Transition Guide

Use this paper to help make the transition from SurfControl Web Filter to Websense Web Security or Websense Web Security Gateway.

- Learn about the differences between the SurfControl and Websense security models.
- Access information and worksheets to help you plan the transition.
- Learn about other resources that can step you through the process of implementing a Websense Web Security solution.

Understanding the Websense Web Security model

Both SurfControl Web Filter and Websense Web Security solutions are designed to help protect you from Internet security risks and help you control access to Internet resources, but the tools use very different models to achieve those results.

The SurfControl world:

SurfControl Web Filter uses a rules-based model.

- Rules either allow or disallow access to users (Who) for places (Where) and protocols (What) at specified times (When).
- Rules processing is top down. Processing stops when the first applicable rule is found.

The Websense world:

Websense Web Security solutions uses a client-centered, policy-based model.

- Websense software identifies the client (user or IP address) making a request, and then applies a policy to the request.
- Only one policy can apply to an individual client at any given time.
- Each policy is made up of a **schedule** and comprehensive enforcement settings (applied to categories and protocols) for each time period in the schedule.

Transition Axiom 1: Know your clients

To prepare for a smooth transition to Websense Web Security solutions, start by identifying your clients and organizing them by shared Internet access requirements or restrictions. Clients may be:

- IP addresses or IP address ranges

  These client types are called **computers** and **networks**, respectively.
- Users, groups, or domains and OUs in a directory service

  These client types are referred to collectively as **directory** clients.

It is a good idea to create a hierarchical organization of clients. This organization may already exist as part of your IT infrastructure design.

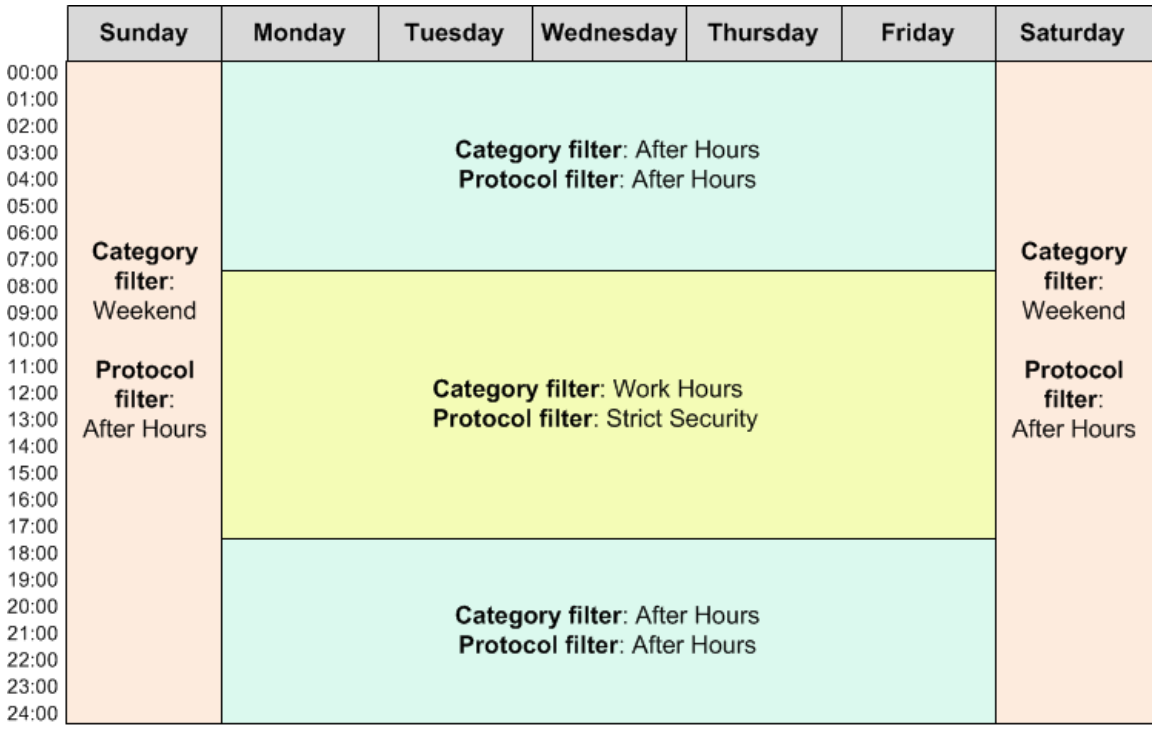
Transition Axiom 2: Know your policies

At its most basic, a Websense Web Security policy is made up of 3 components:

