



Cisco IOS[®] Content Filtering



April 2008

www.cisco.com/go/ioscontentfiltering

Improving Employee Productivity

Up to **2% of Revenue Losses** and **51% of Downtime Costs** Are Due to Security Problems



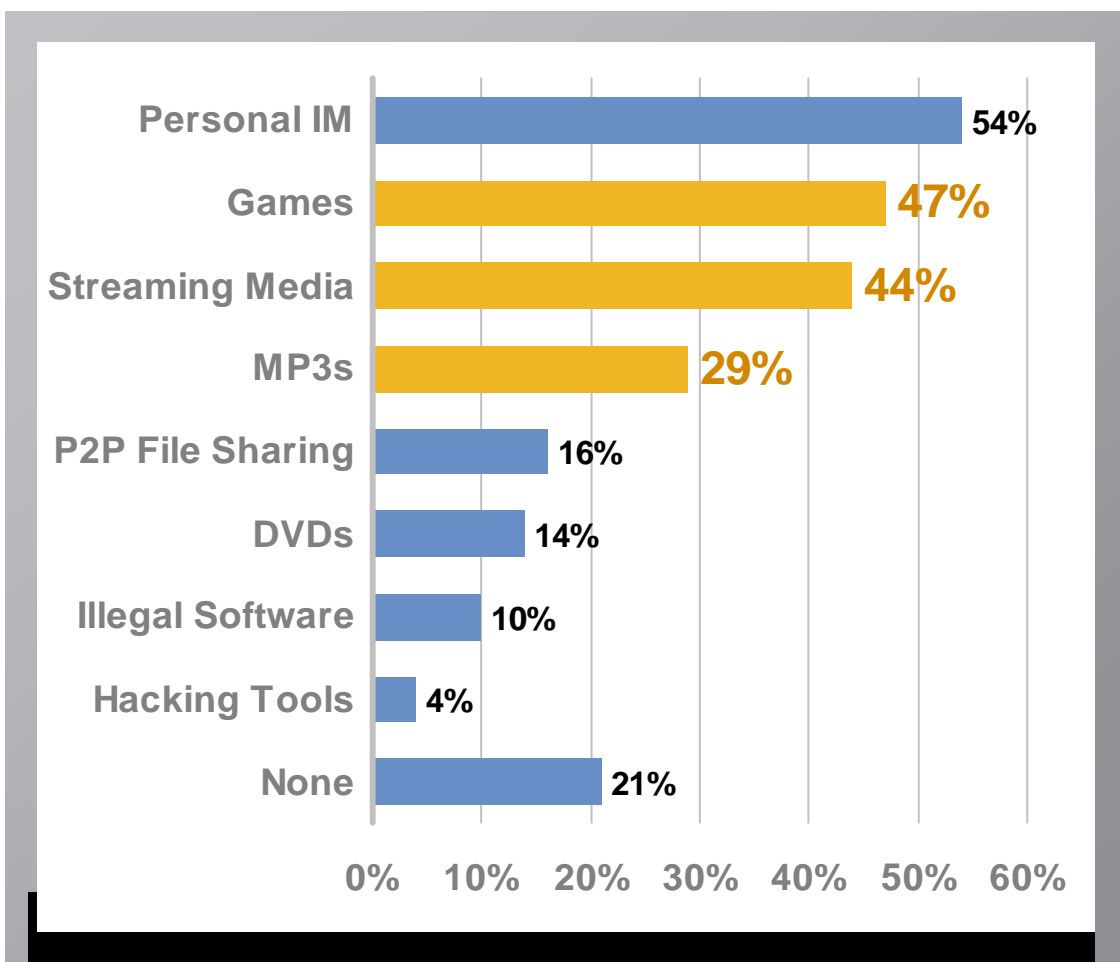
- Nearly 50% of user downtime due to spyware alone*
 - Each system crash: 15 minutes
 - Multiple crashes per day per infection
 - Incalculable information loss or damage



- Upwards of 25% of IT support time spent on preventable infections**
 - Average support call: 1 hour
 - Cost per hour: \$75

