Deynao

Oracle monitoring & diagnostics

Network requirements

Flow matrix & diagnostics

Version 1.0.1 · September 2026

Pilot documentation · 100% on-premise

Deynao — Network requirements guide

Audience: Infrastructure, network and security (CISO) teams, IT management

1. Overview & deployment models

Deynao is a **100% on-premise** Oracle monitoring solution. It connects **directly** to Oracle instances over the Oracle Net protocol (TCP), using a **read-only** account, and **never** communicates with the Internet.

Two deployment models:

- **Portable** (workstation): Deynao runs on a workstation and the interface opens locally. **No inbound flow** is required.
- **Server** (Windows service): Deynao runs as a service; the interface can be opened remotely from other machines on the network (inbound port 8000 **optional**).

Flow overview:

Flow	Port	Direction	Required
Deynao → monitored Oracle databases	1521 (or the listener's port)	Outbound	**Yes**
Deynao → SMTP relay (e-mail alerts + daily report)	587 (or 465 / 25)	Outbound	If e-mail alerting is enabled
Admin workstations / probe → Deynao interface	8000	Inbound	Optional (Server model)
Deynao → Internet	—	—	**None**

This document covers **strictly the network prerequisites** to validate before installation, as well as **network diagnostics**. Related topics are covered in their own documents:

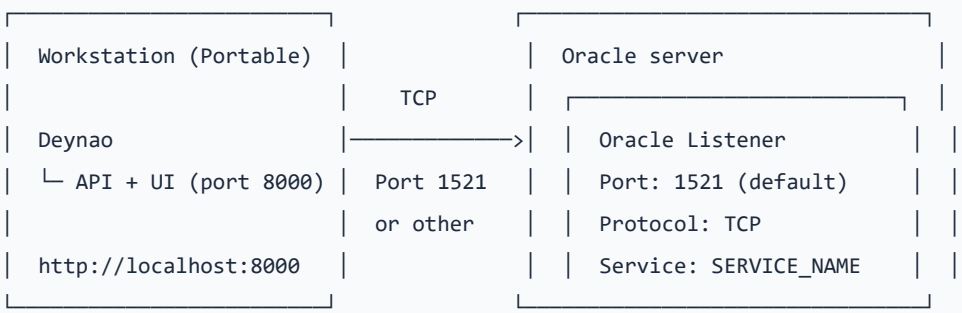
- **SMTP relay configuration** (values, encryption, authentication, FAQ) → *E-mail (SMTP) configuration*.
- **Oracle monitoring account & queried views** → *Oracle Transparency* and the *Windows operations guide* (Oracle account section).
- **Installation & remote access (step-by-step commands)** → *Step-by-step installation*.

2. Network architecture

In both models, the API and interface are served on **port 8000**; connections to Oracle and SMTP are **outbound**.

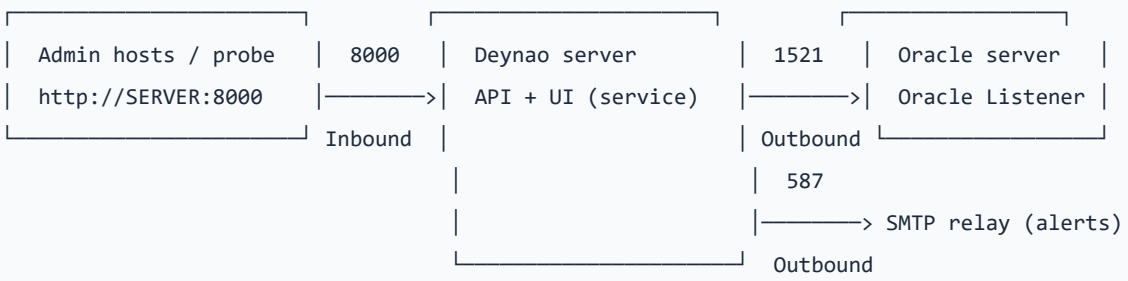
2.1 Portable model (workstation)

The interface opens locally on the workstation. **No inbound connection** is required.



2.2 Server model (Windows service)

Deynao runs as a service on a server. Admin workstations (and the external monitoring probe) can reach the interface remotely through the **inbound port 8000** (optional). Deynao contacts Oracle and the SMTP relay **outbound**.



Key points:

- The Deynao API and interface are served on **port 8000**.
- The **Portable model** requires no inbound flow; the **Server model** opens inbound 8000 only if remote access is wanted.
- Connections to Oracle are **read-only**; no change is required on the Oracle servers.

---

3. Required network flows

3.1 Flow matrix

Source	Destination	Port	Protocol	Direction	Purpose	Required
Deynao server / workstation	Oracle server	1521 (or custom)	TCP	Outbound	Monitoring (read-only)	Yes
Deynao server / workstation	SMTP relay	587 (or 465 / 25)	TCP	Outbound	E-mail alerts + daily report	Yes, if alerting enabled
Admin hosts + monitoring machine	Deynao server	8000	TCP	Inbound	Remote UI + external probe	Optional (Server model)
(none)	Internet	-	-	-	No Internet flow	-

> The **inbound 8000** flow only concerns the **Server model** with remote access (see 3.4). In the **Portable model**, the API and interface stay on the local loopback (`localhost:8000`) and no inbound flow is required.