- A **schedule** determines when each group of security settings applies.
- A **category filter** defines enforcement actions (permit, block, confirm, quota) for each URL category during the selected time period.

  Instead of a category filter, each time period in the schedule can apply a **limited access filter** (a list of specific URLs and IP addresses that users can access). When a limited access filter is used, client requests for sites not appearing in the list are blocked.
- A **protocol filter** defines enforcement actions (permit, block) for each non-HTTP protocol during the selected time period.

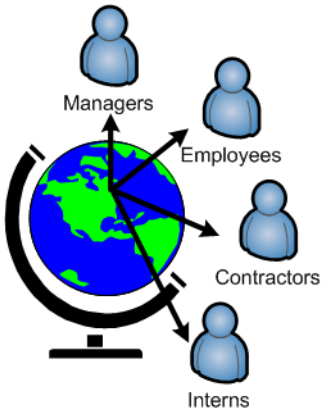
This makes it easy to create a single policy that applies more restrictive filters during work or school hours, or at times of peak bandwidth usage, with less restrictive filters at other times, as shown here:



Transition Axiom 3: Make the Default policy your foundation

With SurfControl Web Filter, ANYBODY rules filter users not specifically named in a previous rule.

With Websense Web Security solutions, the **Default** policy applies to any client to whom no other policy is assigned. It acts as a safety net, or baseline.



After installation, the Default policy initially monitors all Internet access requests without blocking.

Customize your Default policy to enforce your organization's fundamental acceptable use policy for Internet access. Remember:

- The Default policy is enforced for new users or machines in your network until you assign them another policy.
- The Default policy is enforced any time no other policy applies.

Once the Default policy has been customized for your organization, use it to derive policies for individuals or groups who need a different (more or less restrictive) set of access permissions.

Understand the Default policy

The Default policy initially monitors Internet requests without blocking, enforcing the **Monitor Only** category and protocol filters 24 hours a day, 7 days a week.

As you prepare to customize the Default policy, it may be helpful to review the default enforcement actions applied by the Default category and protocol filters. You can:

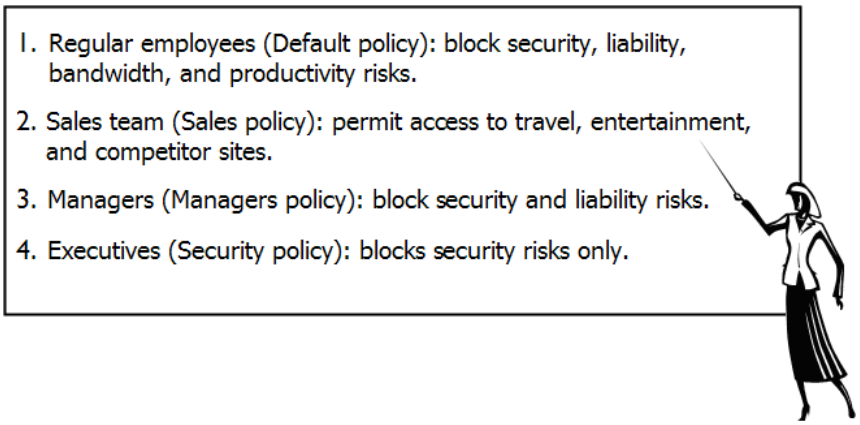
- Customize the Default category and protocol filters and use them to establish your organization's basic Internet access restrictions.
- Use the Default category and protocol filters as a template for creating custom category and protocol filters.

