Web Content Filtering

Web Content Filtering

What is Web Content Filtering (WCF)?

- A classification system for filtered access to web pages
  - Only pages matching the allowed categories are displayed

Web Content Filtering

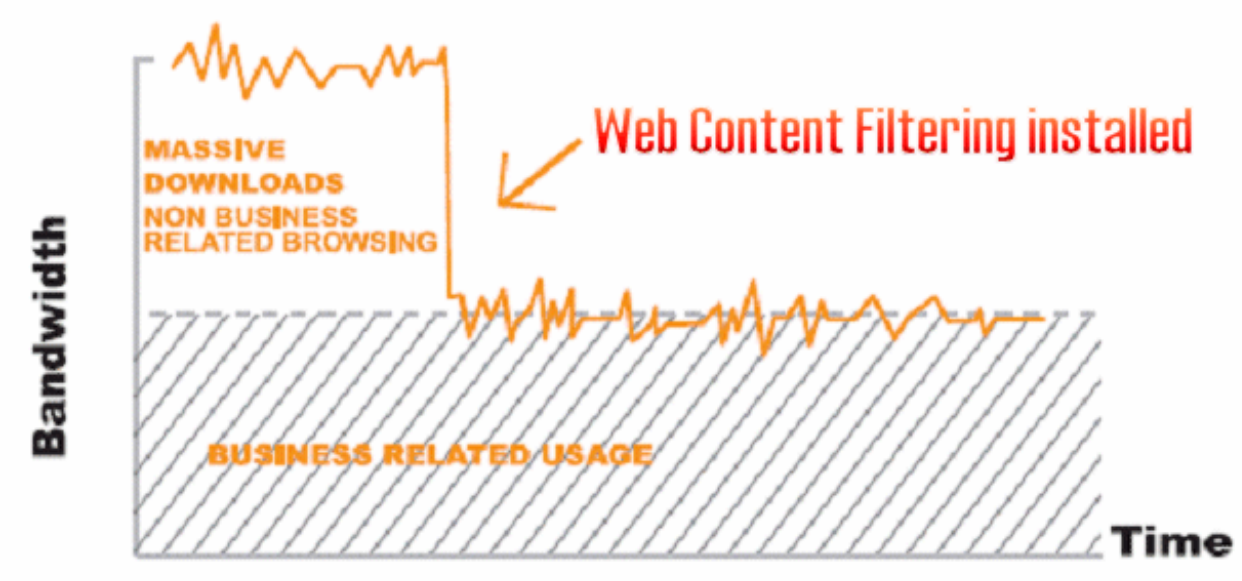
Why Web Content Filtering (WCF)?

- Conservation of bandwidth
- Less malware from web browser exploit pages
- Less joysurfing during working hours
- Legal requirements
- Company bad-will if employees surf to illegal/inappropriate pages
- Can block active content
  - ActiveX, Flash, Java Applets, Javascript, VBScript, Cookies etc
- Can block advertisements, sites-in-sites, malware responses etc
- Logging of user behaviour (URLs visited)
- Save time and money!

Web Content Filtering

Save time and money!

- Saves bandwidth
- Reduces wasted staff time
  - 1 hour/day * 50 employees *£€$ 30/hour * 240 days/year = £€$ 360 000/year



Web Content Filtering

Categorization

- URLs classified by AI system under human control
  - Collect
    - Web spider / crawler
    - Reported unclassified pages from SeGWs
  - Analyse
  - Categorise
  - Edit / Reclassify
  - Distribute
- Reclassification is possible by authorized users
  - Compressed and encrypted traffic
  - Anonymously submitted
  - Manual review at datacenter
  - Classification list correction
  - Distribution to SeGWs in the field

Web Content Filtering

Clavister HTTP ALG

- Filtering in real-time
  - Poll CSPN when a non-cached site discovered
    - Locally discovered URLs uploaded
    - Updates downloaded
  - 2-8 hours from discovery of URL to filtering
  - Reclassification can take more time (manual control)
- Communication with CSPN
  - Automatic update and failure handling
  - Compressed and encrypted traffic
  - Anonymously submitted URLs

Web Content Filtering

HTTP Filtering Policies

- Filtering policies can be applied on
  - Users
  - Groups
  - Networks
  - IP-addresses
- Policies based on
  - Category settings
  - Custom URL settings
    - Whitelist
    - Blacklist
    - Active Content blocking
  - Time of day
- Blocking
  - Coaching (warning) page informs user why page is blocked
  - Coaching pages fully customizable (HTML)

Web Content Filtering

HTTP Filtering Policies

- Classification of web pages
  - One site might have several classes
  - To allow the site, all classes must be allowed

Web Content Filtering

Tips for deployment at a site

- First allow all categories, audit the traffic
- Slowly activate one blocked category after another
  - A few days between each
  - Don't irritate all users at once
  - Slowly make users understand what's happening
  - Don't overload the admin with huge logs / e-mail from users

Web Content Filtering

Custom HTTP Pages

- To create custom HTTP pages, select SeGW in manager > Properties > Options Enter HTTP ALG Root Directory.
- Action > Communication > Upload > HTTP ALG HTML Files
  - Will upload the pages to the SeGW
- In the ALG, select the subdirectory with the http pages.

