Network Monitoring - nzyme Documentation

Archived: 2026-04-06 03:33:30 UTC

What is Network Monitoring?

Nzyme works to protect your WiFi networks by consistently comparing the expected state of access points with the observed reality. For instance, if you configure nzyme with a list of all your access points, the activation of an additional access point by an attacker would prompt an alert from nzyme.

Given the WiFi protocol's inherent characteristics, some monitored parameters are relatively easy to spoof, while others are notably more difficult to manipulate. The reliability and specific characteristics of each monitoring parameter type are further explained below. Despite the potential ease of circumventing certain alarms, it's still recommended to enable them, as they add additional layers of defense against potential attackers.

Configuring a Monitored Network

You can create as many monitored networks as you wish from the *WiFi - Monitoring* page. Note that you have to either be a super administrator, organization administrator or a tenant user with the *Manage Monitored WiFi Networks* feature permission.

The recommended workflow is as follows:

- Create a new monitored network for the SSID you wish to monitor
- Build the expected BSSID configuration based on your WiFi inventory. If you don't have access to a complete inventory of access points serving your network, you can copy BSSIDs from the *WiFi - Access Points* page. It is important to cross-check the BSSIDs you add against any sort of confirmation that they are indeed yours to avoid adding hostile BSSIDs in case of an already ongoing attack.
- Copy and add expected fingerprints of your BSSIDs from the *WiFi - Access Points* page to the monitoring configuration.
- Repeat this process for expected channels and security suites.
- Enable the monitored network and watch alerts for any deviations from the expected configuration. In case of alerts, decide if you have to add the detected deviated value to the monitored network configuration. You can delete or mark the alerts as resolved after you remediated them.

Configuring Alerting

You can enable/disable any of the monitor detections from the monitored network details page. For example, if you are not interested in alerts for mismatched fingerprints, you can disable that alert entirely.

Expected BSSIDs / Access Points

This list must include all BSSIDs (MAC addresses) of access points serving your network. For instance, if you have five access points, you must include the addresses of all these access points here.

An alert will be triggered if any other BSSID advertises your network.

BSSIDs are fairly easy to spoof. A sophisticated attacker is likely to utilize an existing and expected BSSID to avoid raising any alerts.

Expected Fingerprints

The nzyme routines assign a fingerprint to each recorded BSSID. You are required to list all fingerprints of an expected BSSID (ordinarily, it should only have a single fingerprint). Should nzyme observe any fingerprint other than those listed, an alarm will be triggered.

You can find all fingerprints on the nzyme access point details pages.

Fingerprints are challenging to spoof, as they are typically based on hardware-defined characteristics of wireless frames. Except for very sophisticated attackers, it's unlikely that anyone could accurately mimic your expected fingerprints in attack scenarios.

However, be aware that false positives can occur if there are hardware changes to your access points, which could result in altered fingerprints.

Expected Channels

You must list all channels on which your network operates. Should a frame advertising your network on any channel not listed be observed, an alarm will be triggered.

You can find all observed channels on the nzyme access point details pages.

However, it's worth noting that attackers can effortlessly observe the channels your network operates on and restrict their attacks to these same frequencies to avoid detection.

Note that some access points will dynamically change the channels they are operating on and can end up using almost any channel of the WiFi spectrum. In that case, it is recommended to disable the *Expected Channels* detection entirely.

Expected Security Suites

Similar to the expected channels, you must list all expected security suites (usually just one). If a frame advertising your network with any suite not listed is observed, an alarm will be triggered.

You can find all observed security suites on the access point details pages within nzyme.

However, it's crucial to note that attackers can easily mimic the same security suites used by your networks.

Signal Tracks

Even if an attacker is perfectly mimicking your access point, there is a parameter that is almost impossible to spoof: Signal strength. Nzyme has a history of the recorded signal strength of your access points. Any attacker not perfectly positioning their signal source to match the signal characteristics of your legitimate access point, will very likely create a second signal track that nzyme will detect and alert one.

This detection requires no configuration. Nzyme will always alert if any monitored BSSID is recorded with more than one signal track.

