

# WEB FILTERING FOR BRANCH SRX SERIES AND J SERIES

Configuring Web Filtering on Branch SRX Series  
Services Gateways and J Series Services Routers

## Table of Contents

|  |    |
|--|----|
| Introduction .....                         | 3  |
| Scope .....                                | 3  |
| Design Considerations .....                | 3  |
| Hardware Requirements .....                | 3  |
| Software Requirements .....                | 3  |
| Description and Deployment Scenario .....  | 3  |
| SurfControl Integrated Web Filtering ..... | 3  |
| Websense Redirect Web Filtering .....      | 4  |
| White and Black Lists .....                | 5  |
| Licensing .....                            | 5  |
| Configuration .....                        | 6  |
| Configuration Examples .....               | 8  |
| SurfControl Integrated .....               | 8  |
| Custom Block Lists .....                   | 9  |
| Adding Custom Block Messages .....         | 11 |
| Scheduling Policies .....                  | 12 |
| Websense Redirect .....                    | 13 |
| Monitoring .....                           | 15 |
| Scalability .....                          | 15 |
| Summary .....                              | 15 |
| About Juniper Networks .....               | 16 |

## Table of Figures

|   |   |
|---|---|
| Figure 1: SurfControl integrated solution ..... | 3 |
| Figure 2: Websense redirect solution .....      | 4 |
| Figure 3: UTM policies .....                    | 6 |
| Figure 4: Example network .....                 | 8 |

## Introduction

Web filtering or URL filtering, is an established part of any unified threat management (UTM) suite and has been available on firewalls for many years. Although the introduction of Web 2.0 has created new security requirements, URL filtering remains an integral part of any security strategy. In some respects, Web filtering acts as a first line of defense. If a website is a known source of malware, what can be easier than simply blocking access to that site? Additionally, URL filtering provides an easy way to enforce enterprise business policy.

## Scope

Juniper Networks® Junos® operating system release 9.5 adds UTM support for Juniper Networks J Series Services Routers and select Juniper Networks SRX Series Services Gateways. Web filtering—one of several features including antivirus, anti-spam, and content filtering that make up Juniper Networks UTM suite—provides the ability to permit or deny access to specific URLs individually or based on the category to which they belong. Two different modes of operation are explained first—SurfControl integrated option and Websense redirect feature—and then several configuration examples are provided.

## Design Considerations

When deciding to deploy Web filtering, network designers should consider the performance impact of value-added security. Specific product guidelines can be found on J Series Services Routers and SRX Series Services Gateways datasheets.

## Hardware Requirements

- Juniper Networks SRX Series Services Gateways for the branch (including the SRX100, SRX210, SRX240, and SRX650)
- Juniper Networks J Series Services Routers (including the J2320, J2350, J4350, and J6350)

## Software Requirements

- Junos OS release 9.5 or later

## Description and Deployment Scenario

The Juniper Web filtering solution is available in two flavors—an integrated solution that queries an in-the-cloud SurfControl database or a redirect solution that requires a locally managed Websense server. By reading this application note, readers will be able to choose which method best meets their needs and be able to easily configure Web filtering on SRX Series Services Gateways or J Series Services Routers.

## SurfControl Integrated Web Filtering

The first and most common Web filtering method is to use the in-the-cloud SurfControl server, which stores a database of categories and associated URLs. The SurfControl integrated option requires the purchase of a Juniper Web filtering license. Every time a user tries to access a site, the Juniper gateway (J Series or SRX Series) captures the requested URL and queries the SurfControl database. The server responds with the site's category, which is then used by a Web filtering policy on the gateway to allow or deny access.