Web Content Filtering

HTTP Filtering Problems

- Some web pages get distorted by the HTTP ALG needed for WCF to work
  - CorePlus updates
  - Contact with web master
- PHP-scripts etc for document download get blocked if they don't use HTTP protocol on port 80 (HTTP ALG)
- Uncategorized pages get blocked until they are categorized
  - Don't block "unknown" pages or...
  - Run in Audit mode long enough to let most of the pages be categorized
- Can't click "continue" in small frames linking to other servers
  - Allow override enabled
  - *Create new HTML coaching pages*
- Not all user groups can tolerate it
  - Home users: "censorship"

Web Content Filtering

Summary

- Policy based filtering of web page access
  - Real-time filtering
  - A.I. plus Human managed categorization database
  - Override possible
  - Recategorization possible
  - URL categories distributed via CSPN

How to implement WCF?

Hands-On Exercise: Web Content Filtering

- **Objectives**
  - Setup Web Content Filtering and test that it works according to policies
- **What to do**
  - Decide filtering policies
  - Setup HTTP_ALG according to the filtering policies
  - Service using the HTTP_ALG
  - Rules using the Service
  - Verify that the filtering works according to the policies
- **What you should know afterwards**
  - How to set up WCF

Hands-On Exercise: Web Content Filtering

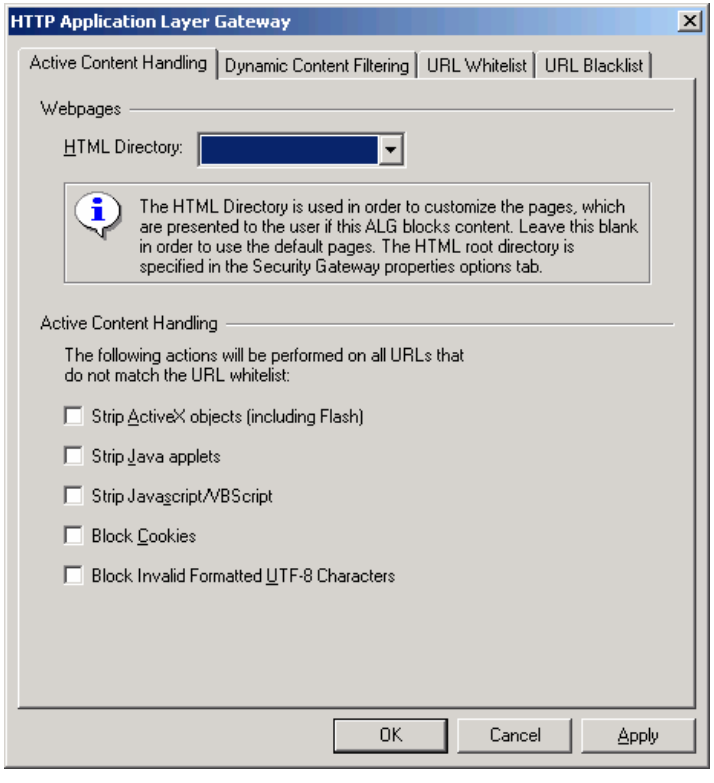
Installing Web Content Filtering

- Overview
  - Create an ALG with the desired policies
  - Create a Service using the ALG
  - Create a Rule using the Service
  - Test the settings by surfing

