

**SOPHOS**

Security made simple.



# Workflow Guide

## How to setup application filter

Product: Sophos XG Firewall

Document Date: November 2017

## Contents

<b>Overview</b> .....	<b>3</b>
<b>Configuration</b> .....	<b>3</b>
Step 1: Configure bandwidth management policy .....	3
Step 2: Apply Traffic Shaping policy on Application Category .....	5
Step 3: Create a new Application Filter Policy .....	6
Step 4: Create Firewall Rule for application filter .....	8
<b>Copyright Notice</b> .....	<b>9</b>

## Overview

An Application Filter Policy controls a user's application access. It specifies which user has access to which applications and allows you to define powerful security policies based on almost limitless policy parameters like:

- Individual users
- Groups of users
- Time of day

The device is shipped with the certain predefined policies such as 'Allow All', 'Deny All' for application filters to address common use cases.

## Configuration

### Step 1: Configure bandwidth management policy

Go to **Configure > System Services > Traffic Shaping** and click **Add** to add a new bandwidth management policy.

Parameter	Value	Description
<b>Name</b>	<b>Restrict_Videodownload</b>	Restricts the bandwidth for a particular user.
<b>Policy Association</b>	<b>Applications</b>	Select Type of Policy Associations from Available Options: <ul style="list-style-type: none"><li>– Users</li><li>– Rules</li><li>– Web Categories</li><li>– Applications</li></ul>
<b>Rule Type</b>	<b>Limit</b>	Select the type of policy. Available Options: <ul style="list-style-type: none"><li>– <b>Limit</b>- In this type of policy, user cannot exceed the defined bandwidth limit.</li><li>– <b>Guarantee</b>- In this type of policy, user is allocated</li></ul>

Parameter	Value	Description
		the guaranteed amount of bandwidth and can draw bandwidth up to the defined limit, if available.
<b>Limit Upload/Download Separately</b>	<b>Disable</b>	Select from the available options. Available Options: <ul style="list-style-type: none"> <li>- <b>Disable</b> - Limits total (Upload + Download) bandwidth.</li> <li>- <b>Enable</b> - Limits Upload and Download bandwidth separately.</li> </ul>
<b>Priority</b>	<b>2-Normal</b>	Set the bandwidth priority. Priority can be set from 0 (highest) to 7 (lowest) depending on the traffic required to be shaped. <ul style="list-style-type: none"> <li>- 0 - Real Time for example, VOIP</li> <li>- 1 - Business Critical</li> <li>- 2 to 5 - Normal</li> <li>- 6 - Bulky - FTP</li> <li>- 7 - Best Effort for Example, P2P</li> </ul>
<b>Limit</b>	<b>512</b>	Specify allowed total bandwidth.
<b>Bandwidth Usage Type</b>	<b>Shared</b>	Select the type of bandwidth usage. Available Options: <ul style="list-style-type: none"> <li>- <b>Individual</b> - Allocated bandwidth is for the particular User/Rule/Web</li> </ul>

## How to setup application filter

Parameter	Value	Description
		Category/Application only. – <b>Shared</b> - Allocated bandwidth is shared among all the Users/Rules/Web Categories/Applications who have been assigned this policy.

System Services
How-To Guides Log Viewer Help admin abcd

High Availability
Traffic Shaping Settings
RED
Malware Protection
Log Settings
Data Anonymization
**Traffic Shaping**
Services

Add Traffic Shaping (QoS) Policy

Name \*

Policy Association  Users  Rules  Web Categories  Applications

Rule Type  Limit  Guarantee

Limit Upload/Download Separately  Disable  Enable

Priority \*

Limit \*  Kbps [2 - 2560000]

Bandwidth Usage Type  Individual  Shared

Description

Add Schedule wise Traffic Shaping Policy Details to override default Traffic Shaping Policy Details

<input type="checkbox"/> Schedule	Rule Type	Up/Down Bandwidth (Min/Max Kbps)	Upload Bandwidth (Min/Max Kbps)	Download Bandwidth (Min/Max Kbps)	Manage
No Records Found					

Save
Cancel

Click **Save** to save bandwidth management policy.

### Step 2: Apply Traffic Shaping policy on Application Category

Go to **Protect > Applications > Traffic Shaping Default** and click **Manage** icon. Apply Traffic Shaping policy to the category.

## How to setup application filter

Applications Log Viewer Help admin  
Sophos Test Account

Application List Application Filter Traffic Shaping Default

This feature requires a subscription. It can be configured but cannot be enforced without a valid Web Protection subscription.

### Edit Download Applications Category

Name	Download Applications
Traffic Shaping Policy	Restrict_VideoDownload ⓘ

### Step 3: Create a new Application Filter Policy

Go to **Protect > Applications > Application Filter** and click **Add**. Enter name and description for application filter.

