Netsurion | EventTracker®

How to – Configure Zyxel Firewall to forward logs to EventTracker

EventTracker v9.2 and later

Publication Date: January 13, 2021

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.

Table of Contents

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**.

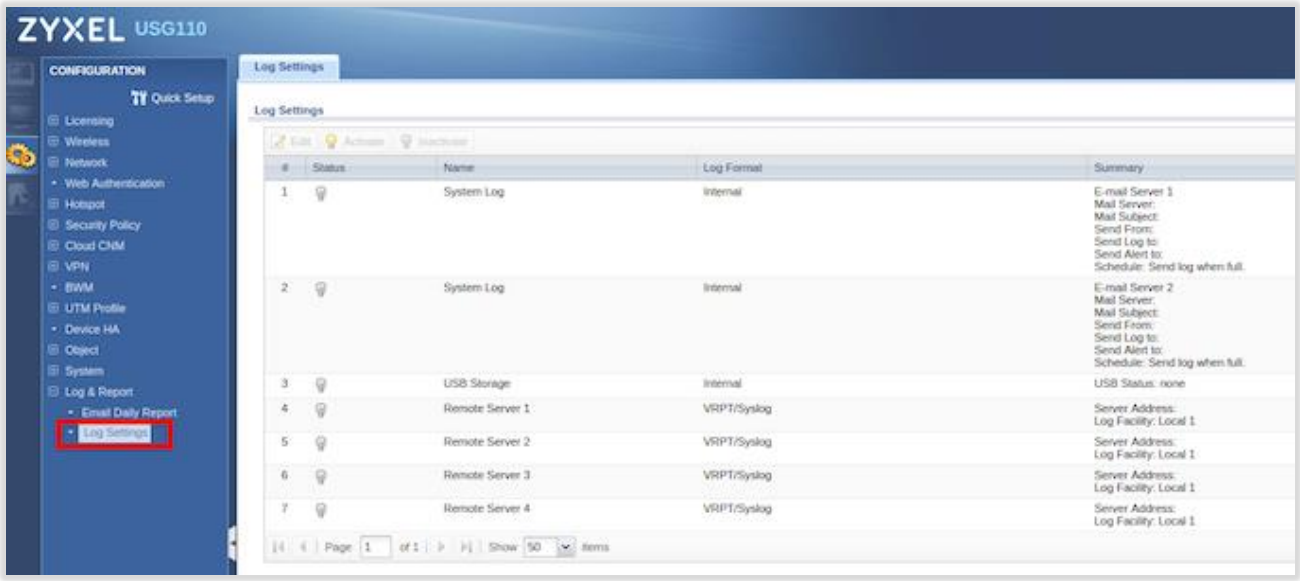

Figure 1

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)

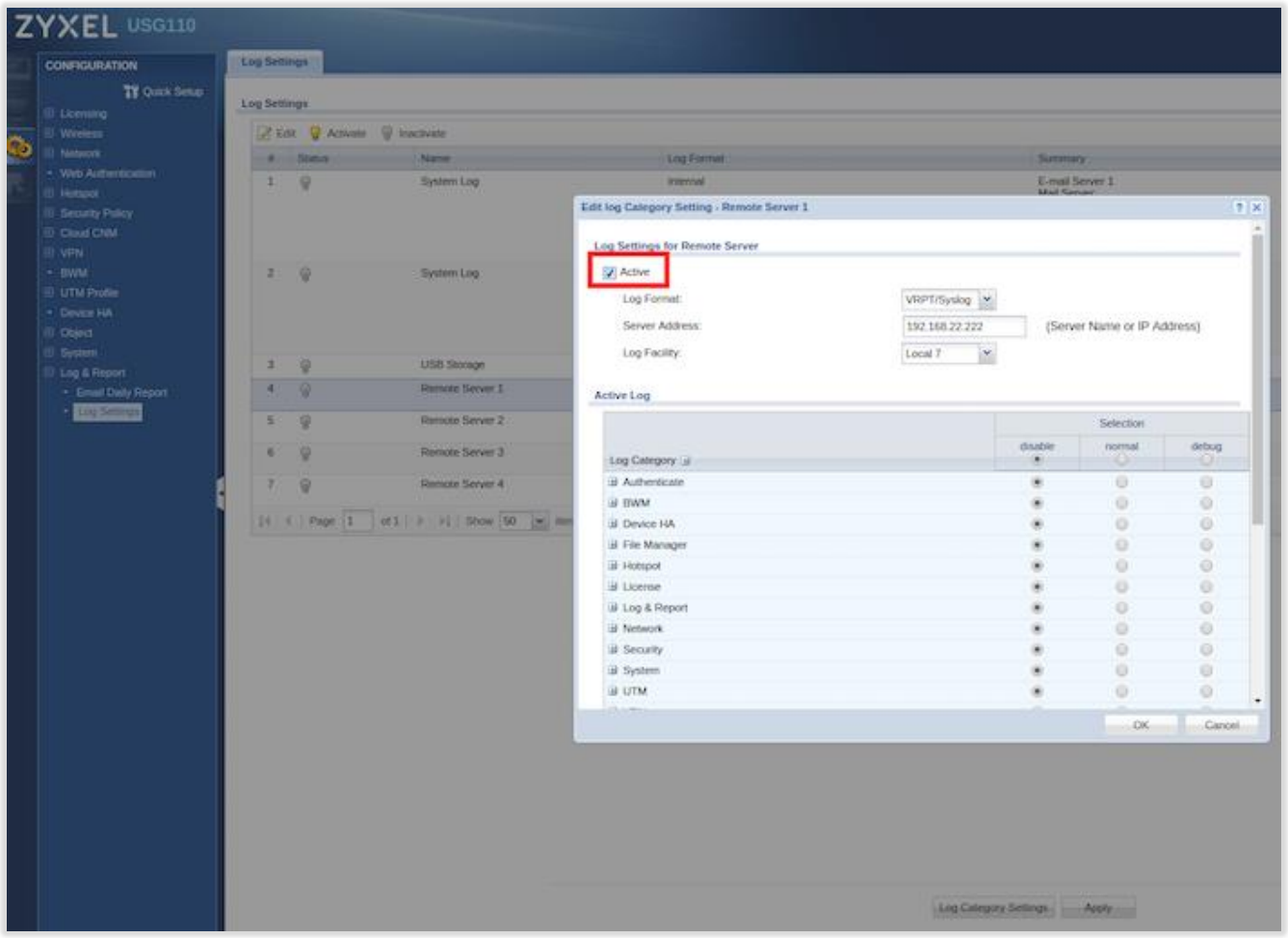

Figure 2