3.2 Flow opening request template

Use this template to request firewall rules from your network team:

```
NETWORK FLOW OPENING REQUEST
_____________________________________


Application     : Deynao (Oracle monitoring)
Requester       : [Your name]
Date            : [Date]

Source          : [IP or subnet of the Deynao workstation/server]
Destination     : [IPs of the Oracle servers, IP of the SMTP relay]
Ports           : TCP 1521, 1522 (Oracle, adjust per environment)
                  TCP 587 (SMTP, for e-mail notifications)
Direction       : Outbound only (source → destination)
Duration        : Permanent
Justification   : Oracle database monitoring (read-only) and e-mail alert delivery
```

3.3 Multi-environment example

Environment	Server IP	Port	Service Name	Note
DEV	<DEV_HOST>	1521	DEVDB	Development database
TEST / UAT	<TEST_HOST>	1521	TESTDB	Pre-production
PRODUCTION	<PROD_HOST>	1522	PRODDB	Restricted access
DR / Standby	<DR_HOST>	1521	DRDB	Disaster-recovery site

> **Reminder**: each **new monitored database** adds an outbound 1521 flow (or its listener port) to open towards its IP. This is the most common thing forgotten when adding a database.

3.4 Remote access to the interface (Server model): bind & firewall

This section only concerns the **Server model** when you want to open the Deynao interface to other machines on the network. In the **Portable model**, it does not apply.

At startup, Deynao “listens” on a **network address** (the *bind*) and **port 8000**:

Bind	Who can reach Deynao
`127.0.0.1` (default, local)	Only from the server itself.
`0.0.0.0` (all interfaces)	Any machine on the network (via the server name or IP), **if the firewall allows it**.

The `127.0.0.1` default is the **safe default**: until exposure is explicitly decided, nothing is reachable from the network. **The installer does not open the firewall by itself** (a deliberate security choice).

Three distinct levers, not to be confused:

- **The bind** (`install.ps1 -BindAddress 0.0.0.0`) is an **application setting**, applied on the server by the application administrator. It is not a network flow.
- **The host firewall** (a Windows rule on the server) opens port 8000 on the server itself, by the server administrator.
- **The network firewall** (between subnets / VLANs) is governed by the security team (CISO), based on the flow matrix (3.1). Neither the bind nor the host rule changes it.

> The bind concerns **inbound** traffic (who can reach the interface). It changes **nothing** about e-mail alerts, which go **outbound**. A server that sends its alerts fine but whose interface is not reachable from a workstation: that is the bind or the firewall (inbound), not alerting.

The **step-by-step commands** (bind on the network, firewall rule, restricting by source IP) are detailed in the *Step-by-step installation* document.

---

4. Pre-installation validation

4.1 Connectivity tests (Windows PowerShell)

Run these commands from the workstation / server where Deynao will be installed:

```
# Step 1: basic connectivity (ICMP). Note: ping may be blocked —
# a failed ping does not necessarily mean Oracle is unreachable.
ping <DEV_HOST>

# Step 2: TCP connectivity to the Oracle port — THIS IS THE MOST RELIABLE TEST
Test-NetConnection -ComputerName <DEV_HOST> -Port 1521
#   TcpTestSucceeded : True   -> flow open
#   TcpTestSucceeded : False  -> flow blocked (or listener stopped)

# Step 3: test several servers in one command
@("<DEV_HOST>:1521", "<TEST_HOST>:1521", "<PROD_HOST>:1522") |
ForEach-Object {
    $parts = $_.Split(":")
    $result = Test-NetConnection -ComputerName $parts[0] -Port $parts[1] `
              -WarningAction SilentlyContinue
    $color = if($result.TcpTestSucceeded){"Green"}else{"Red"}
    Write-Host "$_ : $($result.TcpTestSucceeded)" -ForegroundColor $color
}
```

4.2 Connectivity tests (Linux / macOS)

Useful if the Portable host runs Linux or macOS (the Deynao server itself runs on Windows).

```
# TCP port (netcat)
nc -zv <DEV_HOST> 1521

# Or without netcat
timeout 5 bash -c 'echo > /dev/tcp/<DEV_HOST>/1521' && echo "OK" || echo "FAILED"
```

4.3 Network pre-installation checklist

```
NETWORK CHECKLIST — DEYNAO PRE-INSTALLATION
_____________________________________________

Deynao machine : _____________________________  Date: _____________
Validated by   : _____________________________

CONNECTIVITY
[ ] The Deynao machine can reach the Oracle servers (Test-NetConnection)
[ ] The Oracle TCP ports (1521/1522/other) are reachable from the machine
[ ] VPN connected if remote access; Oracle subnets routed (see 5.4)
[ ] No proxy needed for Oracle (direct TCP, not HTTP)

FIREWALL
[ ] OUTBOUND TCP rules created (Deynao → Oracle servers)
[ ] OUTBOUND SMTP 587 flow open if e-mail alerting is enabled
[ ] (Server model, remote access) INBOUND 8000 flow agreed with the CISO

ORACLE SIDE (prerequisite for the TCP test to succeed)
[ ] The Oracle Listener is started on the target server(s)
[ ] The Oracle service name(s) are confirmed: ____________________

Signature : _____________________________  Date: _____________
```

> The **Oracle monitoring account** (creation, read-only privileges) is not a network prerequisite: it is described in *Oracle Transparency* and in the *Windows operations guide*.