Sources: *Infonetics Research and **Cisco customer survey

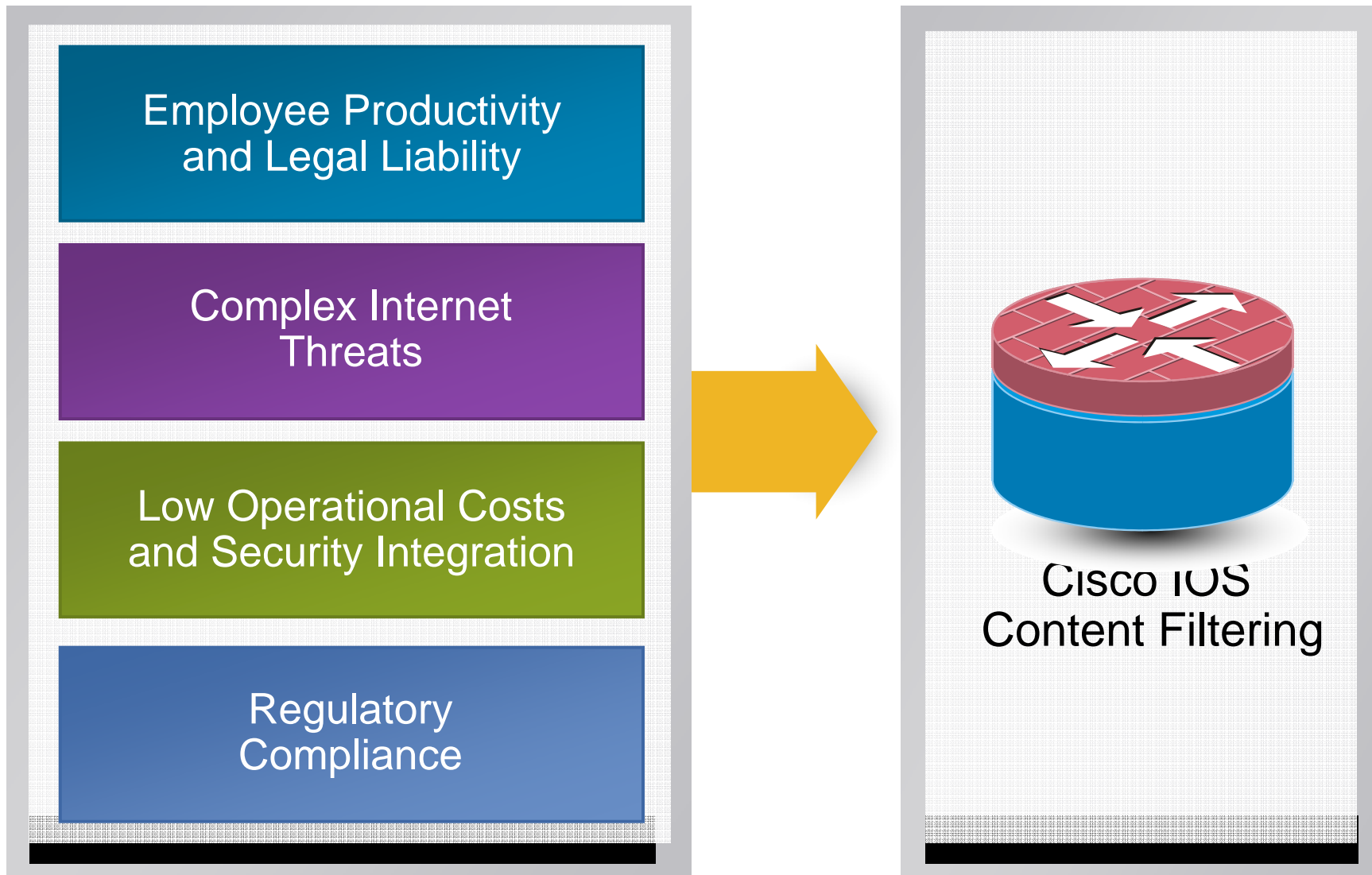
Add the Human Factor: Innocent Accomplice



- 30% to 40% of employee Internet use is not work related*
- 55% of online users have been infected with spyware*
- A typical 25-employee company can lose over \$150K annually in lost productivity from Internet misuse