Policy examples

The number of policies appropriate for your organization depends more on the variation in different users' Internet access requirements than on the number of clients. Once you have identified the clients and their basic needs, you should be able to get a feel for the number of policies required to govern their Internet access.

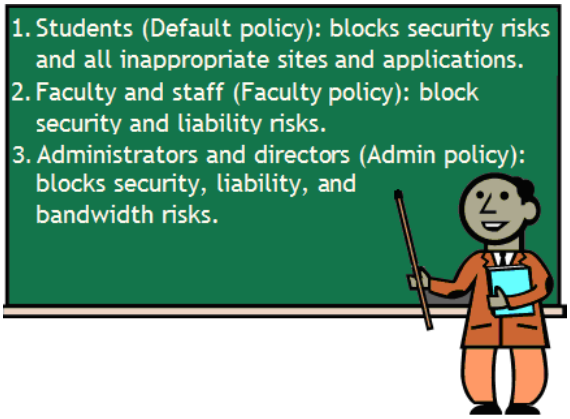
Universal Parts Supply

- 400 clients: 310 regular employees, 60 sales people, 20 managers, 10 executives
- 4 policies



Township Schools

- 3 campuses with centralized Internet services
- 1635 clients: 1200 students, 400 faculty and staff, 30 administrators, 5 directors
- 3 policies

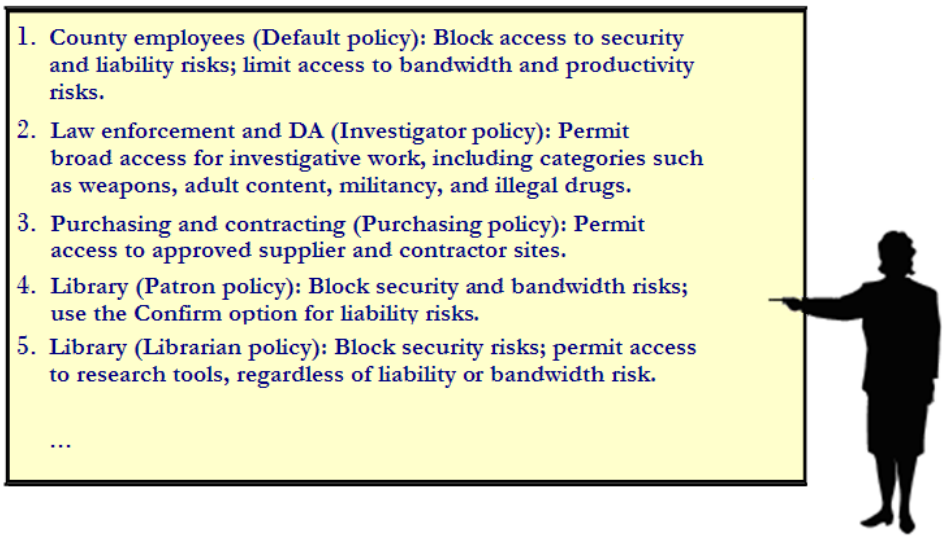


Big Mountain County

- 21 county offices:

Agriculture, Weights/Measures	Environmental Health	Medical Examiner
Animal Services	Finance and General Government	Planning and Land Use
Assessor/Recorder/County Clerk	Grand Jury	Public Defender
Board of Supervisors	Health and Human Services	Public Works
Child Welfare Services	Land Use and Environment	Purchasing and Contracting
District Attorney	Law Enforcement	Technology Office
Emergency Services	Library	Treasurer/Tax Collector

- 6000 clients with a wide range of responsibilities
- Required policies:??



In large organizations with many distinct functions, the IT department's organizational network topology or directory service structure can help to graph out a client hierarchy to simplify the policy creation process.

One alternative to a comprehensive, top-down analysis is to simply identify the exceptions. For example, although most county employees are likely to have similar Internet access needs, regardless of department:

- Some Law Enforcement officers and investigators for the District Attorney require access to otherwise restricted sites.
- Given freedom of information concerns, libraries may want to limit restrictions on patrons as much as is practical.

