Exposing a web service to the Internet

> **Who this page is for** — the PI and the technical administrator of a VM hosted by DCSR who want to make a web service reachable from the Internet. **To start the request**: email `helpdesk@unil.ch` — see section 2.

1. In short

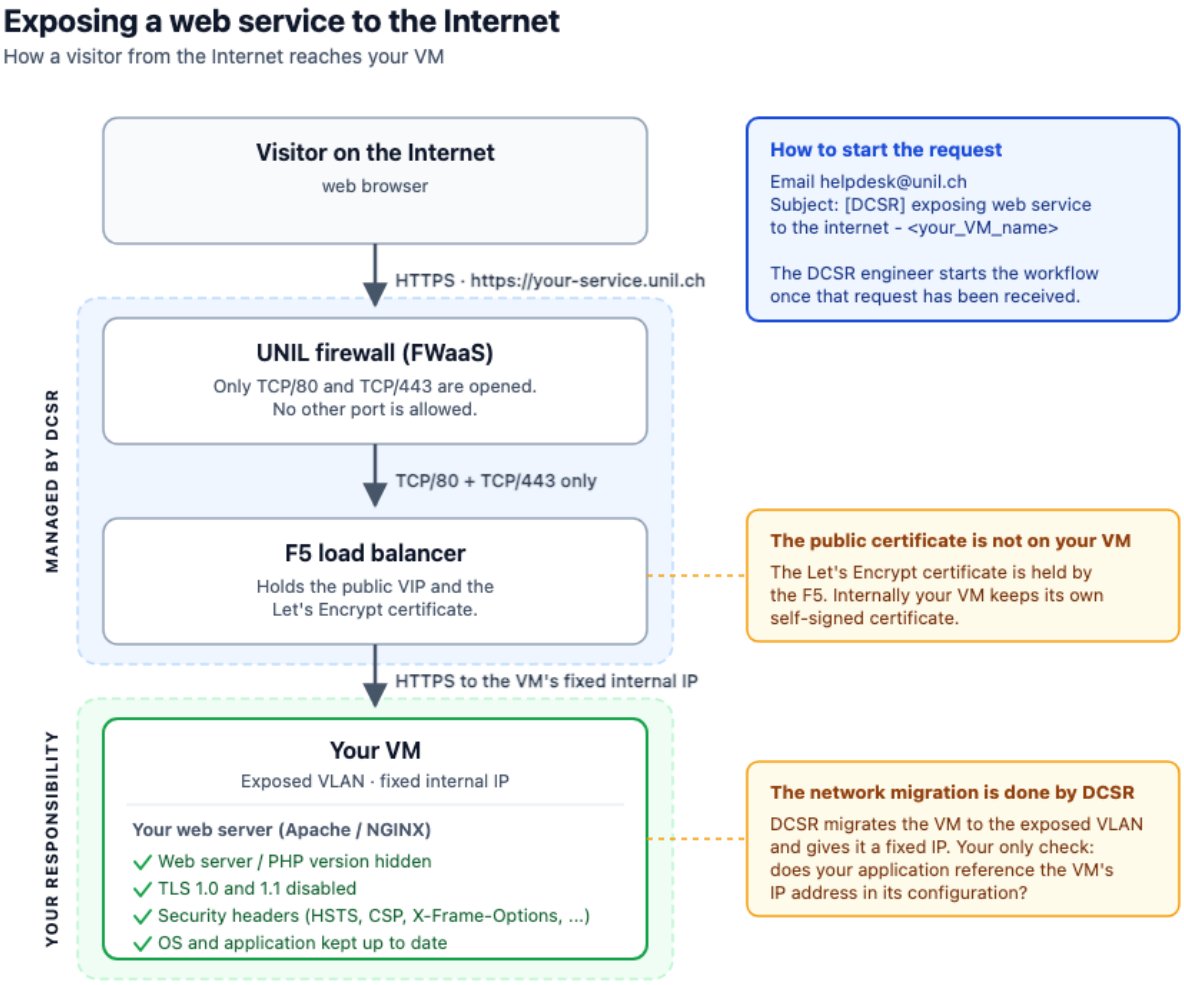
Question	Answer
Which ports can be exposed?	**TCP/80 and TCP/443 only.** No other port (SSH, 8080, databases, ...) is allowed.
Which path does the traffic take?	Internet → UNIL firewall (FWaaS) → F5 load balancer → your VM.
Who provides the public certificate?	A Let's Encrypt certificate held by the F5, not by your VM.
What changes on my VM?	DCSR migrates it to a dedicated VLAN and gives it a fixed internal IP.
What do I have to do?	Harden the web service, fix the vulnerabilities found by the scan, and keep that level over time.