*International Data Corporation, Consumer Affairs, Bigfoot Interactive, Gartner

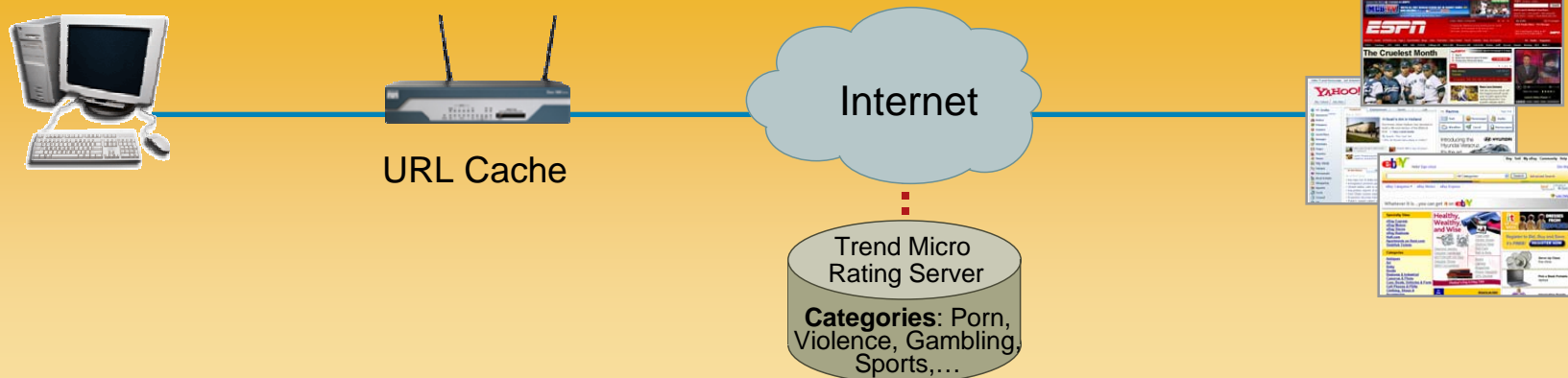
The Need for Cisco IOS Content Filtering



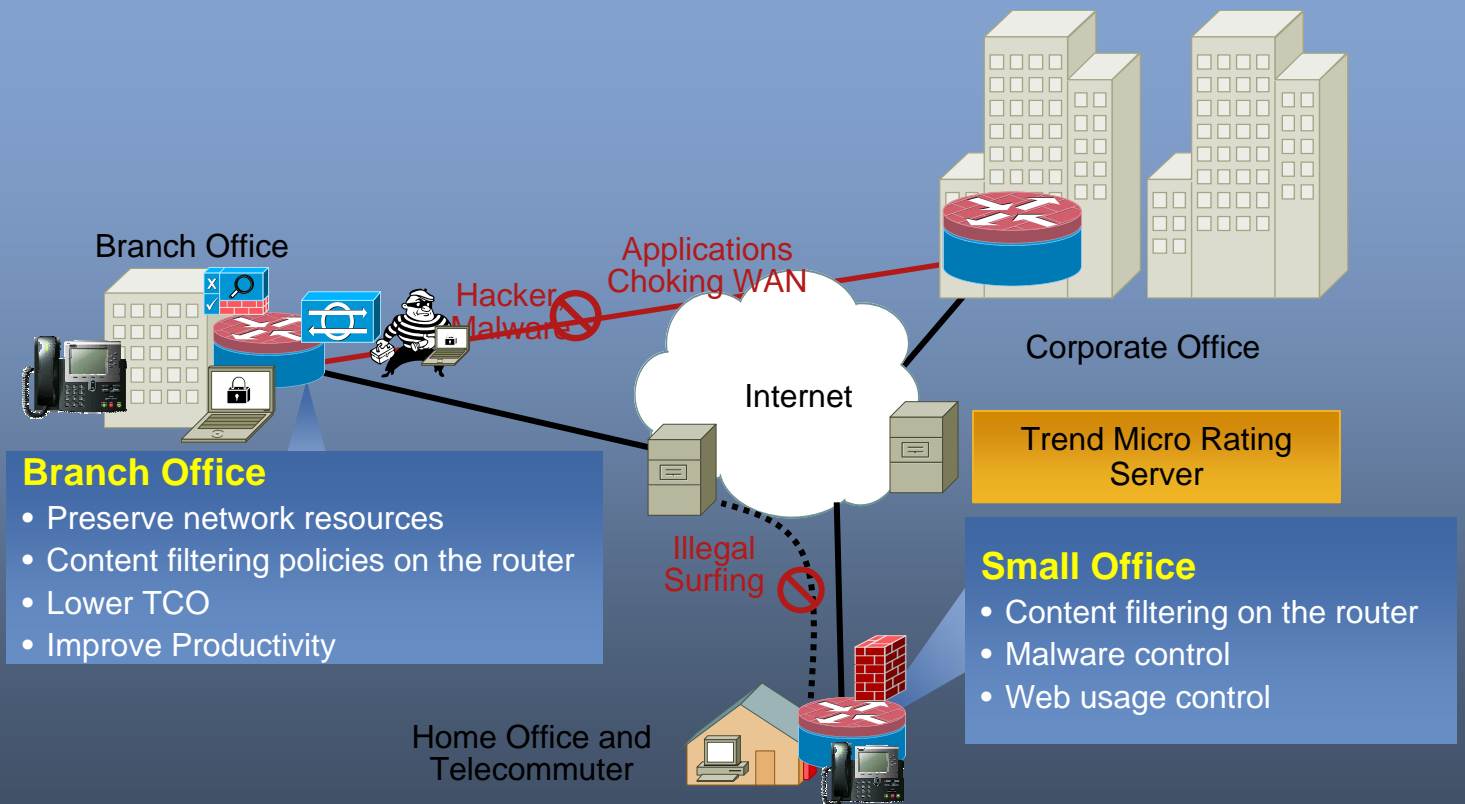
Cisco IOS[®] Content Filtering with Trend Micro