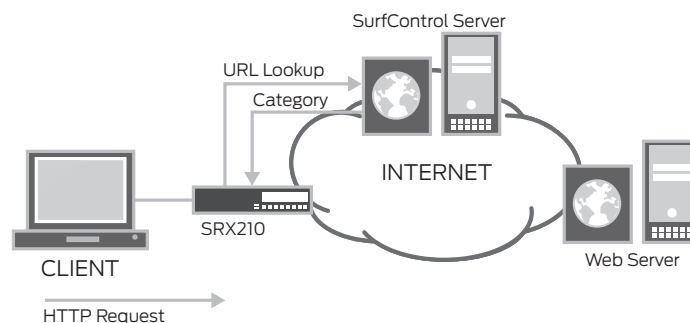


Figure 1: SurfControl integrated solution

The SurfControl database features:

- More than 26 million URLs
- Approximately 40 categories (the number of categories may change from release to release)
- More than 70 languages

The current SurfControl server uses the following categories:

**Table 1: SurfControl Integrated Categories**

| CATEGORIES              |                 |                               |                          |
|-------------------------|-----------------|-------------------------------|--------------------------|
| Adult Sexually Explicit | Advertisements  | Arts Entertainment            | Chat                     |
| Computing Internet      | Criminal Skills | Drugs Alcohol Tobacco         | Education                |
| Finance Investment      | Food Drink      | Gambling                      | Glamour Intimate Apparel |
| Government Politics     | Hacking         | Hate Speech                   | Health Medicine          |
| Hobbies Recreation      | Hosting Sites   | Job Search Career Development | Kids Sites               |
| Lifestyle Culture       | Motor Vehicles  | News                          | Personals Dating         |
| Photo Searches          | Real Estate     | Reference                     | Religion                 |
| Remote Proxies          | Search Engines  | Sex Education                 | Shopping                 |
| Sports                  | Streaming Media | Travel                        | Usenet News              |
| Violence                | Weapons         | Web-Based Email               |                          |

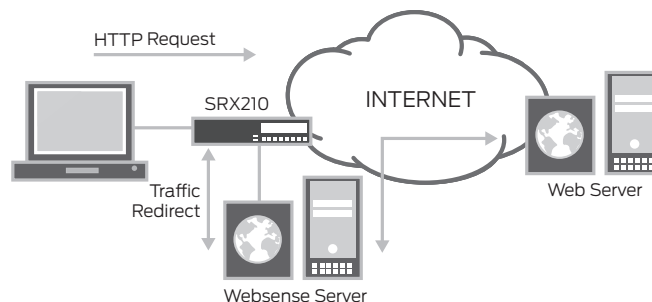
After the request returns a category and the gateway policy is evaluated, the SRX Series device for the branch or J Series router generates a log message indicating the action taken based on the returned category and configured policy. This message can either be locally stored and/or sent to a remote system log server or log collector (like Juniper Networks STRM Series Security Threat Response Managers).

Once a site is associated with a category, the result is cached locally. Subsequent requests for the same URL do not require a new query to the centralized database. The main advantage of this solution is that users do not need to host the database, which often requires a redundant server infrastructure. However, there are some trade-offs associated with using the in-the-cloud SurfControl solution. In particular:

- There will be some delay associated with the centralized server query. The local cache mitigates the delay, but first-time requests (or requests for entries that have timed out) will always experience an extra delay.
- Additional features (like the ability to detect and block some peer-to-peer traffic if IPS is enabled), which can be provided using a redirect solution, are not possible when using an integrated solution.

## Websense Redirect Web Filtering

A second approach is to use the Websense redirect feature. The redirect option does not require a separate Juniper license, but utilizes a local database, which must be purchased separately from Websense. As opposed to querying the SurfControl-hosted server, the services router redirects the URL to the local Websense server, which contains both the category database and the Web filtering policies. The Websense server then compares the URL against its database and returns the result according to its configured policy. The response is then forwarded to the SRX Series device or J Series router, indicating whether the URL is allowed or denied.



**Figure 2: Websense redirect solution**

The Websense redirect server features:

- 95 categories
- Support for over 100 protocols
- Local policy evaluation
- Logging and reporting support

This solution has the advantage of minimizing processing delays (since the database is locally stored), but requires:

The purchase of Websense software and subscription license to keep the database current

- A server or multiple servers for redundancy at each site (or at a central site, which would then increase processing delays similar to the integrated solution)
- Administrators to keep the category database current

Additionally, HTTPS URLs cannot be filtered, since the URL cannot be extracted.

