Example - Configure a Syslog Proxy and CC Syslog Server

https://campus.barracuda.com/doc/73719512/

The following example describes the essential settings for the syslog proxy service (on the box) and the CC syslog server (on the box level of the CC). For more in-depth information see How to Configure Syslog Streaming.

- Log message streaming using TCP&UDP (non SSL)
- Log message streaming using SSL
- Relaying of log messages using SSL

Log Message Streaming using TCP&UDP (non SSL)

To specify the settings for log message streaming using TCP&UDP, proceed as follows:

Configuration of Syslog Streaming

1. Log into the Barracuda Firewall Control Center at box level (select **Box** in the login window).
2. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
3. Click **Lock**.
4. In the **Basic Setup** section, set the parameter **Idle Mode** to **no**.
   Though not using an SSL certificate, leave the parameter **Use Box Certificate/Key** set to **yes**. If the setting is changed to **no**, the parameters **SSL Private Key** and **SSL Certificate** become mandatory, as it is assumed that another certificate than the box certificate will be used. With all other parameters set properly, availability of a certificate will be ignored.
5. From the **Configuration** menu on the left, select **Logdata Filters**.
6. Click the **+** icon, enter a descriptive name and click **OK**.
7. In the section **Affected Box Logdata** and **Affected Service Logdata**, specify the log file types to be sent to the CC Syslog server.
8. Click **OK**.
9. From the **Configuration** menu on the left, select **Logstream Destinations**.
10. Click the **+** icon, enter a descriptive name and click **OK**.
11. In the **Destination Address** section set the parameter **Remote Loghost** to **explicit-IP**. This setting causes the log files to be streamed to the CC-Server IP.
12. Set the parameter **Use SSL Encapsulation** to **no**.
13. Set parameter **Add Range/Cluster** Info to **yes** to maintain the log files structure Range/Cluster/Box. If set to **no**, the log files are saved in a directory labelled with the box' name below the **Local Log Directory** defined on the CC Syslog server (see below).
14. Click **OK**.
15. From the **Configuration** menu on the left, select **Logdata Streams**.

16. Click the **+** icon, enter a descriptive name and click **OK**.
17. Define combinations of **Log Filters** and **Log Destinations** in this section. Generally, this feature is useful when:
    1. Log files are streamed to multiple destinations.
    2. Streaming is not required continuously for all log file types.

    Through setting parameter **Active Stream** to **no**, streaming can be interrupted at all times.
18. Click **OK**.
19. Click **Send Changes** and **Activate**.

Configuration of CC Syslog Service

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > servicename (msyslog) > CC Syslog Service**.
2. Click **Lock**.
3. In the **Basic Setup** section, set the parameter **Idle Mode** to **no**.
4. Create **Service Key** and **Service Certificate**.

   Creation is mandatory, though key and certificate are not used without SSL encapsulation.
5. Set parameter **Support Trusted Data Reception** to **no**.
6. Set parameter **Store on Disk** to **yes** to enable saving of received log messages to harddisk.
7. From the **Configuration Mode** menu on the left, select **Active View** (if not already selected).
8. From the **Configuration** menu on the left, select **Local Storage**.
9. Specify the **Local Log Directory** as saving location for received log messages. The default path is */var/phion/mlogs* . You may leave the default settings.
10. Click **OK**.
11. Click **Send Changes** and **Activate**.

Log Message Streaming using SSL

To configure log message streaming using SSL proceed as follows:

Configuration of Syslog Streaming

1. Log into the Barracuda Firewall Control Center at box level (select **Box** in the login window).
2. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
3. Click **Lock**.
4. In the **Basic Setup** section, set the parameter **Idle Mode** to **no**.
5. Set parameter **Use Box Certificate/Key** to **yes**.
6. From the **Configuration** menu on the left, select **Logdata Filters**.
7. Click the **+** icon, enter a descriptive name and click **OK**.
8. In the section **Affected Box Logdata** and **Affected Service Logdata**, specify the log file types to be sent to the CC Syslog server.