Hands-On Exercise: Web Content Filtering

ALG > HTTP Application Layer Gateway

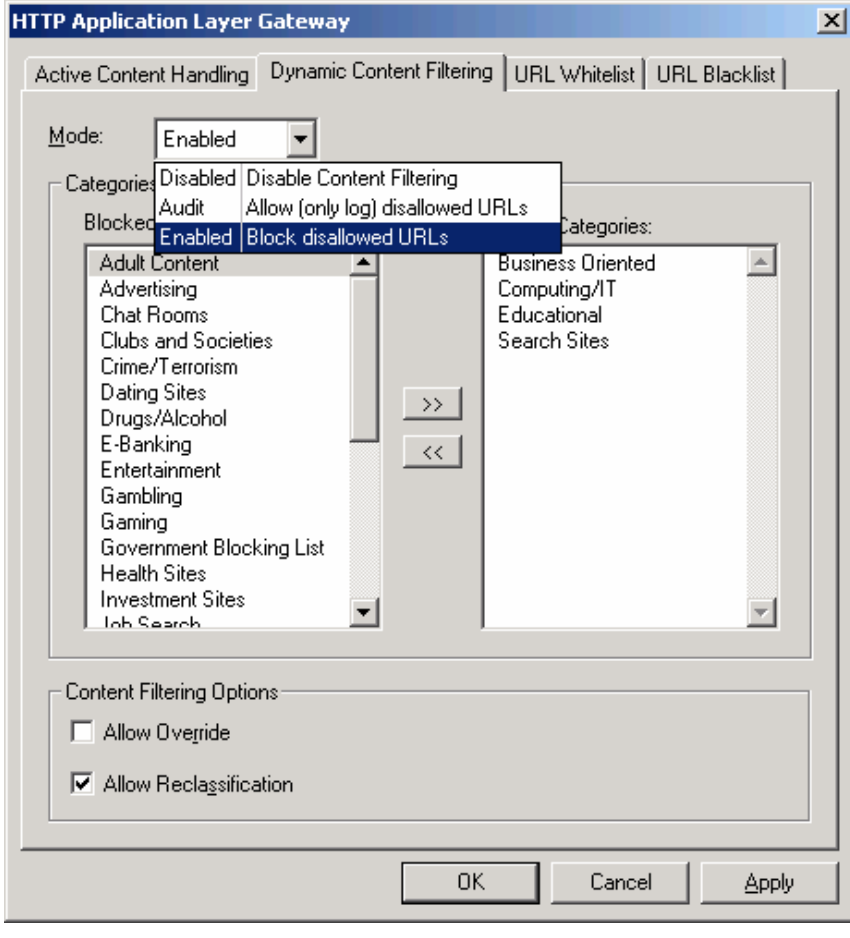
- About ALGs
  - HTML > Properties
- Active Content Handling tab
  - HTML Directory
    - Customized HTML pages
  - Strip
    - ActiveX objects
    - Java Applets
    - Java Script/VB Script
  - Block
    - Cookies
    - Invalidly formatted UTF-8 characters
- *Some web pages may cease to work when blocking / stripping Active Content*



Hands-On Exercise: Web Content Filtering

ALG > HTTP Application Layer Gateway

- Dynamic Content Filtering tab
  - 31 standard categories
    - Audit
    - Block
  - Override
    - Gives user option to continue
  - Reclassification
    - Option to send suggestion of new classification