And so on. Still, requests from the majority of Big Mountain County employees can be managed using the Default policy.

Summary

Helpful correlations between SurfControl and Websense solutions

Now that you have a basic understanding of the Websense Web Security model, you can see that SurfControl Web Filter and Websense Web Security do correlate in some helpful ways:

- Clients: Who
- Schedule: When
- Category and protocol filters: Where and What

Mining information from SurfControl rules

As you configure Websense Web Security policies, you may encounter special clients for whom you need or want to examine the SurfControl rules to confirm the policy settings.

Because the rules model distributes the security settings for any particular user across many rules, it may be difficult to quickly pinpoint how a particular client is filtered at a particular time of day. To find that information may mean looking at many, many rules.

To print your SurfControl rule set:

1. Open the Rules Administrator and select **Tools > Options**.
2. In the **Rules Print Options** tab, for each category in the **Category Name** list, select the entry and enable **Detailed** for the **Selected Column Detail Level**.
3. After **Detailed** has been set for all categories, click **OK** to save the changes and close the dialog.
4. Go to **File > Print**, select a printer, select **All** for the **Page Range** (the default), and click **OK**.
5. Retrieve the printed pages.

When you mine for information for a particular Who, always start with the first rule. Because rules are processed from the top down, you can stop when you come to the first rule that applies.

URL category and Internet protocol differences

Websense Web Security solutions classify sites into more categories, and identifies more default non-HTTP protocols.

- The SurfControl Threat Database includes 55 URL categories.
- The Websense Master Database defines more than 125 categories.

The granularity of Websense Master Database categories gives you more control. It also means that you have more choices to make when you set up a policy.

Both SurfControl and Websense products allow you to define your own custom categories and protocols.

Planning and configuration

A *Configuration Guide*, worksheets, video tutorials, Knowledge Base articles, and other resources are available to help you through every step in the transition process.

The Configuration Guide provides installation and configuration instructions for a standard deployment of Websense Web Security or Websense Web Security Gateway, with policy enforcement components on a V-Series appliance and management and reporting components on a 64-bit Windows server.

Use the *Configuration Guide* in conjunction with the following worksheets to develop a comprehensive security and reporting solution:

- ❑ 1. Use the Client Worksheet to catalog and organize your clients. Group clients with similar Internet usage requirements as a first step in policy planning.
- ❑ 2. Use the Policy Planning Worksheet to construct your Default policy. This establishes the default set of Internet access regulations that apply to the most representative set of users in your organization.
  - See the URL Category Map reference for help understanding SurfControl categories map to Websense categories.
  - Use the Category Filter Planning Worksheet to construct each category filter to be enforced by the Default policy.
  - Use the Protocol Filter Planning Worksheet to construct each protocol filter to be enforced by the Default policy.
- ❑ 3. Copy the worksheets used to plan the Default policy to serve as a baseline for developing additional policies.
- ❑ 4. Configure your Websense Web Security solution to apply policies to your clients.

If you are deploying Websense software in a larger network (over 2500 users), consult the Websense Deployment & Installation Center for additional help in planning your environment.

Additional resources are available to help you both with your initial Websense implementation, and with any questions that may arise as you work with Websense software. Refer to the Websense Knowledge Base for technical articles, short tips, video tutorials, and complete product documentation for your Websense product and version.

The following materials may be especially helpful as you start to use your Websense software.

Articles

- How do I create Web Security policies?
- Applying policies to clients
- How do I change the way an invididual website is managed?
- Configuring Websense software to communicate with Active Directory
- What is a limited access filter?
- Getting started with Network Agent. This Web Security component corresponds to the SurfControl Device Driver for Stand Alone Mode.
- Configuring system and usage alerts.
- How do I back up or restore my configuration?
- Web Security default ports

References

- Deployment and Installation Center
- Websense Web Security Help