

How to – Configure Zyxel Firewall to forward logs to EventTracker

EventTracker v9.2 and later

Abstract

This guide provides instructions to retrieve the **Zyxel firewall** events by syslog. After **EventTracker** is configured to collect and parse these logs, the dashboard and reports can be configured to monitor the **Zyxel firewall**.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 or above and **Zyxel firewall USG60(W), USG 310, USG110**.

Audience

Administrators who are assigned the task to monitor **Zyxel firewall** events using EventTracker.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright Zyxel firewall is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2021 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

| | |
|--|---|
| 1. Introduction | 3 |
| 2. Prerequisites | 3 |
| 3. Configuring Zyxel firewall Syslog logging | 3 |

1. Introduction

Zyxel firewalls are next-generation firewalls designed to deliver high availability, anti-malware protection, and consolidated policy enforcement for medium to large-sized businesses and campuses.

Zyxel firewall when configured sends events to EventTracker using syslog. Zyxel Firewall sends events like antivirus scan, intrusion detection and prevention, anti-spam, anti-virus, content filtering, unified security policy, IPsec VPN, SSL VPN, and WLAN management. Generates reports on antivirus spam detail, intrusion activities, configuration changes, interface statistics, traffic denied, etc. It contains username, client IP address, status, message, action, file path, file name, and hash. Graphically displays interface statistics, traffic denied by reason, traffic denied by IP address, threat detected by file name, device name, device IP, etc.

2. Prerequisites

- Administrative access on Zyxel firewall Console.
- EventTracker manager IP address.
- Allow port number 514 from the firewall end.

3. Configuring Zyxel firewall Syslog logging

1. Log into the Zyxel Web Interface.
2. Navigate to **Configuration > Log & Report > Log Settings**.

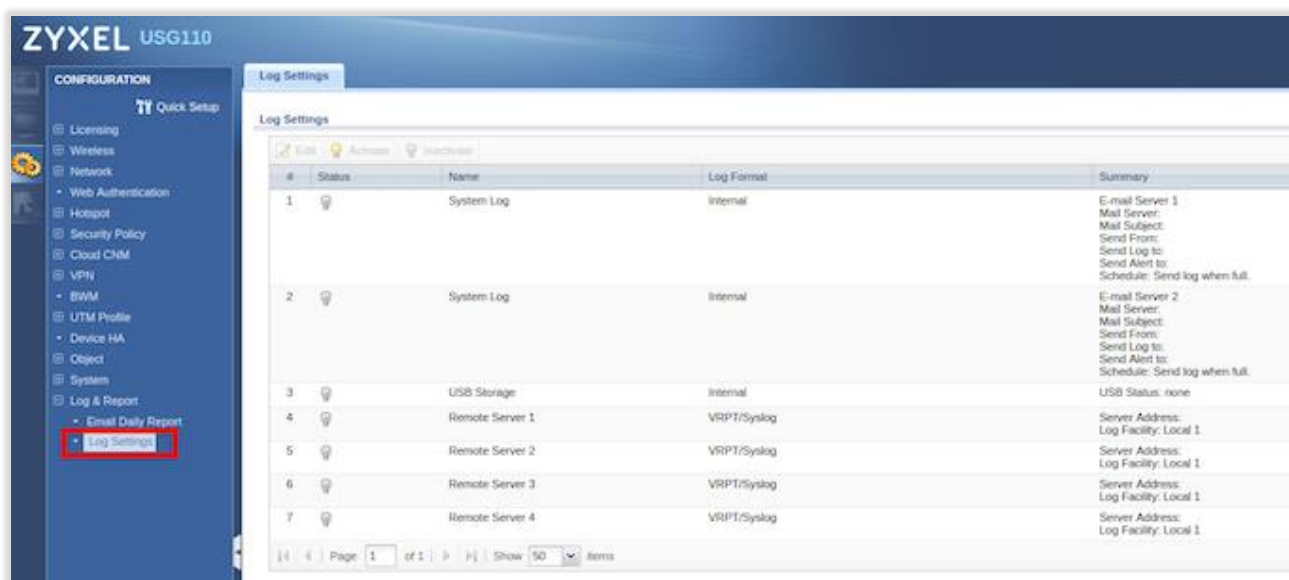


Figure 1

3. Choose a **Remote Server**.
4. Click **Active**.
5. Choose Log Format as **VRPT/Syslog**.
6. Enter the IP address of the **EventTracker**.
7. Select **Local 7** in the **Log Facility** field.
8. Select the **Categories** you want to be logged (normal = default logs, debug = very detailed logs, disable = no logs)

