



Pocket Guide

How to setup application filter

For Customers with Sophos Firewall

Document Date: November 2016

Contents

Overview	3
Configuration	3
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.....	7
Copyright Notice.....	9

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

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

Parameter	Value	Description
Name	Restrict_Videodownload	Restricts the bandwidth for a particular user.
Policy Association	Applications	Select Type of Policy Associations from Available Options: <ul style="list-style-type: none"> – Users – Rules – Web Categories – Applications
Rule Type	Limit	Select the type of policy. Available Options: <ul style="list-style-type: none"> – Limit - In this type of policy, user cannot exceed the defined bandwidth limit. – Guarantee- In this type of policy, user is allocated the guaranteed amount of bandwidth and can draw bandwidth up to the defined limit, if available.
Limit Upload/Download Separately	Disable	Select from the available options. Available Options: <ul style="list-style-type: none"> – Disable - Limits total (Upload + Download) bandwidth. – Enable - Limits Upload and Download bandwidth separately.

Parameter	Value	Description
Priority	2-Normal	<p>Set the bandwidth priority. Priority can be set from 0 (highest) to 7 (lowest) depending on the traffic required to be shaped.</p> <ul style="list-style-type: none">– 0 - Real Time for example, VOIP– 1 - Business Critical– 2 to 5 - Normal– 6 - Bulky - FTP– 7 - Best Effort for Example, P2P
Limit	512	Specify allowed total bandwidth.
Bandwidth Usage Type	Shared	<p>Select the type of bandwidth usage.</p> <p>Available Options:</p> <ul style="list-style-type: none">– Individual - Allocated bandwidth is for the particular User/Rule/Web Category/Application only.– Shared - Allocated bandwidth is shared among all the Users/Rules/Web Categories/Applications who have been assigned this policy.

System Services Log Viewer Help admin
 Sophos Test Account

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

Edit Traffic Shaping (QoS) Policy

Name *	<input type="text" value="Restrict_VideoDownload"/>
Policy Association	<input type="radio"/> Users <input type="radio"/> Rules <input type="radio"/> Web Categories <input checked="" type="radio"/> Applications
Rule Type	<input checked="" type="radio"/> Limit <input type="radio"/> Guarantee
Limit Upload/Download Separately	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Priority *	<input type="text" value="2 - [Normal]"/>
Limit *	<input type="text" value="512"/> KBps (2 - 2560000)
Bandwidth Usage Type	<input type="radio"/> Individual <input checked="" type="radio"/> Shared
Description	<input type="text" value="This policy restricts video downloading by users."/>

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					

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

Step 2: Apply Traffic Shaping policy on Application Category

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

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

Navigate to **Protect > Applications > Application Filter** and click **Add**. Enter name and description for 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.

Name *	<input type="text" value="Video Download Filter"/>
Description	<input type="text"/>
	<input checked="" type="checkbox"/> Enable Micro App Discovery

<input type="checkbox"/>	Application	Application Filter Criteria	Schedule	Action	Manage
No Records Found					

Click **Add** to add filter criteria as shown below:

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 List of Matching Applications (1 - 50 of 54) * Scroll down to view more

Category

Mobile Applications

Software Update

Download Applications [54]

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]

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 *

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

Step 4: Create Firewall Rule for application filter

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

How to setup application filter

Add User / Network Rule

Log Viewer Help admin Sophie Test Account

Rule Name *
Video_Download_Rule

Action
 Accept Drop Reject

Description
Enter Description

Rule Position
Bottom

Summary

Video_Download_Rule
 Allow

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 a destination with no heartbeat allowed
Masquerading is ON

Source

Source Zones *
Any
Add New Item

Source Networks and Devices *
Any
Add New Item

During Scheduled Time
All Time on Weekdays

Destination & Services

Destination Zones *
Any
Add New Item

Destination Networks *
Any
Add New Item

Services *
Any
Add New Item

Identity

Match known users
 Show captive portal to unknown users

User or Groups *
Any
Add New Item

Exclude this user activity from data accounting

Malware Scanning

Scan FTP
 Scan HTTP
 Decrypt & Scan HTTPS

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
Video Download Filter
 Apply Application-based Traffic Shaping Policy

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** to save the firewall rule for application control.

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.