## White and Black Lists

Administrators can also configure custom URL categories, which can be included in black and white lists that are evaluated on the gateway. All URLs for each category in a black list are denied, while all URLs for each category in a white list are permitted. The processing order is as follows:

- A new URL is first compared to the black list URLs. If a match is found, the traffic is dropped without any further processing.
- If no match is found, the URL is evaluated against the white list where traffic is allowed if a match is found.
- If no user-defined category results in a match, processing continues as normal—either by the SurfControl integrated or the Websense redirect method.

Custom categories can also be used as part of the SurfControl integrated solution. In this case, custom categories are added to the gateway policies exactly as predefined categories are added.

## Licensing

As previously discussed, a license is required to enable the SurfControl integrated solution, but is not required to enable the Websense redirect solution. The installed licenses in a device can be displayed with the “show system license” command.

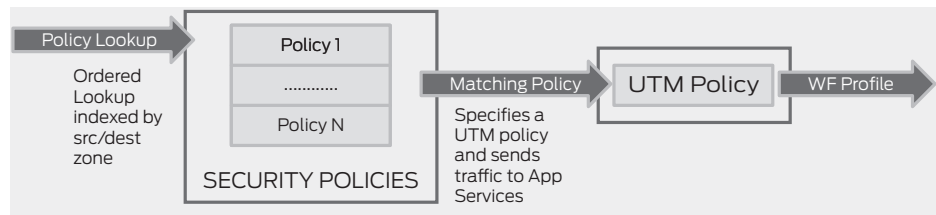
```
pato@SRX210-1# run show system license
License usage:

```

| Feature name               | Licenses used | Licenses installed | Licenses needed | Expiry     |
|----------------------------|---------------|--------------------|-----------------|------------|
| av_key_kaspersky_engine    | 1             | 1                  | 0               | 2009-11-20 |
| 00:00:00 UTC               |               |                    |                 |            |
| anti_spam_key_symantec_sbl | 0             | 1                  | 0               | 2009-11-20 |
| 00:00:00 UTC               |               |                    |                 |            |
| wf_key_surfcontrol_cpa     | 0             | 1                  | 0               | 2009-11-20 |
| 00:00:00 UTC               |               |                    |                 |            |
| idp-sig                    | 0             | 1                  | 0               | 2009-11-20 |
| 00:00:00 UTC               |               |                    |                 |            |
| ...                        |               |                    |                 |            |

## Configuration

Web filtering is part of the UTM feature set. Security policies act as the central reference point for all the traffic forwarded by the gateway. A security policy is used to associate a UTM policy with certain traffic. The UTM policy specifies which Web filtering policy the gateway should use to filter users' HTTP requests.



**Figure 3: UTM policies**

In other words, a security policy specifies a UTM policy, which then specifies a Web filtering profile. The reason for the double level of indirection is that the UTM policy controls not only which profile is used for Web filtering, but also other UTM profiles such as antivirus, content filtering, and anti-spam.

The configuration hierarchy for UTM policies is shown in the following example:

```
security {
    utm {
        utm-policy <policy name> {
            anti-spam {...}
            anti-virus {...}
            content-filtering {...}
            web-filtering {
                http-profile <web-filtering profile name>;
            }
        }
    }
}
```

The Web filtering profiles are configured under the [security utm feature-profiles] hierarchy as shown in the following:

```
security {
    utm {
        feature-profile {
            web-filtering {
                url-blacklist <black-list user defined category>;
                url-whitelist <white-list user defined category>;
                type surf-control-integrated|websense-redirect;
                surf-control-integrated {
                    cache {
                        size <max number of entries in the cache>;
                        timeout <time, in seconds, after which an
entry is declared invalid>;
                    }
                    profile <profile name> {
                        category <category name> {
                            #One or more categories are allowed
                            action block|log-and-permit|permit;
                        }
                        custom-block-message <block-message>;
                        default block|log-and-permit|permit;
                        fallback-settings {...};
                    }
                }
            }
        }
    }
}
```



## Configuration Examples

The following examples illustrate how some of the discussed features are configured. The examples assume that interfaces (with IP addresses), zones, and routing are already configured. Please refer to standard Juniper documentation should you have questions about initial configuration.