A Web Security Solution That Protects Organizations from Known and New Internet Threats, While Improving Employee Productivity

- Ideal for Enterprise Branch and Small-Medium Businesses
- Block malicious sites and enforce corporate policies
- Offers category based security and productivity ratings
- Regulations such as HIPAA, FISMA, CIPA (Children's Internet Protection Act) mandate reliable content filtering.
- Policy is enforced and maintained on the router locally



Deployment Scenarios and Benefits



- Secure internet access to branch, without the need for additional devices
- Control spyware and malware right at the remote site; conserve WAN bandwidth
- Improve employee productivity and protect network resources by enabling content filtering

Comprehensive Content Filtering Features

Feature

Benefit

- Security Ratings
Adware, phishing,
spyware, hacking

- **Block malware**; use security rating of a Website to prevent malware downloaded by the end users

- Category-based URL classification
Over 70 categories available

- **Block unwanted Web activity**; enforce access to both objectionable and productivity affecting Websites

- Keyword blocking

- Localized filtering on Cisco[®] router allows blocking of Websites based on keywords

- Black and White List support

- Support for 100 Black and 100 White Lists in Cisco IOS[®]

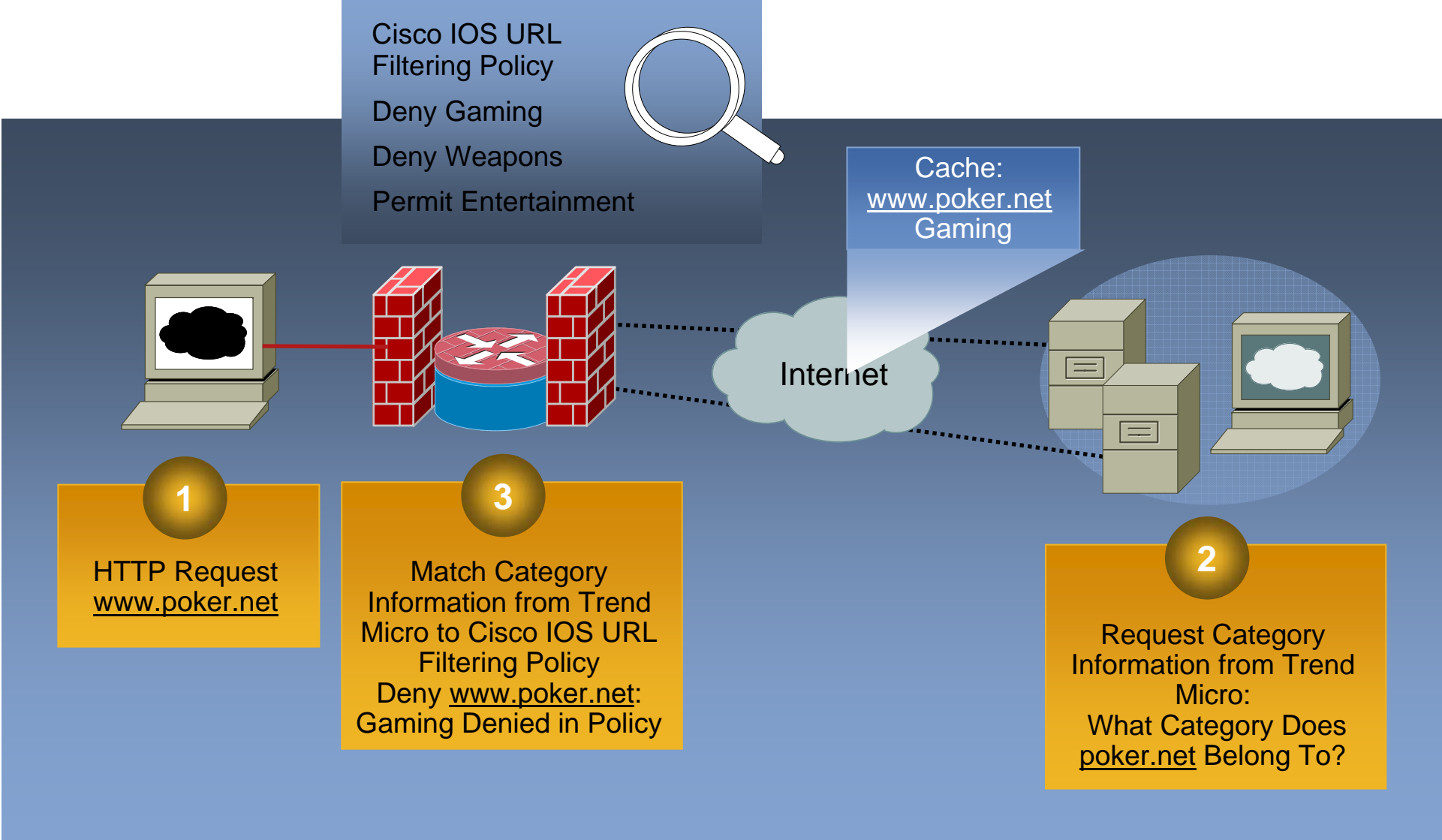
Cisco IOS® Content Filtering Management: Cisco® Configuration Professional