2. How to start the request

> **Send an email to** `helpdesk@unil.ch` with the subject line: `[DCSR] exposing web service to the internet - <your_VM_name>`
>
> In the body, give:
>
> - **a short description of the web service you want to expose** (a few words are enough);

> - **the public DNS name you want users to type**, of the form `https://<your_service>.unil.ch`.
>
> This creates an Otobo ticket. **The DCSR engineer starts the workflow once that request has been received** — nothing happens before it.

3. How a visitor reaches your VM



Only one inbound path exists: Internet → Firewall → F5 → VM. Neither SSH nor any other port is exposed to the Internet.

The key point: **two components are not yours** (the firewall and the F5, managed by DCSR), and **one is your responsibility** — your VM and the web service running on it. The security level of the whole chain is the security level of your VM.

4. Prerequisites before requesting

☐ The web service works and has been tested **inside the UNIL network** (including HTTPS) via `https://dcsrs-<vmname>.ad.unil.ch`.

☐ The VM is up to date (OS + application).

☐ A **technical administrator** is identified and available throughout the procedure — the PI can take on that role.

☐ The **PI** is identified and will fill in the FWaaS form at the end of the process.

☐ The desired public URL has been chosen: `xx.unil.ch`.

5. What going public means for your VM

The network migration is handled by DCSR. Your VM is migrated to the exposed VLAN and given a fixed internal IP. You have nothing to do for that migration itself.

One thing to check on your side: if your web application, its virtual hosts or any of its configuration files reference the VM's IP address, that reference must be updated to the new IP. If your application only uses host names, there is nothing to change.

Agents are installed. Monitoring (Prometheus) and vulnerability scanning (Nessus/Tenable agent).

Your VM becomes a target. It is scanned from the outside, and will keep being scanned. A critical vulnerability found after going public must be fixed — if necessary by temporarily removing public access.

6. Who does what

Actor	Role
DCSR system engineer	Handles the request, coordinates the workflow, internal IP and DNS reservation, VLAN migration, fixed IP, agents, Nessus/Tenable scan, header check, final access validation with you.
Researcher / VM administrator	Web service hardening, vulnerability remediation, functional testing.
PI	Fills in the FWaaS form (port opening request).

Actor	Role
DCSR network engineer	Public DNS, F5 VIP, F5 and firewall configuration, Let's Encrypt certificate.

7. Security requirements on your side

These four points cause most of the back-and-forth. Handling them **before** the scan saves several days.

a) Hide the web server and PHP version

- Apache: hide the version
- NGINX: hide the version
- Check: `curl -Ik https://your-service.ad.unil.ch` (`-k` is needed as long as the certificate is self-signed)

b) Disable TLS 1.0 and TLS 1.1 — only TLS 1.2 and 1.3 are accepted.

c) Set the security headers

Header	Purpose
`Strict-Transport-Security`	Forces HTTPS on subsequent visits.
`X-Frame-Options`	Prevents your site being embedded in a third-party iframe.
`X-Content-Type-Options`	Prevents MIME type sniffing.
`Referrer-Policy`	Limits the information sent to third-party sites.
`Permissions-Policy`	Restricts access to browser APIs (camera, microphone, ...).
`Content-Security-Policy`	Limits allowed content sources (as far as feasible).

