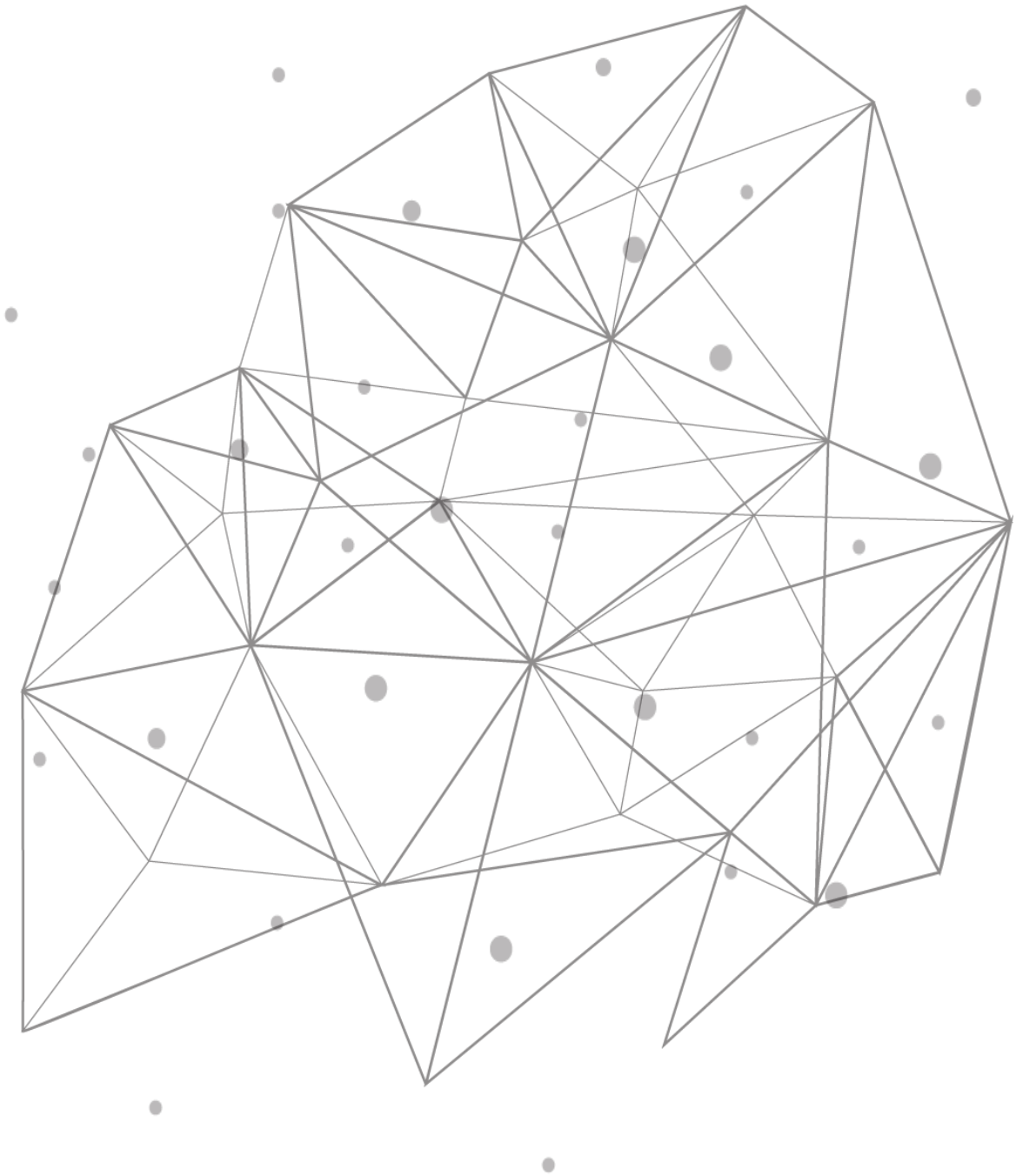
# TCPWave DDI – Force Recheck Monitoring



# Introduction

Monitoring and Alerting are the two vital components of DNS protection for organizations since DNS is the heart of any network infrastructure. The organization's business is at stake, and revenue declines if the DNS malfunctions. Any downtime due to DNS issues is detrimental to the organization's brand. Therefore, it is essential to monitor DNS server performance and alert the network administrators to help head off problems that could affect the end-user experience. This white paper provides insights on re-checking an alert within the TCPWave IPAM application.

# Force Recheck

The alerts platform keeps the network administrators in the loop if the appliances ever receive an unusual number of requests that could flag a potential DNS attack. In the TCPWave IPAM application, the Force Recheck monitoring option permits the administrators to manually re-invoke a monitoring check and update an alert's status.

When the network administrators perform Force Recheck, the monitoring checks the specified alert and sends the updated alert into the existing notification queue from which notifications are inserted into the database as per the **Monitoring Notification Processing Interval** defined in the Global Policy Management. By default, the processing interval is 2 minutes. Users must refresh the current alarms section to view the latest alert.


Overall, monitoring is a cyclic process that occurs repeatedly and infinitely when left undisturbed. Often, it becomes necessary to force a recheck to keep the infrastructure up and running. The current monitoring

model does the monitoring as per defined schedules, without any manual overrides. Suppose a particular threshold is alerted, and the network command center has resolved the incident management ticket. Instead of waiting for the alert to disappear, the network administrator can perform a force recheck on any alert for which corrective action has been initiated.

When the command center initiates a force recheck instruction, the threshold in question is re-checked immediately. When such a check informs the TCPWave management system that the alerting situation persists, the fault management dashboard continues to have a red alert. On contrary, if the force recheck clears the alerting state of the threshold, then the TCPWave management system observes a change from red to green for that particular alert. In addition to that, the ability to perform the force recheck operation is strictly controlled by the permissions of the TCPWave Identity Administration module.

## Conclusion

With such a robust and powerful monitoring engine embedded as an integral part of the TCPWave IPAM, organizations can dramatically improve their service level agreements and keep their mission-critical services up and running. For a quick demo on enforcing monitoring and enhancing the organization's DNS service availability, contact the TCPWave Sales Team.