The image displays two overlapping windows from the Cisco Configuration Professional Firewall Wizard. The background window is titled "URL Filter Server Configuration" and contains the following text: "Please specify the URLs that has to be allowed or blocked without connecting to the URL Filter vendor server." It features three input fields: "Enter the keywords in the URL that has to be blocked", "(Use comma to separate multiple)", "Enter the URLs that has to be blocked", and "Enter the URLs that to be allowed". The foreground window is titled "URL Filter Category Selection" and contains the following text: "Select the category and action for the web request for the website in the category. Selecting SDM default profiles automatically selects the categories as per the profile selected. You can select None to select your own categories." It includes radio buttons for "Default Category" (selected) and "Custom Category", and a dropdown menu for "SDM Default Profiles" set to "School". Below this is a table with columns for Category, Description, and Action.

	Category	Description	Action
<input checked="" type="checkbox"/>	Abortion		Allow
<input type="checkbox"/>	Adult-Content		Deny
<input checked="" type="checkbox"/>	Alcohol		Deny
<input checked="" type="checkbox"/>	Arts		Allow
<input type="checkbox"/>	Auctions		Deny
<input checked="" type="checkbox"/>	Blogs		Deny
<input checked="" type="checkbox"/>	Brokerage		Allow
<input checked="" type="checkbox"/>	Business		Allow
<input type="checkbox"/>	Chat		Deny
<input checked="" type="checkbox"/>	Computers-internet		Deny

Navigation buttons at the bottom: < Back, Next >, Finish, Cancel, Help.

Cisco IOS Content Filtering Subscription Service Architecture



Feature Details

- **Flexible Configuration**

- Category and URL (productivity or security) is cached
- Default cache size 300 Kbytes -> ~100 URLs
- Cache is flushed upon reboot
- Default cache lifetime – 24 hours

- **High Availability**

- Trend Micro server information is entered into router CLI by DNS, enabling easy failover between Trend Micro servers if one is unreachable

- **Ease of Use**

- Trend Micro maintains and updates the security and productivity database so no local database is required on the router
- Router Registration and Configuration through Cisco Configuration Professional®
- Local filtering in IOS by black and white lists
- Support for partial domain names
- IOS Image 12.4(15)XZ for fixed platforms, modular platforms – 12.4(20)T

