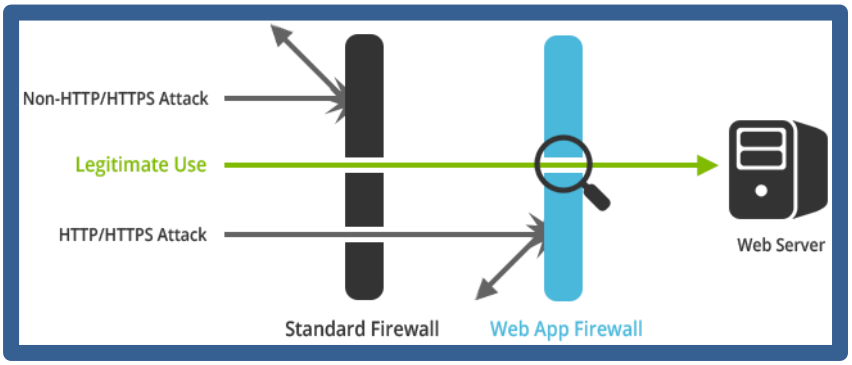
Web Application Protection

Add a level of protection to your **PrivateCloud™** by using CPN's **SecureCloud™** against threats and data loss that standard firewalls simply can't provide.



Features and Benefits

- **Application agnostic:** Instant protection without changing your web server code. Increase web server performance by offloading SSL (HTTPS).
- **Application firewall:** Process and intelligently modify all web server communication to identify and block hacking attempts. Stop intruders from manipulating your web content.
- **Malware scanning:** Dual antivirus engines scan your files and web content. Protect your web server from spreading viruses.
- **Detailed logging:** Reports of logged and analyzed transactions and attacks. Logs are required for clients seeking HIPAA and PCI compliance.

Main Security Features

- Deep packet inspection (protocol based)
- Server-based intrusion prevention (signature based)
- Server vulnerability mitigation (signature based)
- URL hardening engine
- Form hardening engine
- Deep-linking control (hot-linking)
- Directory traversal prevention
- SQL injection protection
- Cross-site scripting protection
- Dual antivirus engines
- HTTPS (SSL) encryption offloading
- Cookie signing with digital signatures
- Geographic IP blocking (by Country)
- Bad IP reputation blocking (black-list)

System Control and Logging Features

- Transaction activity logging
- Activity reporting and usage graphs
- Load balance visitors across multiple servers
- Site path routing directs specific paths on the site to desired server

SecureCloud™

Business data needs constant protection. CPN's **Securecloud™'** offers a full range of professional technical services, so your IT systems are safely up and running when you need them. By working proactively to resolve issues and threats, we mitigate problems before they affect your systems. Clients have the ability to establish policies that control their staff's usage and access to specific websites from their network.

Included Infrastructure Services

- Firewalling to block unauthorized third-party access to network
- Intrusion prevention to secure against malicious hacking attempts
- Application threat inspection to analyze software for exploits and vulnerabilities
- Network-based antivirus and malware protection to mitigate threats (ex. keyloggers, trojans, spyware)
- Web filtering with ability to restrict access to specific websites, content categories, and by individual users or groups of users.
- User activity reports available via automated email notification

Optional capabilities that may be added to this service include:

- SSL data inspection to protect against harmful activity within a secure connection
- Data loss prevention that can be programmed to protect personal data such as social security numbers, account numbers, or credit cards
- Web firewalling (WAF) to protect against unauthorized access to public accessible servers and websites

Note: In situations wherein remote support is determined to be impractical, Cloud Proven Networks will provide onsite support and this will billed at an hourly rate.

Fee-based Services

- On-site support billed at an hourly rate to cover trip charges and on-site work completed
- Design and implementation projects
- End user operating issues, end user computing issues, end user device support
- Application specific problems requiring support
- Domain/Active Directory issues
- Consulting services which require changes to infrastructure will be quoted separately

Client Responsibilities

To familiarize Cloud Proven Networks' Engineers with the client's environment, the following information is needed:

- Documentation of network architecture
- Inventory of servers, server function, hardware specifications, and software applications
- Service and connectivity contracts
- List of supported applications
- Ongoing updates of any changes to the IT infrastructure

To learn more about Cloud Proven Networks' SecureCloud™, contact sales@cloudproven.net or (877) 790-HOST(4678).