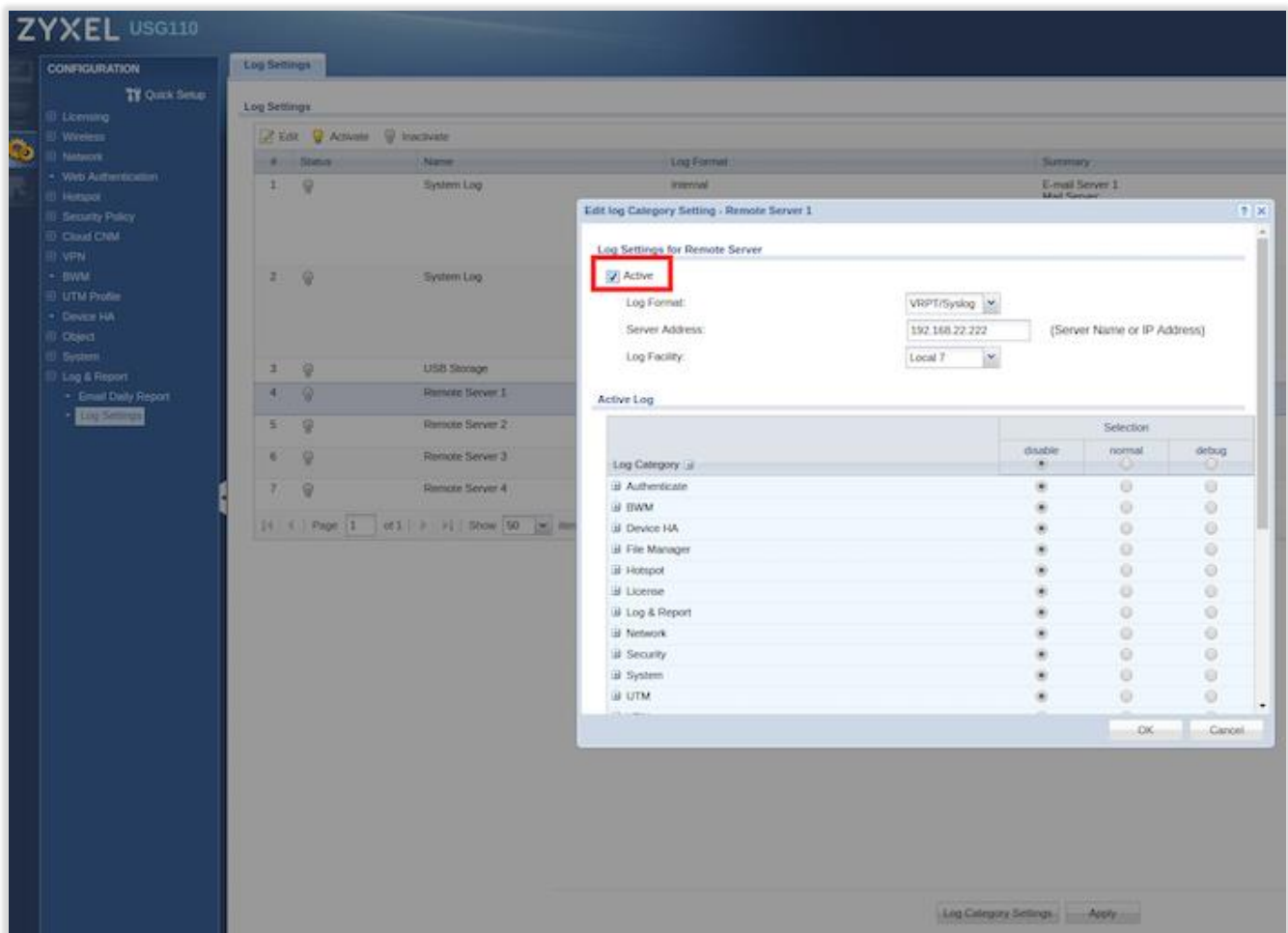


Figure 2