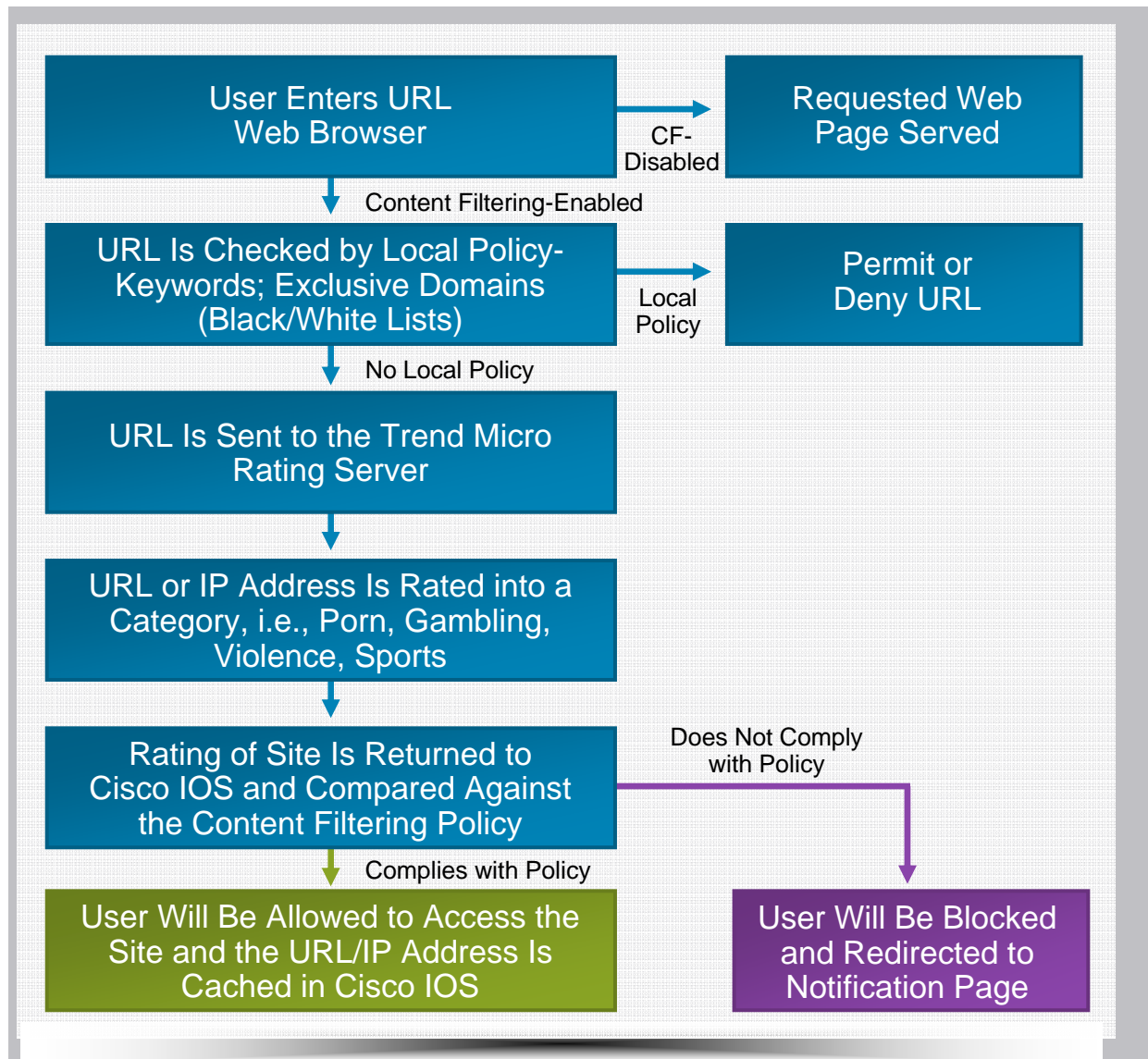
License Activation

- Upon SKU purchase, customer receives PAK (product activation key) by e-mail.
- Customer enters PAK, product ID, and router serial number at the licensing portal on www.cisco.com/go/license.
- If credentials match, appropriate license is activated, and customer receives an e-mail message to confirm.
- Renewal notifications are sent by router as license nears expiration.
- 30-day grace period available after license expires.

Feature Configuration

- Customers can enter the router's public IP address and download a security certificate. The public IP address is entered at http://www.cisco.com/en/US/products/ps5854/products_configuration_example09186a0080816c23.shtml
- Certificate is used to communicate with the Trend Micro Rating Server.
- Customer can then follow easy, intuitive steps to configure Cisco IOS® content filtering using Cisco Configuration Professional or through the command-line interface (CLI).
- More details at www.cisco.com/go/ioscontentfiltering

Content Filtering Service Flow



Cisco Services and Support

Cisco and its partners provide a broad portfolio of security services that help you to:

- **Protect privacy and integrity of information**
- **Achieve and maintain regulatory compliance,**
- **Protect your network investment,**
- **Optimize network operations, and**
- **Extend the power of your business by preparing your network for new applications**

For more information, visit

http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html .

