Pocket Guide

Customize Category of Synchronized Applications Captured by Sophos Endpoints

Product: Sophos XG Firewall
Customize Category of Synchronized Applications Captured by Sophos Endpoints

Contents
Overview ................................................................................................................................. 3
Prerequisites ............................................................................................................................ 4
Configuration .......................................................................................................................... 5
  Customize Synchronized Application Category ............................................................... 5
  Scenario 1: Sophos Endpoint identifies the application .................................................... 5
  Scenario 2: Sophos Endpoint does not identify application .......................................... 6
Result ....................................................................................................................................... 8
Copyright Notice .................................................................................................................... 9
Customize Category of Synchronized Applications Captured by Sophos Endpoints

**Overview**

This document describes how to customize the category of synchronized applications, which are captured by Sophos Endpoints, from Sophos XG Firewall.

Sophos Central Endpoint Advanced (CEA) protection and Intercept X (CIX) installed on endpoints can identify applications generating network traffic, and can update XG Firewall with the App ID and Cat ID (application and category IDs), actual path of the application, and the normalized path. If the endpoint is unable to identify the application, it sends the application’s actual and normalized paths to the device. You will need to categorize the unknown app manually.

The following scenarios emerge related to the identification of applications generating network traffic:

A. **Synchronized Applications**, which are captured by Sophos Endpoints and are unknown to XG Firewall, are listed on Protect > Applications > Synchronized Application Control.
   a. When Sophos Endpoints capture and identify an application, the application category is automatically assigned.
   b. Applications captured but not identified by Sophos Endpoints are listed in the pre-defined category SyncAppCtl Discovered.

B. **Applications**, which are identified by XG Firewall, are listed on Protect > Applications > Application List.
   a. XG Firewall’s IPS engine identifies and classifies the application, and the configured policies and firewall rules are applied.
   b. When a Sophos Endpoint identifies an application known to XG Firewall, the latter sends a message to the endpoint not to forward information about the application any more.
Prerequisites

- You must have read-write permissions on the SFOS Admin Console for the relevant features.
- You must have access to Sophos Central Admin Console.
- You must install the following on endpoint computers whose Security Heartbeat you wish to monitor:
  - Sophos Endpoint Advanced (CEA)
  - Intercept X (CIX)
- To enable Synchronized Application Control, you require Sophos Endpoint Advanced and Intercept X of version 11.x.
- You must enable Synchronized Application Control on XG Firewall (Protect > Synchronized Security).
- XG Firewall must receive a valid Heartbeat from Sophos Endpoints.
Customize Category of Synchronized Applications Captured by Sophos Endpoints

**Configuration**

Customize Synchronized Application Category

**Scenario 1: Sophos Endpoint identifies the application**

We use the scenario in which an employee uses VLC media player to stream YouTube streaming content. The application is not identified by XG Firewall since its signature is unknown (Protect > Applications > Application List).

- Go to Protect > Applications > Synchronized Application Control.
- VLC Player has been identified and automatically assigned the category Streaming Media.

- Click Customize to view the Application Category. You can change the category if you wish to.
Customize Category of Synchronized Applications Captured by Sophos Endpoints

Scenario 2: Sophos Endpoint does not identify application
We use the scenario in which an employee plays Hedge Wars. The application is not identified by XG Firewall since its signature is unknown.

- Go to Protect > Applications > Synchronized Application Control.
- Hedge Wars has been captured, but not identified as a gaming application by the Sophos Endpoint.
Customize Category of Synchronized Applications Captured by Sophos Endpoints

- Click Customize to view the Application Category. Hedge Wars has been assigned the category SyncAppCtl Discovered, which is the default category for unidentified synchronized applications. Change the Application Category to Gaming if you wish to, and click Save.

The existing application filter policy for streaming media and gaming, and the firewall rule for the configured source zones, networks or devices will apply to these applications. If the policy does not exist, you can create an application filter policy (Protect > Application Filter) and create the firewall rule.
Customize Category of Synchronized Applications Captured by Sophos Endpoints

**Result**

You have customized the category of synchronized applications captured by Sophos Endpoints.
Copyright Notice
Copyright 2016-2017 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.