Check: securityheaders.com (tick the `hide` option so the result is not published).

d) Fix the vulnerabilities found by the scan — DCSR runs a Nessus/Tenable scan. You receive the report and fix what is identified, with the support of your DCSR engineer. A disputed vulnerability that is hard to fix can be escalated to the security team for a decision.

8. SSL certificates

Context	Certificate
Before going public (UNIL internal)	Self-signed certificate on the VM.
After going public	**Let's Encrypt certificate held by the F5.** Your VM manages nothing on the public side.

Procedures: Self-signed (NGINX) · Self-signed (Apache)

9. How the request unfolds

Your DCSR engineer keeps you informed at each step. Three phases need something from you.

Phase	What happens	What is expected from you
1. Preparation	Internal IP and DNS reservation, documentation.	Confirm the desired public URL.
2. Network compliance	VLAN migration, switch to fixed IP, agent installation, AD/AWX attachment.	**Check whether your application references the VM's IP**, and re-validate the service.
3. Hardening	—	**Hide versions, disable TLS 1.0/1.1, set the headers.**
4. Security scan	Nessus/Tenable scan and analysis.	**Fix the identified vulnerabilities.**
5. Public opening	Public DNS, F5 VIP and configuration, firewall opening.	**The PI fills in the FWaaS form** — see section 10.
6. Validation	Header verification, access test.	**Confirm the service works from the Internet.**

10. The FWaaS form

> **Fill in the form only when your DCSR engineer explicitly tells you to** — that is, once they confirm every prerequisite has been completed. A form submitted too early leads to a rejected or reopened ticket, and delays the whole request.

Filled in by the **PI**: Firewall as a Service.

- Requested ports: **TCP/80 and TCP/443 only**.
- Field *DNS name of the destination server*: the chosen public URL — it must be **valid at the time of the request**.

- Field *Comment*: give the VM name and its internal IP.

The form automatically creates an Otobo ticket handled by the network/security teams.

11. After going public

You will receive automatic email notifications about your VM. They are not informational noise — each one calls for an action on your side:

Notification	What you have to do
Vulnerabilities identified on your VM	Analyse the report and fix them, with the support of your DCSR engineer.
OS updates available	Apply them within a reasonable delay.
Reboot required after OS security updates	Schedule and perform the reboot; the updates are not effective until then.

Ignoring these notifications leaves a publicly exposed VM vulnerable, and public access may be suspended until the situation is fixed.

Also:

- **New vulnerability found?** Contact your DCSR engineer; depending on severity, public access may be suspended until it is fixed.
- **Changing the public URL**: requires a new FWaaS request and new F5 configuration.
- **End of service life**: request decommissioning so that public exposure and DNS entries are removed cleanly.

12. FAQ

Can I expose another port (SSH, 8080, a database)? No. Only TCP/80 and TCP/443 can be exposed. For administrative access or a non-web protocol, use the UNIL VPN or an internal jump host.

How long does the procedure take? The DCSR part is usually quick (1-2 days); the real delays come from hardening/remediation on your side and from the firewall ticket being processed.

My service handles sensitive data. Say so in your initial request: those VMs are tracked separately and public exposure is not always the right answer.

Is my VM backed up? Yes, with a **3-month retention**. To restore it to a given date, email `helpdesk@unil.ch` with the subject `[DCSR] request VM restore - <your_vm_name>` and state the date of

the archive you want.

My service does not need to be public, only reachable from off campus. The UNIL VPN covers that without any Internet exposure — often the better option.

Who do I contact? Your DCSR engineer, or `helpdesk@unil.ch` for a new request.

13. Useful links

- FWaaS form
- securityheaders.com
- Self-signed certificate with NGINX
- Self-signed certificate with Apache

Créé 2026-09-13 14:45:18 UTC par Toan Nguyen
Mis à jour 2026-09-13 14:56:56 UTC par Toan Nguyen