

Web Policy Enforcement Services

CGI's MSS Web Policy Enforcement service allows organizations to monitor Internet usage and optionally block requests that violate Corporate Policy. The policies supported by this service are extremely flexible and are easily and quickly configurable. The Web Policy Enforcement service allows government IT to monitor and enforce an Acceptable Use Policy (AUP) for employees accessing the Internet via the Web. In addition, based on the AUP in place, you can filter and report on the five major risk classes and over 90 major categories of Internet Web sites and protocols.

CGI's web policy enforcement solution monitors all web traffic. Based on predefined policies and network configuration, activity may be logged and/or blocked. Summary as well as granular detailed reports representing the monitored and blocked network activity can be provided. This service integrates seamlessly with leading network infrastructure solutions to offer unequalled flexibility and control.

Basic Services

- Enforces acceptable use policy
- Provides optional leak detection service
- Provides extensive category and protocol sets
- Provides automatic generation of management reports
- Allows the ability to issue ad hoc reports at any level of granularity
- Assists in investigative support including providing evidence for legal council

Optional Service Components

- Acceptable Use Policy Enforcement
 - Allows Blocking for categories and protocols that violate policy
 - Management of multiple policies
 - Issues a client defined custom message to user indicating that a policy violation has occurred
 - Bilingual, "More Info" link
 - Integrates with a client's Active Directory to allow more granular policy enforcement and reporting
 - Ability to provide password override to allow access to specific classes of sites for select number of users
- Real Time Detailed Reporting
 - Allows a client's Security Officer or other client authorized personnel to run ad hoc reports
 - Reports can be batch oriented or run in real-time
 - Runs on dedicated hardware to minimize performance issues to policy enforcement service
- Instant Messaging Policy Enforcement
 - Policy can allow or deny service by group
 - Policy can allow or disallow Instant Messaging attachments
- Protocol Policy Enforcement
 - Specific protocols can be allowed or denied by group (examples include: FTP, Kazaa, Bit Torrent, Skype)

Benefits

CGI's experience will help government to streamline and define a WPE workflow with actionable items. Then, CGI manages the WPE to manage the AUP and reduce web-based risks to the organization. Through the CGI Web Policy Enforcement Solution your organization will:

- Mitigate legal liability
- Realize staff cost savings
- Manage the risk of Internet use
- Receive 24x7 coverage through the MSS SOC