Pelion

DINA

An overview of **Pelion's** resilient architecture

Pelion.com

DINA

Direct Inbound Network Access (DINA) provides customer's with the ability to remotely access their subscriber base using functionality within the Pelion Connectivity Platform. Where a customer requires remote access to a device they identify the subscriber on the platform and, from the specific SIM management screen, create a DINA session. For the duration of the DINA session the customer can connect via the internet to a temporarily allocated public IP, linked to the SIM in their device.

Using DINA is simple and can be used in conjunction with SSH, or other secure transport technologies, to protect the data flowing between device and application.

Some IoT connectivity providers supply public fixed IP for device accessibility. DINA is a far more secure option whilst still providing accessibility when required.

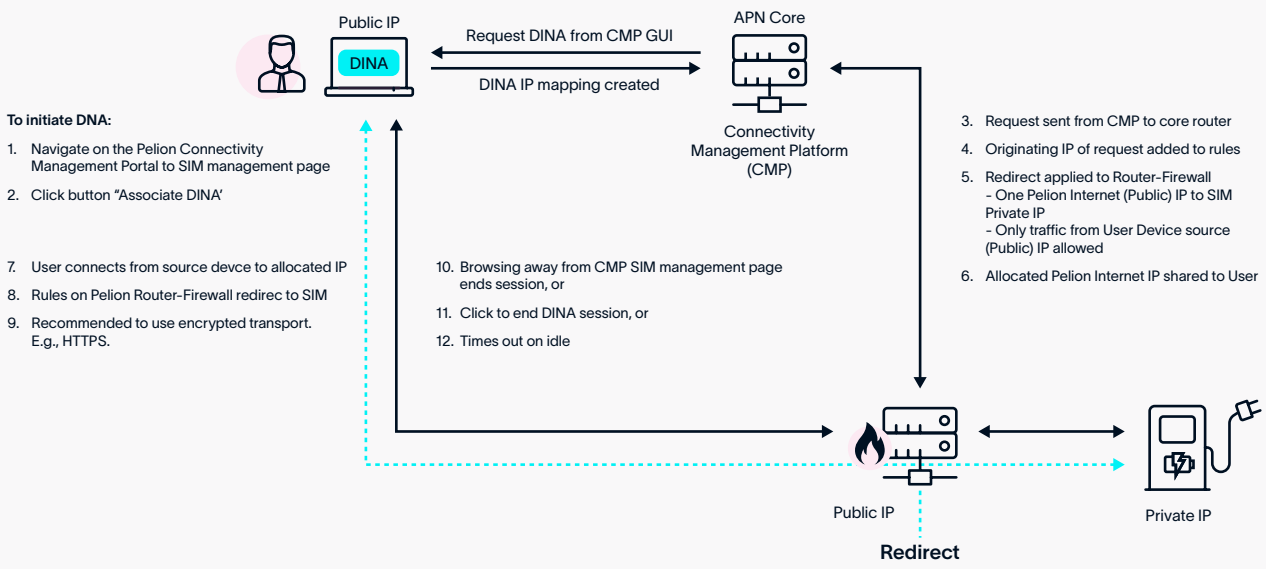
DINA is suitable for those customers needing ad-hoc access to their subscribers e.g., engineers accessing device management pages.

Technical Description

Though it sounds similar, DINA is not a VPN technology. It does not provide any encryption of customer traffic.

DINA temporarily associates a fixed (private) IP subscriber with a public IP address. This public address is randomly associated and is reclaimed to the pool once the session is disassociated. This means a user accessing a device using DINA is given a public IP address which can only be accessed by them.

Architecture



DINA functionality is available via the Pelion Connectivity Management Portal (CMP), access to which can only be made with a Username and Password. From the SIM management page, a DINA Association is requested which sends a request via CMP to a core router. This temporarily allocated one public IP from a designated pool and a redirect to the private IP of the SIM in your device.

Critically, the firewall rule created will only allow connectivity to the public IP if it originates from the same IP as the device used to request a DINA association. All other traffic inbound to this public IP is automatically discarded.

The session ends if the user navigates away from the SIM management page, clicks to “Disassociate DINA”, or it times out on idle.

Security Features

- DINA functionality is accessible to Pelion CMP users and has password control.
- Source IP of the device requesting DINA is only able to reach the assigned public IP.
- Recommended: Password protected access to device via SIM interface.
- Recommended: Secure transport using HTTPS, SSH, or similar.
- Recommended: Customer uses FW rule to allow only traffic from DINA public subnet.

Service Features

- Simple and secure
- Suited for Ad-Hoc access to subscribers
- GUI Access
- No configuration required

Pelion

Contact us today or visit our website

hello@pelion.com | Pelion.com