NXLog

Why do we need NXLogs

NXLog is a log collection and processing platform used in IT and cybersecurity environments to gather, normalize, and forward logs from systems, devices, and applications.

This section explains how to configure NXLog to send the **IP address–to–username association** to the **NWB proxy**.

Overview

The NWB maintains a database that maps IP addresses to authenticated users.

When a user browses the internet, the NWB proxy uses this mapping to associate browsing activity with the correct username **without requiring the user to authenticate to the proxy**.

This method is known as **Transparent Authentication**

How It Works

1. Users authenticate to Active Directory (Windows logon).
2. NXLog collects logon events from domain workstations or servers.
3. NXLog extracts:
    a. username
    b. assigned IP address
    c. logon timestamp
4. NXLog forwards this information to the NWB proxy.
5. NWB builds and maintains an IP ↔ user mapping database.
6. When web traffic passes through the proxy:
    a. the source IP is matched
    b. browsing activity is linked to the user

Benefits

User-based policy enforcement

Create proxy rules using:

- usernames
- Active Directory groups
- departments or roles

No proxy authentication prompts

Users browse normally without additional login prompts.

Accurate activity reporting

Generate reports showing:

- user browsing activity
- security violations by user
- compliance and audit trails

Simplified rule management

Policies can follow users instead of devices or IP addresses.

Use Cases

- Enforcing acceptable-use policies by AD group
- Blocking categories for specific departments
- Investigating security incidents by user identity
- Compliance reporting and audit requirements

Next Section

The following section provides step-by-step instructions to configure NXLog to extract logon events and forward IP–user association data to the NWB proxy.

Installing and configuring NXLogs

Install NXLOG software on the customer network server.

The NXLOG site can be found here:

http://nxlog.org/

The community edition software should be downloaded and installed on the windows server:

http://nxlog.org/products/nxlog-community-edition/download

Configure NXLOG to send event logs to Network Box

Now configure the software using the code on the next page. Replace the x.x.x.x with the correct IP of the Network Box LAN.

```
<<<<<<<<<<<<<<<<CUT / PASTE BELOW HERE>>>>>>>>>>>>>>>>>>>
# Path to the NXLOG software directory
define ROOT C:\Program Files (x86)\nxlog

Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
LogFile %ROOT%\data\nxlog.log

<Extension _syslog>
  Module     xm_syslog
</Extension>

<Extension json>
 Module  xm_json
</Extension>

<Input in>
 Module     im_msvistalog
</Input>

<Output out>
  Module     om_tcp
  Host       X.X.X.X  (replace with the LAN IP of your NWB)
  Port       514
 Exec if not ($EventID == 4624) drop();
 Exec      $Message = to_json();
 Exec      to_syslog_bsd();
</Output>

<Route 1>
  Path      in => out
</Route>

#<EOF>#
```