### SurfControl Integrated

For the network shown in Figure 4, assume that the integrated SurfControl method is chosen and the following categories are to be blocked:

- Criminal Skills
- Remote Proxies
- Violence
- Weapons

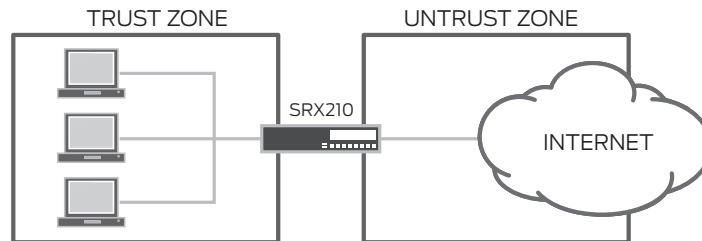


Figure 4: Example network

The SurfControl integrated feature is subsequently enabled by creating a Web filtering profile with a default permit action that blocks the categories previously listed.

```

security {
  policies {
    from-zone trust to-zone untrust {
      policy utm {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit {
            application-services {
              utm-policy wf-block-specific-categories;
            }
          }
        }
      }
    }
  }
}
utm {
  feature-profile {
    web-filtering {
      type surf-control-integrated; #This causes the device to use
                                   # the surfcontrol integrated
    }
  }
}
solution
surf-control-integrated {
  profile block-selected-sites {
    category {
      Criminal_Skills {

```



This category is then used as the black list in a Web filtering policy, which in this case is the policy that was created in the previous example

```

policies {
  from-zone trust to-zone untrust {
    policy utm {
      match {
        source-address any;
        destination-address any;
        application any;
      }
      then {
        permit {
          application-services {
            utm-policy wf-block-specific-categories;
          }
        }
      }
    }
  }
}
utm {
  feature-profile {
    web-filtering {
      url-blacklist bad-sites;  #This causes sites in the bad-sites
category
#to be blocked
      type surf-control-integrated;
      surf-control-integrated {
        profile block-selected-sites {
          category {
            Criminal_Skills {
              action block;
            }
            Remote_Proxies {
              action block;
            }
            Violence {
              action block;
            }
            Weapons {
              action block;
            }
          }
          default permit;
        }
      }
    }
  }
  utm-policy wf-block-specific-categories {
    web-filtering {
      http-profile block-selected-sites;
    }
  }
}

```

## Adding Custom Block Messages

Administrators can also configure custom messages when sites are blocked. Building on the previous example, the Web filtering profile will be changed so that when a site is blocked the message "The site requested is not a work-related site. Go back to work!" is sent to users.

```

policies {
  from-zone trust to-zone untrust {
    policy utm {
      match {
        source-address any;
        destination-address any;
        application any;
      }
      then {
        permit {
          application-services {
            utm-policy wf-block-specific-categories;
          }
        }
      }
    }
  }
}
utm {
  feature-profile {
    web-filtering {
      url-blacklist bad-sites;
      type surf-control-integrated;
      surf-control-integrated {
        profile block-selected-sites {
          category {
            Criminal_Skills {
              action block;
            }
            Remote_Proxies {
              action block;
            }
            Violence {
              action block;
            }
            Weapons {
              action block;
            }
          }
          default permit;
          custom-block-message "The site requested is not a work-
related site! Go back to work!";
        }
      }
    }
  }
  utm-policy wf-block-specific-categories {
    web-filtering {
      http-profile block-selected-sites;
    }
  }
}

