WebSense

1.0 Purpose

WebSense web security gateway provides layered threat protection against modern Web threats. WebSense provides real-time security scanning and content classification for all outbound web traffic including dynamic Web 2.0 content. This layered protection helps to prevent such web threats as malware, surf-by infections, and fake anti-virus in addition to what client protection can provide.

2.0 Scope

Web content is monitored and classified by WebSense Security Labs and their ThreatSeeker technology. WebSense is a world leader in web security solutions, and offers an inline approach that delivers real-time reputation analysis and expanded behavioral analysis to provide us with the most accurate protection against malicious threats. This network includes 50 million real-time data collecting systems that scan 40 million+ Web sites per hour for malicious activity on more than 2 million domains. More than 100 million Web sites are analyzed daily as well as 10 million spam, phishing or exploit campaigns.

3.0 Policies

Current policies for protection are as follows and are broken down by groups.

- All devices, groups and users are filtered from the following categories
  - Elevated exposure
  - Emerging Exploits
  - Potentially Damaging
  - Bot Networks
  - Key loggers
  - Malicious Web Sites
  - Phishing and/or Fraud
  - Spyware
  - Peer-to-Peer
  - Proxy Avoidance
  - Hacking
  - Web and Email Spam
  - Pay-to-Surf
- All devices, groups and users are filtered from the following protocols
  - Brosix
  - Chikka
  - Globe 7
WebSense

- Goober
- iSpQ
- Mail.RU
- netFM
- Palringo
- Bot
- Im file attachment
- All P2P
- All Proxy

If you are filtered from a site you will receive a web browser message similar to the one below. If you do not receive a content blocked message inability to access web content is caused by another factor. Please submit a Customer care ticket so that a technician can troubleshoot what may be happening.

*Exceptions for sites in these categories or protocols will not be made.*

- **Employee (non faculty), Public access wireless clients, Community patrons, Wired network devices not meeting other group requirements** are filtered from the following categories:
  - Adult Content
  - Nudity
  - Sex
WebSense

- Gambling

Exceptions to these categories can be requested through Customer Care. Please submit a ticket request with the site(s) that need to be accessed along with documentation including the business case for access.

- Faculty are given the option to ‘CONTINUE’ to the following categories for educational purposes.
  - Adult Content
  - Nudity
  - Sex
  - Gambling

A web browser message will appear similar to the following. Clicking the CONTINUE button highlighted below will allow access to the site.