9. Click **OK**.
10. From the **Configuration** menu on the left, select **Logstream Destinations**.
11. Click the **+** icon, enter a descriptive name and click **OK**.
12. In the **Destination Address** section set the parameter **Remote Loghost** to **Barracuda CC Control**. This setting causes the log files to be streamed to the CC-Server IP.
    With **Remote Loghost** set to **Barracuda CC Control**, the Master Certificate of the CC is automatically used as Remote Certificate, that is Peer SSL Certificate. Importing the Master Certificate into the Peer SSL Certificate field is thus not necessary.
13. Configure the parameter **Loghost Port** to match the value in parameter **SSL Listen Port** (Trusted Data Reception view) on the CC Syslog Server. By default, port 5143 is used for SSL connections.
    Do not use port 5144, as this setting only works when log messages are streamed without SSL Encapsulation. The log file data will arrive corrupt on the CC Syslog Server if port 5144 is used.
    If you change the port assignment to another port than the default 5143, adjusting the local firewall rule set might become necessary.
14. Set parameter **Transmission Mode** to **TCP**.
15. Set parameter **Add Range/Cluster** Info to **yes** to maintain the log files structure *Range/Cluster/Box*. If set to **no**, the log files are saved in a directory labelled with the box' name below the **Local Log Directory** defined on the CC Syslog server.
16. Click **OK**.
17. From the **Configuration** menu on the left, select **Logdata Streams**.
18. Click the **+** icon, enter a descriptive name and click **OK**.
19. Define combinations of **Log Filters** and **Log Destinations** in this section.
20. Click **OK**.
21. Click **Send Changes** and **Activate**.
    Creation is mandatory, though key and certificate are not used without SSL encapsulation.

Configuration of CC Syslog Service

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > servicename (msyslog) > CC Syslog Service**.
2. Click **Lock**.
3. In the **Basic Setup** section, set the parameter **Idle Mode** to **no**.
4. Create **Service Key** and **Service Certificate**.
   Creation is mandatory, though key and certificate are not used without SSL Encapsulation.
5. Set parameter **Support Trusted Data Reception** to **yes**.
6. Set parameter **Store on Disk** to **yes** to enable saving of received log messages to harddisk.
7. From the **Configuration Mode** menu on the left, select **Active View** (if not already selected).
8. From the **Configuration** menu on the left, select **Support Trusted Data Reception**.
9. Configure the parameter **SSL Listen Port** to match the value in parameter **Loghost Port** (**Logstream Destinations** view) on the Syslog Proxy. By default, port 5143 is used for SSL connections. Pay attention to the limitations concerning port choice as described above.
10. Set parameter **Service Certificate** to **USE_MC_SSL_Cert**. With this setting, boxes

can authenticate themselves at the CC Syslog Server using their box certificates.
11. Set parameter **Client Authentication** to **verify_peer_with_locally_installed_certificate** . The setting causes the box certificate to be authenticated against the CC certificate.
12. Import the box certificate of every box, whose log messages are collected by the CC Syslog Server, into the **Trusted Clients** field.
13. From the **Configuration** menu on the left, select **Local Storage**.
14. Specify the **Local Log Directory** as saving location for received log messages. The default path is */var/phion/mlogs* . You may leave the default settings.
15. Click **OK**.
16. Click **Send Changes** and **Activate**.

Relaying of Log Messages Using SSL

Relaying follows the streaming of log messages. Relaying can be configured with or without SSL encapsulation, regardless of encryption settings defined for streaming. Log messages can be relayed to an external host after they have been written to disk on the CC Syslog Server or they can immediately be passed to the external host without this intermediate step. The following example settings can succeed both of the configurations described above. To configure relaying using SSL proceed as follows.

Syslog Proxy Configuration

No further settings are required on the box where log messages are generated.

A configuration requirement exists, though, regarding the setting of the parameter **Add Range/Cluster Info** in the **Log Data Tagging** section as it directly influences usage of the parameter **Filter Box Affiliation** in the **Relay Filters** view of the CC Syslog Server. See below for details.