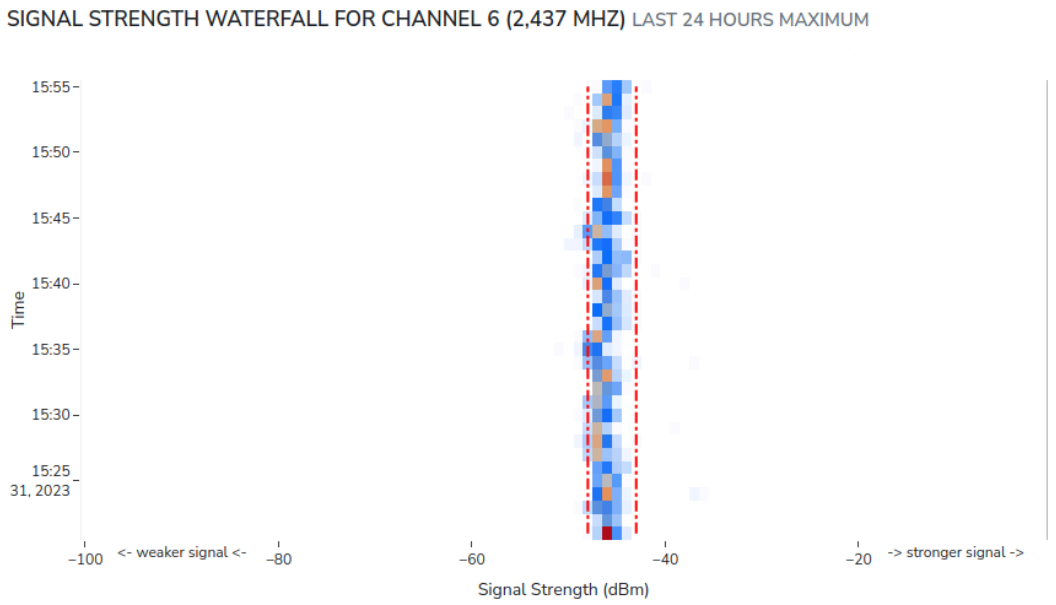
Warning

The signal track detection will only run for data from monitored/expected channels of the network. It would make no sense to monitor signal tracks of unexpected channels and an attacker operating on such channels would trip the *unexpected channel* alert.

Warning

The signal track alert is looking at the recorded tracks of the last 8 hours. Such an alert is likely to re-trigger if you delete it or mark it as resolved until no second track is visible for the last 8 hours. This is an area of future improvement.

You can see the signal track of each access point on the access point details page:



A single signal track

The red dashed/dotted box represents a single track.

Configuring the Track Detector

The default track detector configuration will not always reliably detect single tracks. It can misidentify tracks under certain circumstances and split up a single legitimate track into multiple tracks or identify mutliple tracks as a single one, leading to false positive or missed alerts.

In that case, **super administrators** and **organization administrators** can use the track detector configuration to influence how nzyme detects tracks:

1. Click on the *Configure Track Detector* button under the signal track chart
2. Configure the parameters. Make sure to read the parameter descriptions to understand what each one influences.
3. Save the configuration. It will be applied immediately and the signal track chart will reflect the changes you made.

The custom configuration is applied to the specific combination of BSSID, SSID, channel and tap, because signal characteristics can wildly differ based on those parameters. Make sure to apply the custom configuration to as many combinations of those parameters as necessary.

Disconnection Anomalies

Deauthentication and disassociation attacks are a very common part of malicious WiFi campaints. In nzyme, those frames are collectively called *disconnection* frames. You can learn more about it on the Disconnection Activity page.

Nzyme can count disconnection frames adressed at or originating from access points of a monitored network and alert you in case of detected anomalies.

To enable this functionality, you have to select and configure an anomaly detection method from the monitored network page.

Anomaly Detection Method: Static Threshold

The *Static Threshold* anomaly detection method does often make the most sense because disconnection frames can be very rare and many non-supervised anomaly detection methods are not good at dealing with such a small sample set.

Observe how many disconnection frames are recorded over a period of 24 hours and set a threshold just above the maximum. In many environments it is common to see long periods of no activity at all, and small bursts of 10 or more frames. Attacks can generate hundreds or thousands of frames per minute, depending on how stealthy the threat actor operates.

More anomaly detection methods will follow in the coming nzyme releases.

Client Monitoring

Similar to SSID Monitoring, you can alert on any unapproved clients connecting to a monitored network.

A difference to SSID monitoring is that client monitoring always happens in the scope of a monitored network, meaning that it alerts on clients that are observed as connected to any BSSID that is part of the configuration of a monitored network.

Configuration

The client monitoring functionality offers the following configuration options per monitored network:

Configuration	Default	Description
Is monitoring enabled	false	Clients are only collected and added to the list of known client if `enabled`. This also disables any alerting for new clients because no new clients are discovered.
Is event generation enabled	false	Events (Alerts) are only triggered if `enabled`. See also *Training Period* below.

Approving Clients

Approving a client will keep it from triggering any alerts and resolve all related alerts within a few minutes.

Revoking the approval of a client will make it trigger alerts again until ignored, deleted or approved.

Ignoring Clients

Ignoring a client will keep it in the list of known clients, keep it from triggering any alerts but not mark it as approved. Existing alerts will automatically resolve within a few minutes.

Deleting Clients

Deleting a client will make it disappear from the list and all related alerts will automatically resolve within a few minutes. The client will re-appear as a new, unapproved client the next time it is observed by nzyme.

Training Period

You can create a training period for the system to learn about all clients in range, approve or ignore as required and then start to enable event/alert creation:

1. Set *Is monitoring enabled* to `true`.
2. Keep *Is event generation enabled* set to `false`. This will make sure no client monitoring events/alerts are created.
3. Wait several hours to make sure that all clients in range are listed in the table of known clients.
4. Approve, ignore and delete known clients as applicable.
5. Set *Is event generation enabled* to `true`. No client monitoring alerts should be triggered if you approved, ignored, or deleted all clients in the previous step.

Retention Cleaning

Nzyme will automatically delete all known clients that have not been seen in the previous 30 days.

Source: https://docs.nzyme.org/wifi/monitoring/network-monitoring/