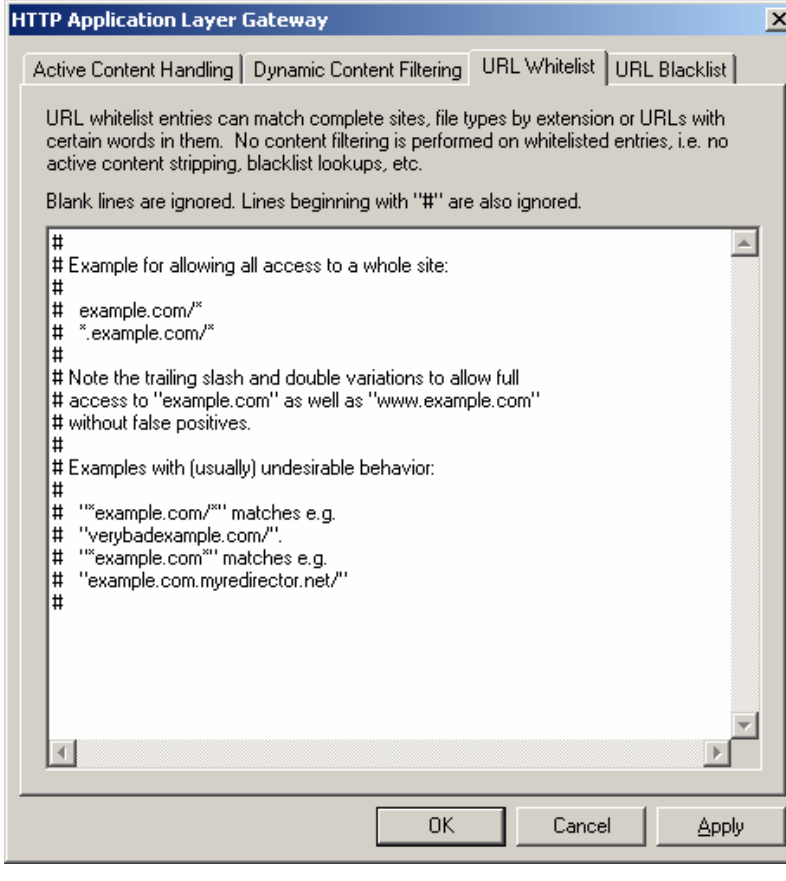


THE SECURITY SERVICE PLATFORM TECHIES LOVE

Hands-On Exercise: Web Content Filtering

ALG > HTTP Application Layer Gateway

- Static Content Filtering
  URL White/Blacklist tabs
  - URL Whitelist
    - Always allowed
    - www.clavister.com/*
    - *.site.com fooled by this: www.badpage.com?.site.com
  - URL Blacklist
    - Forbidden site(s)
    - * = all are forbidded, except those whitelisted



Hands-On Exercise: Web Content Filtering

Web Content Filtering

- Create an HTTP ALG
  - Local Objects > Application Layer Gateways
    - Name: `HTTP_ALG`
    - Type: `HTTP`
    - Parameters > Dynamic Content Filtering:
      - `Enabled`
      - Add Allowed Categories:
        - » `Business oriented`
        - » `Search sites`
        - » `Educational`
        - » `Advertising`

Hands-On Exercise: Web Content Filtering

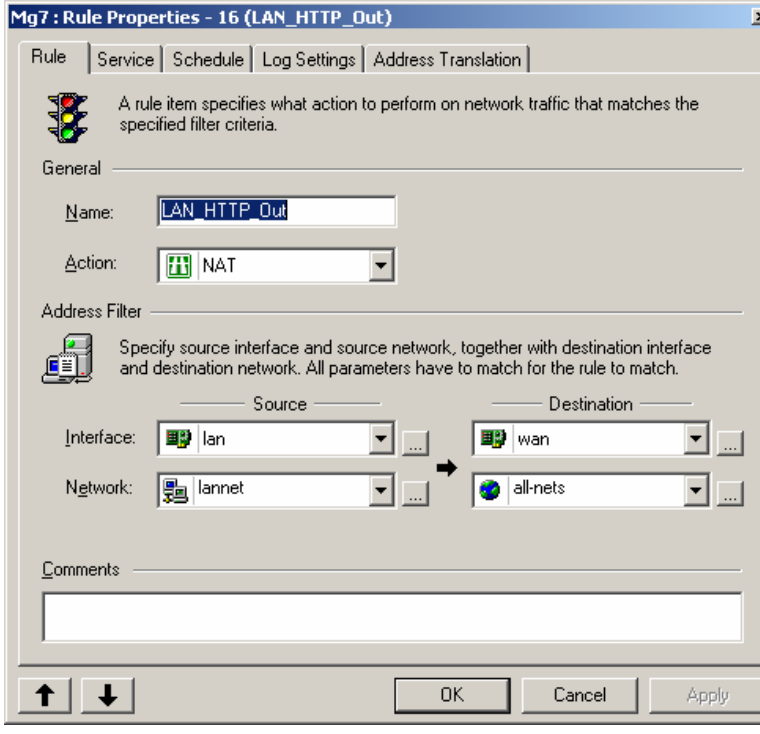
Web Content Filtering

- Create a Service using the HTTP ALG
  - Local Objects > Services
    - Name: `HTTP_Business`
    - Type: `TCP`
    - ALG: HTTP_ALG (created above)
    - > TCP/UDP Parameters > Destination port: `80`

Hands-On Exercise: Web Content Filtering

Rules

- Create a NAT rule using the service created
  - `LAN_HTTP_Out NAT lan lannet wan all-nets HTTP_Business`
- Now it should filter web access for users at the lannet!



Hands-On Exercise: Web Content Filtering

- Try by surfing to a few random sites:
  - http://www.google.com
    - Allowed
      - Search sites (+ Educational?)
  - http://www.cnn.com
    - Blocked
      - News
  - http://www.slashdot.org
    - Blocked
      - News, Entertainment, Sports, Computing/IT

Hands-On Exercise: Web Content Filtering

Hints and tips

- Verify that the Security Gateway has access to the global network with HTTP, ICMP Ping, DNS and TCP:9998
- Create the ALG, the Service and the Rules
- White lists and Black lists can be utilized
- All classifications a page has must be allowed before it is allowed
- Allow Reclassification and Allow Override can be used in some scenarios
- Audit mode can be used during a trial period at a customer site
  - Logs will show user behavior
  - Pages have time to be categorized