Configuration of CC Syslog Service

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > servicename (msyslog) > CC Syslog Service**.
2. Click **Lock**.
3. In the **Basic Setup** section, set the parameter **External Relaying** to **yes**.
4. Create **Service Key** and **Service Certificate**.
   Export the SSL Certificate to a file and make it available for the external host. The external host has to import the certificate in order to authenticate itself against the CC Syslog Server (see also parameter **Destination SSL Certificate** below with destination types using SSL).
5. From the **Configuration Mode** menu on the left, select **Relaying Setup**.

6. From the **Configuration** menu on the left, select **Support Trusted Data Reception**.
7. Set parameter **SSL Peer Authentication** to **verify_peer_with_locally_installed_certificate**.
8. From the **Configuration** menu on the left, select **Relay Filters**.

   Configuration options in the **Relay Filters** view have a similar function to the filtering options specified through the **Logdata Filters** view in the **Syslog Proxy** configuration. Here they allow defining the log messages, which are to be relayed, by their type. The effect of parameter **Filter Box Affiliation** set to **yes** is directly dependant of parameter setting **Add Range/Cluster Info** in the **Log Data Tagging** section of the **Syslog Proxy** (see above). Reason for this is, that for example relaying through a **Range-Cluster-Box** hierarchy structure can only work, if Range-Cluster-Box information has originally been maintained during log file streaming.
   Using Filter Box Affiliation demands specification of Originator Systems. This demand can only be satisfied, if Range/Cluster/Box information has been maintained during log message streaming.
9. Specify the parameter **Affected Box Logfiles / Affected Service Logfiles**. The all-embracing method easiest to configure, is to relay Affected Box Logfiles and Affected Service Logfiles. If unfiltered relaying is not desired, choose **Selection** in the **Affected Box/Service Logfiles** parameters and select the log file types to be relayed.
10. Configure the parameter **SSL Listen Port** to match the value in parameter **Loghost Port** (**Logstream Destinations** view) on the Syslog Proxy. By default, port 5143 is used for SSL connections. Pay attention to the limitations concerning port choice as described above.
11. Specify the parameter **Special File Patterns** (This setting allows setting relay filters on terms of filtering for character strings (for example *box_Event*).
12. From the **Configuration** menu on the left, select **Relay Destinations**.

Using Destination Type Stream SSL to Passive Destination:

The connection type **Stream plaintext to passive destination** is used when log messages are relayed without SSL Encapsulation.

- Set parameter **Connection Type to Stream SSL to passive destination**, if the destination the CC Syslog server is relaying to, is passively awaiting log message delivery.
- In the **Destination SSL Certificate** section, import the destination server's certificate in this place - define the destination IP through the parameter **Destination SSL IP**.

  Connection type using SSL require certificate exchange with the external client/host messages are relayed to.
- From the **Configuration** menu on the left, select **Local Storage**.
- In the **Destination SSL IP** section, define the connection port for relaying through the parameter **Destination SSL Port**. The standard port range for this purpose spans ports 5244 to 5253.
- Set the parameter **Keep Structural Info** to **yes** to maintain the original names of the relayed log files.

Using Destination Type Stream SSL to Active Destination:

- Set parameter **Connection Type** to **Active SSL connect by destination** if the external host is actively querying for log messages.

- Specify a Local SSL Port (parameter requires **Advanced View** in order to be available). The connection between CC Syslog Server and destination system will be established on this port. The standard port range for this purpose spans ports 5244 to 5253.
  In case the CC Syslog Server has been configured to Sync to HA Partner, do not specify the same port as is defined in the parameter SSH Listen Port in the HA Synchronization view.
- In the **Destination SSL Certificate** section, set the parameter **Keep Structural Info** to **yes** to maintain the original names of the relayed log files.
  Connection types using SSL require certificate exchange with the external client/host messages are relayed to. Import the remote SSL client's certificate in this place.

13. From the **Configuration** menu on the left, select **Relay Streams**.
14. Define combinations of **Relay Destinations** and **Relay Filters** in this section. Generally, this feature is useful when log files are relayed to multiple destinations and/or relaying is not required continuously for all log file types.
    Through setting parameter **Active** to **no**, relaying can be interrupted at all times.
15. Click **OK**.
16. Click **Send Changes** and **Activate**.