Pocket Guide

Configure Discover (TAP) Mode and Security Audit Report

Product: Sophos XG Firewall
Configure Discover (TAP) Mode and Security Audit Report

## Contents

**Overview** .................................................................................................................. 3

**Prerequisites** ............................................................................................................. 3

**Features supported in TAP mode** ............................................................................. 4

**Network Diagram** .................................................................................................. 5

**Configuration** .......................................................................................................... 6

- Deploy XG Firewall in Discover Mode ........................................................................ 6
  - Step 1: Connect and Access XG Firewall ................................................................. 6
  - Step 2: Connect and Enable Discover Mode ............................................................ 6
  - CLI ............................................................................................................................. 6
  - Wizard ....................................................................................................................... 7
  - Step 3: Verify Configuration .................................................................................... 8
  - Step 4: Configure Port Mirroring on Network Switch ............................................ 8
  - Step 5: Security Audit Report [SAR] ...................................................................... 9
  - Schedule SAR Emails .............................................................................................. 9

**Result** ......................................................................................................................... 11

**Appendix** .................................................................................................................. 12

- Configure Authentication Server to send API Request and Integrate it with XG Firewall .................................................. 12
- Configure Sophos Firewall to accept API Request ................................................... 13

**Copyright Notice** ..................................................................................................... 14
Overview

This document describes how you can deploy Sophos XG Firewall device in discover (TAP) mode to enable passive monitoring of traffic flow in your network. When you connect an interface of the device to a SPAN or mirror port on a switch, traffic from the other switch ports is copied and provided to the device for analysis. The device can work with any existing firewall, and does not displace or disrupt existing IT security infrastructure.

Prerequisites

- You must have read-write permissions on the SFOS Admin Console and Command Line Interface for the relevant features.
- XG Firewall should be connected to the Internet for on-cloud web classification, IPS updates and SAR generation.
- The device must be connected to a switch that supports SPAN or mirror port configuration.
- You must have an unbound interface to enable discover mode.

Note: To unbind an interface, go to Configure > Network > Interfaces, select the interface and set Network Zone to None.
## Features supported in TAP mode

<table>
<thead>
<tr>
<th>Subscription</th>
<th>Features</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Protection</td>
<td>Synchronized App Control</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Heartbeat</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>IPS Detection</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Advanced Threat Protection</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>IPS Control</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>RED Device Support</td>
<td>No</td>
</tr>
<tr>
<td>Base Subscription</td>
<td>Reports</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Traffic Discovery</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>DoS</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>User Identity</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>High Availability</td>
<td>Yes (HA can be configured in TAP mode)</td>
</tr>
<tr>
<td></td>
<td>User Identity-based Control</td>
<td>No (User-based policy cannot be applied)</td>
</tr>
<tr>
<td></td>
<td>Network Services (ARP, Routing, DNS, DHCP)</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Firewall</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Spoofing</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>QoS</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Traffic ACLs</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>VPN</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>SSL VPN</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>IPv6</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Wireless Device Support</td>
<td>No</td>
</tr>
<tr>
<td>Email Protection</td>
<td>Mail Usage</td>
<td>No</td>
</tr>
<tr>
<td>Web &amp; Email Protection</td>
<td>AntiSpam</td>
<td>No</td>
</tr>
<tr>
<td>Web Protection</td>
<td>AntiVirus</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Application Classification (Signature-based)</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Web Categorization (Uses IPS)</td>
<td>Yes (Categorization against URLs)</td>
</tr>
<tr>
<td></td>
<td>Microapps (HTTPS Micro Apps)</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Application Filtering</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Web Filtering</td>
<td>No</td>
</tr>
<tr>
<td>Web Server Protection</td>
<td>WAF</td>
<td>No</td>
</tr>
</tbody>
</table>
Network Diagram

- **Internet**
- **Gateway Router**
- **Network Switch**
- **XG Firewall in Discover Mode**
- **Management Port**
  - Port A: 172.16.16.2/255.255.255.0
- **Discover Mode Enabled Port D**
- **WAN Port**
  - Port B: 172.16.16.16:4444
Configuration

Deploy XG Firewall in Discover Mode

Step 1: Connect and Access XG Firewall

- Connect one end of the straight-through cable to Port A of the device. Connect the other end to the Management Computer.
- Make the following changes to the LAN computer from which you wish to access the Admin Console of XG Firewall [Management Computer):
  - IP Address: 172.16.16.2
  - Subnet mask: 255.255.255.0

Step 2: Connect and Enable Discover Mode

Connect another cable from an unbound XG Firewall port [Example: Port D in this illustration] to the mirror port [on which you wish to configure port mirroring] on the network switch.

