Workflow Guide

How to setup application filter

Product: Sophos XG Firewall
Document Date: November 2017
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 .........................................................................8
Copyright Notice ...............................................................................................................................9
How to setup application filter

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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Restrict_Videodownload</td>
<td>Restricts the bandwidth for a particular user.</td>
</tr>
<tr>
<td>Policy Association</td>
<td>Applications</td>
<td>Select Type of Policy Associations from Available Options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Rules</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Web Categories</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Applications</td>
</tr>
<tr>
<td>Rule Type</td>
<td>Limit</td>
<td>Select the type of policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Available Options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Limit - In this type of policy, user cannot exceed the defined bandwidth limit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Guarantee - In this type of policy, user is allocated</td>
</tr>
</tbody>
</table>
## How to setup application filter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Limit</strong></td>
<td><strong>Value</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| **Upload/Download Separately** | **Disable** | Select from the available options. Available Options:  
- **Disable** - Limits total (Upload + Download) bandwidth.  
- **Enable** - Limits Upload and Download bandwidth separately. |
| **Priority**               | **2-Normal** | Set the bandwidth priority. Priority can be set from 0 (highest) to 7 (lowest) depending on the traffic required to be shaped.  
- 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** | Select the type of bandwidth usage. Available Options:  
- **Individual** - Allocated bandwidth is for the particular User/Rule/Web |
How to setup application filter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Category/Application only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Shared</strong> - Allocated bandwidth is shared among all the Users/Rules/Web</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Categories/Applications who have been assigned this policy.</td>
</tr>
</tbody>
</table>

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

Step 3: Create a new Application Filter Policy

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

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

Click **Save** to save the application filter policy.
Step 4: Create Firewall Rule for application filter

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

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.