```

## Scheduling Policies

The previously configured policies will now be used to block traffic to certain sites, but only during business hours. To create such a schedule, two security policies will be configured—one with Web filtering enabled and the other one without. The “block” policy, when active, will take precedence (by being first in the list) over the “allow” policy and will be enabled only during business hours.

```

security {
  policies {
    from-zone trust to-zone management {
      policy webfilter-on-business-hours {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit {
            application-services {
              utm-policy wf-block-specific-categories;
            }
          }
        }
        scheduler-name Business-hours;
      }
      policy accept-all {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
  }
}
utm {
  feature-profile {
    web-filtering {
      url-blacklist bad-sites;
      type surf-control-integrated;
      surf-control-integrated {
        profile block-selected-sites {
          category {
            Criminal_Skills {
              action block;
            }
            Remote_Proxies {
              action block;
            }
            Violence {
              action block;
            }
            Weapons {
              action block;
            }
          }
          default permit;
          custom-block-message "The site requested is not a work-
related site! Go back to work!";
        }
      }
    }
  }
}

```



```

    }
    utm-policy wf-redirect {
        web-filtering {
            http-profile server1-redirect;
        }
    }
}

```

The sockets parameter configures how many simultaneous connections (for redundancy and load-balancing purposes) the Junos OS-based gateway can establish with the Websense server.

Finally, both the Websense redirect and the SurfControl integrated solutions allow users to specify how requests should be treated when a failure occurs. The following example shows a scenario in which traffic is allowed when the gateway is overloaded, but denied for all other failure scenarios—such as when the server is down, or a client cannot connect to the server.

```

policies {
    from-zone trust to-zone management {
        policy webfilter-websense {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit {
                    application-services {
                        utm-policy wf-redirect;
                    }
                }
            }
        }
    }
}
utm {
    feature-profile {
        web-filtering {
            type websense-redirect;
            websense-redirect {
                profile server1-redirect {
                    server {
                        host 10.1.1.100;
                        port 15868;
                    }
                    custom-block-message "Websense says... you are not allowed!";
                    fallback-settings {
                        default block;
                        too-many-requests log-and-permit;
                    }
                    sockets 8;
                }
            }
        }
    }
    utm-policy wf-redirect {
        web-filtering {
            http-profile server1-redirect;
        }
    }
}

```

## Monitoring

Both the integrated and the redirect solutions provide a command, which displays the number of requests received and the resulting action.

```
>show security utm web-filtering statistics
UTM web-filtering statistics:
  Total requests:                0
  white list hit:                0
  Black list hit:                0
  Server reply permit:          0
  Server reply block:           0
  Web-filtering sessions in total: 4000
  Web-filtering sessions in use: 0
  Fall back:                     log-and-permit          block
    Default                      0                0
    Timeout                      12               0
    Connectivity                  0                0
  Too-many-requests              0                0
```

## Scalability

The following are the maximum platform-independent configuration limits for customer categories, white lists and black lists:

**Table 2: Platform-Independent Scalability Numbers**

|   |      |      |      |
|---|------|------|------|
| Maximum user defined categories             | 30   | 40   | 50   |
| Maximum URL lists per user defined category | 15   | 20   | 30   |
| Maximum URLs per URL list                   | 500  | 1000 | 1500 |
| Maximum URLs per whitelist/blacklist        | 8192 | 8192 | 8192 |
| Max length of URL list name                 | 29   | 29   | 29   |
| Max length of URL string (bytes)            | 512  | 512  | 512  |
| Max length of category name                 | 29   | 29   | 29   |

## Summary

The Web filtering feature introduced in Junos OS 9.5 for SRX Series Services Gateways and J Series Services Routers provide a simple way to permit or deny access to URLs based on easy-to-manage lists or predefined categories. Although this has been a common firewall feature for many years, it still remains an integral part of any security strategy by acting as a first line of defense.

## About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at [www.juniper.net](http://www.juniper.net).

---

### Corporate and Sales Headquarters

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
Phone: 888.JUNIPER (888.586.4737)  
or 408.745.2000  
Fax: 408.745.2100  
[www.juniper.net](http://www.juniper.net)

### APAC Headquarters

Juniper Networks (Hong Kong)  
26/F, Cityplaza One  
1111 King's Road  
Taikoo Shing, Hong Kong  
Phone: 852.2332.3636  
Fax: 852.2574.7803

### EMEA Headquarters

Juniper Networks Ireland  
Airside Business Park  
Swords, County Dublin, Ireland  
Phone: 35.31.8903.600  
EMEA Sales: 00800.4586.4737  
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.