

# Web Filtering as a Critical Security Service

## **Monitor, Control, and Block Unwanted Traffic**

Web filtering continues to gain momentum as a key technology to combat cyber threats and provide a safe cyber environment, especially for children. As the variety of devices accessing the internet grows, and the complexity of client-side solutions grows exponentially, individuals and enterprises alike are finding it increasingly difficult to achieve a 'safe internet' experience. As a result, service providers are discovering web filtering solutions to help mitigate these cyber security challenges. Furthermore, in many cases, government mandates require carriers to provide safe internet alternatives.

# **Accurate and Cost-Effective Web Filtering**

The Cyber NetControl solution from ISC8 is a carrier-grade system enabling granular web filtering and traffic enforcement on a per-protocol and per-user basis, all without requiring interaction with external devices.

Cyber NetControl employs technology that permits transparent and accurate enforcement of site accessibility without modifying general DNS server infrastructure configurations, thereby adding an extra layer of protection from illicit hackers. Cyber NetControl is an easy-to-deploy solution that avoids the complexity of more expensive and less-effective proxy gateways.

[secure]®



# ISC8's Cyber NetControl solution offers:

- Reliable Safe Internet Services with 100% Inspection of All Network Traffic
- **Full Filtering on a Per-User Basis**
- Highly Accurate URL Filtering
- Easy to Install and Easy to Manage
- **Real-Time Security**
- Strong Policy Enforcement
- Self-Directed Policy Configuration
- Cost-Effective Solutions to Complement Current Security Infrastructure

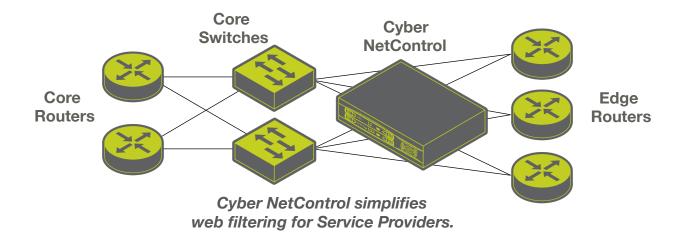


CyberSecurity@isc8.com

© Copyright 2013 ISC8

All Rights Reserved

### ISC8 Cyber NetControl™



# Accurate Web Filtering as a Critical Security Service

Service providers recognize that web filtering is a critical service. Whether serving families and individuals that are seeking a safe internet experience, or instead serving enterprise organizations that seek to enforce their internet usage policy, service providers understand that these security services help differentiate services in a very crowded market.

### **Avoid Costly Challenges**

Service providers ready to deploy a carrierready web filtering solution from ISC8 can avoid many costly challenges, including:

- □ Significant network redesign required in order to provide the service
- ☐ Enterprise-style per-user licensing fees that make service provider solutions extraordinarily expensive
- Proxy-based solutions that leave gaps in coverage

## **Granular Filtering: Per-Protocol, Per-Flow, and Per-User**

An innovative deep packet inspection (DPI) engine resides at the core of the system, enabling complex processing at very high networking speeds with unlimited flexibility. This results in granular web filtering on a per-protocol, per-flow, and per-user basis, all without requiring interaction with external devices. In addition, the engine provides auto-discovery of user-authentication protocols, which greatly simplifies the deployment and management of the system.

### **The Best Solution for Web Filtering**

Completely self-contained and capable of operating transparently inline, Cyber NetControl can be deployed at any location, such as a data center, internet gateway, or point of presence (POP).

The Cyber NetControl system delivers the best web filtering control and traffic enforcement to protect and optimize fixed and mobile network communications infrastructure.

[secure] 
[secure]

ISC8