Integrating Check Point FireWall-1 Monitoring

https://campus.barracuda.com/doc/96767777/

This information is from Check Point.

Introduction

Syslog (System Logging Protocol) is a standard protocol used to send system log or event messages to a specific server, the syslog server.

The syslog protocol is enabled on most network devices, such as routers and switches.

Syslog is used by many log analysis tools. If you want to use these tools, make sure Check Point logs are sent to from the Security Gateway to the syslog server in syslog format.

Check Point supports these syslog protocols: RFC 3164 (old) and RFC 5424 (new).

These features are not supported: IPv6 logs and Software Blade logs.

Configuring Security Gateways

By default, Security Gateway logs are sent to the Security Management Server.

You can configure Security Gateways to send logs directly to syslog servers.

Important - Syslog is not an encrypted protocol. Make sure the Security Gateway and the Log Proxy are located close to each other and that they communicate over a secure network.

To Define Syslog Server Objects in SmartConsole

1. With **SmartConsole**, connect to the **Management Server**.
2. In the left navigation panel, click **Gateways & Servers**.
3. To create the Host object, in **Object Explorer**, click **New** > **Host**.
4. Enter the following information in these fields:
    - **Name** - Enter a unique name.
    - **IPv4 address** - Enter the correct IPv4 address of the syslog server.
    - **IPv6 address** - Optional: Enter the correct IPv6 address of the syslog server. This requires the IPv6 Support be enabled on the Security Gateway.

5. Click **OK**.
6. To create the Syslog Server object that represents the Syslog server, in **Object Explorer**, click **New** > **Server** > **More** > **Syslog**.
7. Enter the following information in these fields:
    - Name - Enter a unique name.
    - **Host** - Select an existing host or click New to define a new computer or appliance.
    - **Port** - Enter the correct port number on the syslog server (default = 514).
    - **Version** - Select **BSD Protocol** or **Syslog Protocol**.
8. Click **OK**.
9. Close the **Object Explore**r.

To Select the Configured Syslog Server Objects in the Security Gateway object

1. Double-click the **Security Gateway** object.
2. In the left tree, click **Logs**.
3. In the **Send logs and alerts to these log servers** table, click the green (+) button to select the Syslog Server object(s) you configured earlier.
4. Click **OK**.
5. Install the policy.

- You can configure a Security Gateway to send logs to multiple syslog servers.
- All syslog servers selected in the Security Gateway object must use the same protocol version: BSD Protocol or Syslog Protocol.
- You cannot configure a Syslog server as a backup server.

To Configure the Logging Properties of the Security Gateways

In Cluster, you must configure each Cluster Member separately.

The fwsyslog_enable kernel parameter enables or disables the Syslog in Kernel feature on Security Gateways:

- Value 0 = Disabled (default)
- Value 1 = Enabled

You can enable or disable the Syslog in Kernel feature temporarily (until the Security Gateway reboots), or permanently (survives reboot).