL Connections	50,000
<b>Caymas 318</b>	
Concurrent Users	500
Overall Throughput	300 Mbps
Encrypted Throughput	300 Mbps
Deep Packet Inspection	1,000 ops/sec
IPSec Tunnels	500
SSL Connections	15,000
<b>Caymas 220</b>	
Concurrent Users	100
Overall Throughput	100 Mbps
Encrypted Throughput	100 Mbps
Deep Packet Inspection	100 ops/sec
IPSec Tunnels	-
SSL Connections	1,000



Caymas Systems, Inc.  
 Phone: 408.985.9000  
 Fax: 408.985.9001  
[www.caymassystems.com](http://www.caymassystems.com)

**Control Access. Control Your Business.**

Caymas Systems award winning Identity-Driven Access Gateways allow organizations to control access and control their business. Caymas offers the only access gateways that leverage the Identities of users, devices, and resources to connect the right user to the right resource every time, dramatically improving enterprise access control and security. Caymas delivers the only ASIC-based appliances that harness The Power of Identity™ to provide a universal access solution—a single platform for network admission and application access control, for both remote and internal users, with centralized access policy.