Applications How-To Guides Log Viewer Help admin  
abcd

Application List Synchronized Application Control Application Filter Traffic Shaping Default

Name *	Video Download Filter
Description	
Template	Allow All

Save Cancel

Note: Option to Enable Micro App Discovery is available for devices running on v16 and below. Click **Add** to add filter criteria as shown below:

# How to setup application filter

Applications Log Viewer Help admin Sophos Test Account

---

Application List      Application Filter      Traffic Shaping Default

This feature requires a subscription. It can be configured but cannot be enforced without a valid Web Protection subscription.

Add Application Filter Policy Rules

Application Filter Criteria

**Category**

Mobile Applications

Software Update

**Download Applications (541)**

**Risk**

Select All

1 - Very Low

2 - Low (10)

**Characteristics**

Select All

Excessive Bandwidth (14)

Prone to misuse (31)

**Technology**

Select All

Browser Based (34)

Client Server (20)

List of Matching Applications [ 1 - 50 of 54 ] \* Scroll down to view more

Select All    Select Individual Application   Search

<input type="checkbox"/>	Name	Description	Category	Risk	Characteristics	Technology
<input checked="" type="checkbox"/>	1Fichier Download	1Fichier Download	Download Applications	3 - Medium	Excessive Bandwidth,...	Browser E
<input checked="" type="checkbox"/>	2shared Download	2shared Download	Download Applications	2 - Low	Excessive Bandwidth,...	Browser E
<input checked="" type="checkbox"/>	ADrive Web Upload	ADrive Web Upload	Download Applications	3 - Medium	Transfer files,Prone...	Browser E
<input checked="" type="checkbox"/>	Akamai Client	Akamai Client	Download Applications	4 - High	Transfer files,Trans...	Client Ser
<input checked="" type="checkbox"/>	AttachLargeFile Download	AttachLargeFile Download	Download Applications	3 - Medium	Transfer files,Trans...	Browser E
<input checked="" type="checkbox"/>	Badonga Download	Badonga Download	Download Applications	4 - High	Prone to misuse,Tran...	Client Ser
<input checked="" type="checkbox"/>	Badongo File Download	Badongo File Download	Download Applications	3 - Medium	Transfer files,Prone...	Client Ser
<input checked="" type="checkbox"/>	Bearshare Download	Bearshare Download	Download Applications	4 - High	Widely Used,Transfer...	Client Ser

Action \*       Allow    Deny

Schedule \*

Save Cancel

Click **Save** to save the application filter policy.

# How to setup application filter

## Step 4: Create Firewall Rule for application filter

Go to **Protect > Firewall** and click **Add User / Network Rule**. Add a rule as shown below:

**Add User / Network Rule**

Log Viewer Help admin Sophos Test Account

Rule Name \* Video\_Download\_Rule Description Enter Description Rule Position Bottom

Action **Accept** Drop Reject

Source

Source Zones \* Any Source Networks and Devices \* Any During Scheduled Time All Time on Weekdays

Destination & Services

Destination Zones \* Any Destination Networks \* Any Services \* Any

Identity

Match known users  Show captive portal to unknown users User or Groups \* Any  Exclude this user activity from data accounting

Malware Scanning

Scan FTP  Scan HTTP  Decrypt & Scan HTTPS

**Summary**

**Video\_Download\_Rule**

**Rule**

Apply "Video Download Filter" app filter, "None" web filter, for any user, when in any zone, and coming from any network

**Source & Schedule**

Any  
Source Networks and Devices: Any  
During Scheduled Time: All Time on Weekdays

**Destination & Services**

Any  
Destination Networks: Any  
Services: Any

**Identity**

Any

**Advanced**

Synchronized Security

Source: Minimum Heartbeat is No Restriction, Clients with no heartbeat allowed  
Destination: Minimum Heartbeat is No Restriction, Request to destination with no heartbeat allowed  
Masquerading is ON

**Advanced**

User Applications

Intrusion Prevention  None

Traffic Shaping Policy

User's policy applied

Web Policy  None  Apply Web Category based Traffic Shaping Policy

**Application Control**  Apply Application-based Traffic Shaping Policy

Video Download Filter

Synchronized Security

Minimum Source HB Permitted:  GREEN  YELLOW  No Restriction  Block clients with no heartbeat

Minimum Destination HB Permitted:  GREEN  YELLOW  No Restriction  Block request to destination with no heartbeat

NAT & Routing

Rewrite source address (Masquerading)  Use Gateway Specific Default NAT Policy

Use Outbound Address

MASQ

MASQ (Interface Default IP)

Primary Gateway

None

Backup Gateway

None

DSCP Marking

Select DSCP Marking

Log Traffic

Log Firewall Traffic

Save Cancel

Click **Save**.



## Copyright Notice

Copyright 2015-2016 Sophos Limited. All rights reserved.

Sophos is a registered trademark of Sophos Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.