



managed content filtering network protection for evolving security threats

managing Internet privileges

While organizations today provide Internet access to their employees as a means to improve productivity, the reality is that some employees abuse their Internet privileges. Companies have tended to address the legal liability and consumption of network bandwidth associated with this abuse primarily by blocking sites.

But this approach is not effective because browser content is not the sole source of legal liability and bandwidth consumption. The majority of Internet abuse occurs via desktop applications such as instant messaging, email, email attachments, and peer-to-peer applications.

For most organizations, the challenges are not limited to inappropriate use of company computers for entertainment and shopping. The misuse of confidential company data and co-worker harassment creates an even broader and more complex organizational security problem.

TELUS has developed a comprehensive, fully integrated solution to this problem. TELUS Managed Content Filtering proactively monitors, blocks and reports any undesirable content. This includes spyware, malicious mobile code, instant messaging, streaming media, and social engineering attacks such as phishing sites.

protect your network; increase productivity

TELUS Managed Content Filtering combines powerful flexibility with rich functionality. Our solution ensures consistent results by:

Providing comprehensive and accurate content filtering. TELUS Managed Content Filtering uses a combination of automated and human classification, and is dynamically tuned to real-life surfing patterns. It is supported by a master database containing over 10 million Web sites, published in 50+ languages and organized into more than 90 categories including gambling, adult content, hacking and gaming.

Balancing work-related and personal surfing. Administrators and policy setters are able to create custom policies for employee Internet use. Policies can control what sites are visited, for how long and at what time of day.

Creating customized block pages. When employees attempt to access the Internet, TELUS Managed Content Filtering intercepts the request at the gateway and enforces your company's acceptable Internet use policy. We verify that content is allowed to be downloaded from the requested URL. If blocked, the employee is redirected to a customized block page.

Monitoring 24x7. TELUS Managed Content Filtering provides around-the-clock monitoring and support. It eliminates the need to hire and train specialized security resources and personnel. TELUS provides online, real-time and historical reporting to keep your IT managers informed and in control.

stop Internet abuse

TELUS Managed Content Filtering is fully integrated solution to Internet abuse.

Protect your network against:

- Spyware
- Phishing
- Malicious mobile code
- Hacking

Increase productivity by monitoring:

- Employee Web browsing
- Instant messaging
- Peer-to-peer file sharing
- Streaming media
- Internet radio and TV

managed content filtering

take control

With TELUS Managed Content Filtering, your organization can create policies that control:

- Time spent Web surfing
- Web sites visited
- Time of day certain sites can be viewed
- How long employees are able to view particular sites

flexible reporting

TELUS delivers online interactive reports with real-time and historical views of business risks related to employee usage. You can then use this information to refine Internet use policies, which effectively reduces the associated risks. Key benefits include:

- **Real-time reporting.** View network activity using live data via a Web browser from any PC on the network.
- **Interactive, point and click.** Minimize the limitations of predefined reporting. Allow your HR or IT managers to generate their own reports.
- **Statistical analysis.** View those individuals with the most liberal Web usage or identify problem areas – from high-level risk to specific protocols.
- **User friendly.** Our click-through approach is designed for non-technical users.

service levels

TELUS Managed Content Filtering delivers:

- Service availability of devices: 99.9% (in HA configuration)
- Notification of critical events: 15 minutes
- Signature updates: every 4 hours
- Average time for non-critical configuration changes: 4 hours

premium package

If your business requires additional functionality, TELUS offers a Premium Web Security Suite. It adds an extra layer of security to your network by preventing employees from unknowingly downloading or accessing phishing sites, key-logging software, malicious mobile code and spyware.

ldap and active directory integration

If your business requires individual-level monitoring, policy enforcement and reporting (beyond simple IP-address), TELUS offers ldap and active directory integrations.

comprehensive product coverage

TELUS Managed Content Filtering integrates with most versions of security products from the following manufacturers:

- 3Comm
- Checkpoint
- Cisco
- Cyberguard
- Dell
- Hewlett-Packard
- Juniper Networks
- Lightspeed
- Microsoft
- NetScreen
- Nokia
- Novell Volera
- SonicWALL
- Sun Microsystems