You can enable discover mode through:
1. **CLI**
2. **Wizard**

**CLI**

- Go to `admin > Console` in the upper-right corner.
• Type 4 to select Device Console.

![Main Menu]

1. Network Configuration
2. System Configuration
3. Route Configuration
4. Device Console
5. Device Management
6. VPN Management
7. Shutdown/Reboot Device
8. Exit

Select Menu Number [0-7]: 4

• Execute the following command to enable discover mode on Port D.
  
  console> system discover-mode tap add PortD

  ![console> system discover-mode tap add PortD]

Wizard

• Go to https://172.16.16.16:4444 from the Management Computer. Click Start and follow the on-screen instructions.
• Go to Network Configuration [LAN], click Enable TAP/Discover Mode.
• Select one or more ports to connect to the mirror port on the switch, click Apply.
Step 3: Verify Configuration

On Configure > Network > Interfaces, the discover mode interface will display Discover, Physical [TAP].

Note: When XG Firewall is deployed in discover mode, it functions in promiscuous mode, and no security policy is applied.

Step 4: Configure Port Mirroring on Network Switch

To configure the mirror port on the network switch, refer to the switch vendor’s documentation.

Note: Mirror port is the one connected to the XG Firewall port on which Discover mode has been enabled.
Step 5: Security Audit Report (SAR)

You can configure periodic email notifications with the Security Audit Report. It provides key observations, users with risk-prone behavior, including User Threat Quotient (UTQ), user application risks and usage, including Application Risk Score, high risk applications and application categories by data transfer, synchronized applications, web risks based on objectionable domains, web usage based on data transfer and hits, intrusion attacks, Advanced Threat Protection (ATP) visibility, and Security Heartbeat of endpoints.

Schedule SAR Emails

- Go to Monitor & Analyze > Reports. Click Show Reports Settings above the menu. Click Report Scheduling and click Add.
- Select Security Audit Report.
- Enter the Name, Organization Name, and To Email Address.
- Select the Email Frequency.

SAR Report
Click Save.

**Note:** SAR can also be generated when XG Firewall is deployed in in-line modes: gateway mode, bridge mode or mixed mode.
Result
You have deployed XG Firewall in discover mode and configured the SAR Report. For successful deployment, ensure the following:

- **Verify:**
  - Device can connect to the Internet
  - All services are running [Configure > System Services > Services]

- **Apply the latest versions [System > Backup & Firmware]:**
  - IPS signatures
  - Application signatures
  - AP firmware
  - RED firmware

- **Retain default settings for:**
  - Pattern updates [System > Backup & Firmware > Pattern Updates]
  - DoS settings [Protect > Intrusion Prevention > DoS & Spoof Prevention]

- **When you create security policies:**
  - IPS: Apply the default 'generalpolicy'
  - Web and Application filters: Apply **Allow All** filters and check for traffic flow
  - Configure email notification settings
  - Advanced Threat Protection: Set Policy to **Log Only**.

**Note:** SFOS does not support HTTPS in TAP mode.
Appendix

Configure Authentication Server to send API Request and Integrate it with XG Firewall

This configuration will ensure user-specific data in reports. The Authentication Server will send an API request to the device when a user sends a login or logout request.

Sample API Request Codes:

Login Request

  <Request>
  <LiveUserLogin>
  <UserName>Sophos</UserName>
  <Password>Sophos</Password>
  <IPAddress>10.21.18.15</IPAddress>
  <MacAddress>00:0C:29:2D:D3:AC</MacAddress>
  </LiveUserLogin>
  </Request>

Logout Request

  <Request>
  <LiveUserLogout>
  <Admin>
  <UserName>admin</UserName>
  <Password>admin</Password>
  </Admin>
  <UserName>Sophos</UserName>
  <IPAddress>10.21.18.15</IPAddress>
  </LiveUserLogout>
  </Request>

API link format

https://<SophosIP>/corporate/APIController?regxml=<Add the XML request here>
Example:

https://172.16.16.16/corporate/APIController?reqxml=<Request><LiveUserLogin><UserName>sophos</UserName><Password>sophos</Password><IPAddress>10.21.18.15</IPAddress><MacAddress>00:0C:29:2D:D3:AC</MacAddress></LiveUserLogin></Request>

Configure Sophos Firewall to accept API Request

- Log in to the SF Admin Console as administrator.
- Go to System > Back Up & Firmware > API and enable API Configuration.
- Add the IP Address from which SFOS receives API Requests.

![API Configuration](image)

Click Apply.
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.