---

5. Network diagnostics

Deynao gives the first symptom in its interface; `Test-NetConnection` (from the right machine) confirms it. General rule: a flow is “not open” when the TCP test fails **from the source that should have access**, while the destination service is up.

5.1 Symptom → flow → decisive test

Symptom in Deynao	Flow involved	Decisive test (from...)
A database stays "unreachable" (DPY-6005 / ORA-12541 / timeout) although it is up	**Outbound Oracle 1521**	**Deynao server**: `Test-NetConnection <DB_IP> -Port 1521` . `False` = flow blocked (or listener stopped).
Alert raised but no mail received, and the send log shows "Failed" (SMTP timeout or refusal)	**Outbound SMTP 587**	**Deynao server**: "Check connection" button (Settings → alerting) or `Test-NetConnection <SMTP> -Port 587` .
Interface unreachable from a workstation (but OK locally on the server)	**Inbound 8000** (bind or firewall)	**From the workstation**: `Test-NetConnection <SERVER_IP> -Port 8000` , then discriminate (below).

Discriminating inbound 8000 (bind, host firewall or network firewall):

1. On the server: `Get-NetTCPConnection -LocalPort 8000 -State Listen | Select-Object LocalAddress` .
   - `127.0.0.1` : this is the **bind** — re-run `install.ps1 -BindAddress 0.0.0.0` (see 3.4 and *Step-by-step installation*).
   - `0.0.0.0` : bind correct, look at the firewall side.
2. Test from a machine on the **same subnet** as the server:
   - Also fails: **host firewall** (the server's Windows) → add the inbound 8000 rule.
   - Works from the same subnet but not from **another**: **network firewall** between subnets (CISO).

5.2 Network error codes

Code	Message	Likely cause	Action
ORA-12170	TNS:Connect timeout occurred	Server/port unreachable — network, VPN or firewall	`Test-NetConnection` ; check VPN and firewall rules
ORA-12543	TNS:destination host unreachable	Unreachable IP address	Check IP, routing, VPN
TNS-12535	TNS:operation timed out	Connection established but response too slow	Check network latency and server load
ORA-12541	TNS:no listener	The Oracle listener is stopped (the TCP port answers, but nothing is listening)	Contact the DBA (`lsnrctl start`)
ORA-12514	TNS:listener does not know of service	Wrong service name or instance stopped	Check the service name with the DBA

> **Authentication or privilege** errors (ORA-01017 credentials, ORA-28000 locked account, ORA-28001 expired password, ORA-01031 privileges) are **not network problems**: once the TCP connection is established, they belong to the Oracle account. See the *Windows operations guide* (troubleshooting) and *Oracle Transparency*.

5.3 Decision tree (network)

```
Connection fails
│
├── ping server → TIMEOUT
│   └── Network/VPN problem → check the VPN, contact the network admin
│
├── ping OK, but Test-NetConnection port → FAILED
│   └── Port blocked by a firewall → request the TCP flow opening (see 3.2)
│
├── Test-NetConnection port → OK, but ORA-12541
│   └── Oracle listener stopped → contact the DBA
│
├── Test-NetConnection port → OK, but ORA-12514
│   └── Wrong service name / instance stopped → check with the DBA
│
└── Test-NetConnection port → OK, connection established
    └── The network is fine. Any refusal belongs to the Oracle account
        (credentials, privileges) — see Oracle Transparency.
```

5.4 VPN: route the Oracle subnets (split tunnel)

The network issue that most often breaks monitoring when working remotely: a **split-tunnel** VPN only routes "corporate" traffic through the tunnel. **The Oracle servers' subnets must be included in the tunnel routes**, otherwise direct TCP connections to the Oracle port fail (`ping` and `Test-NetConnection` time out) while web applications (which go through a proxy) keep working.

- **Full tunnel**: works if the Oracle subnets are routed.
- **Split tunnel**: the Oracle subnets **must** be added to the tunnel routes.
- **Multiple VPN profiles** (per environment): make sure the profile in use routes **all** the Oracle subnets to be monitored.

If connectivity drops **after a VPN client update**, it is usually the tunnel routing table that changed: ask the network administrator to restore routing to the Oracle subnets (reuse the request template in section 3.2).

---

*This document is part of the Deynao deployment kit. It is intended for the client's infrastructure and security team, to validate **before** installation.*