WORKSHOP GARR 2026

NET MAKERS

eduVPN: una VPN nazionale per INFN

Francesco Laruina

INFN

Da dove siamo partiti

CA openVPN in scadenza

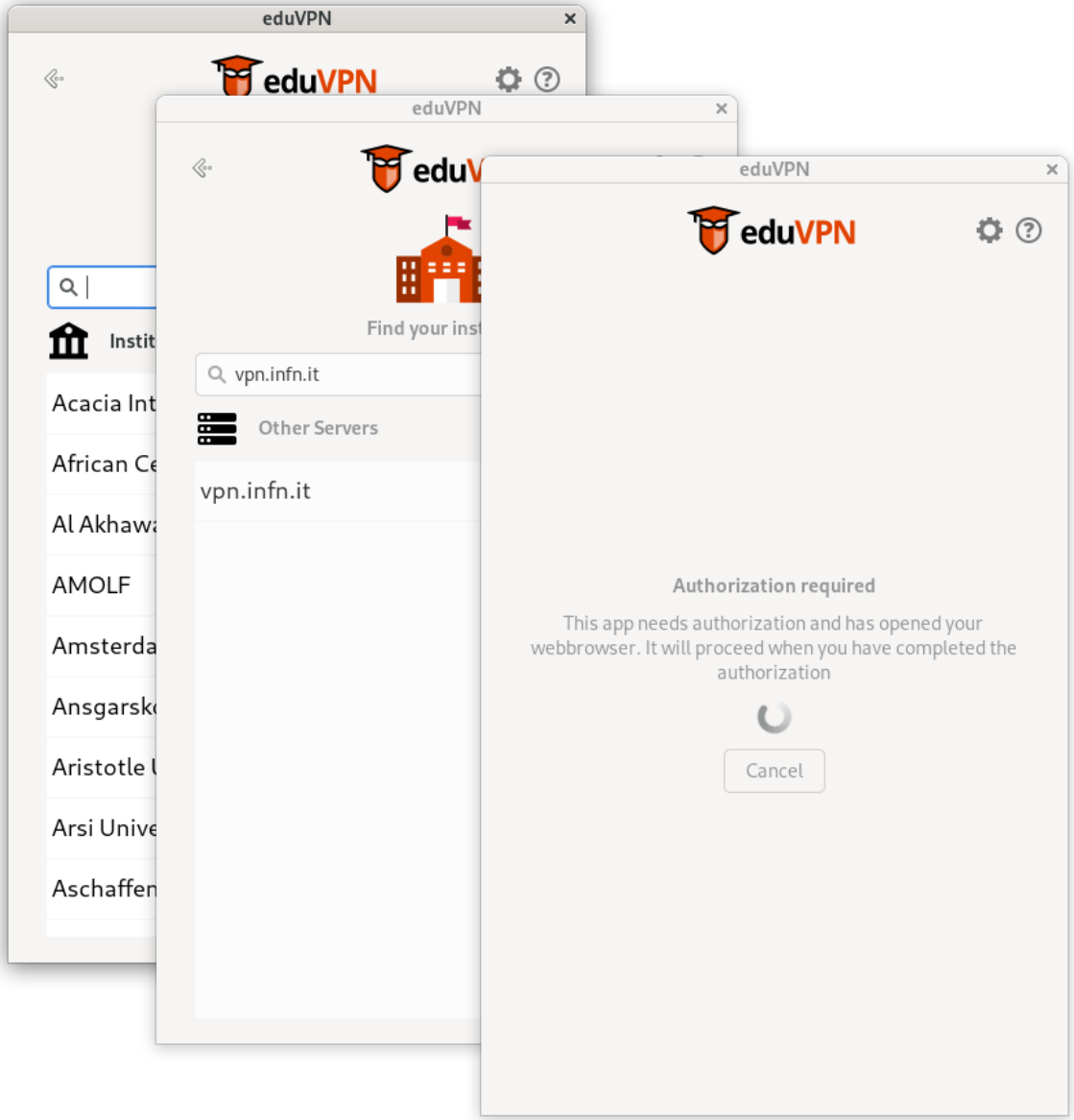
- Tocca passare in rassegna tutti i client
- Fondamentale una mail urbi et orbi (e sperare che venga letta)

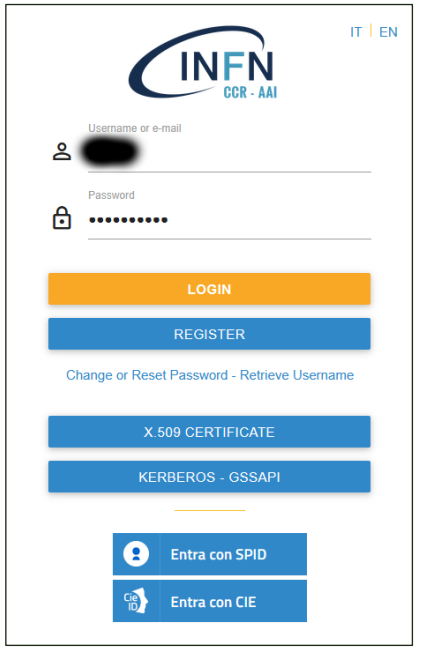
  ogni modifica genera ticket

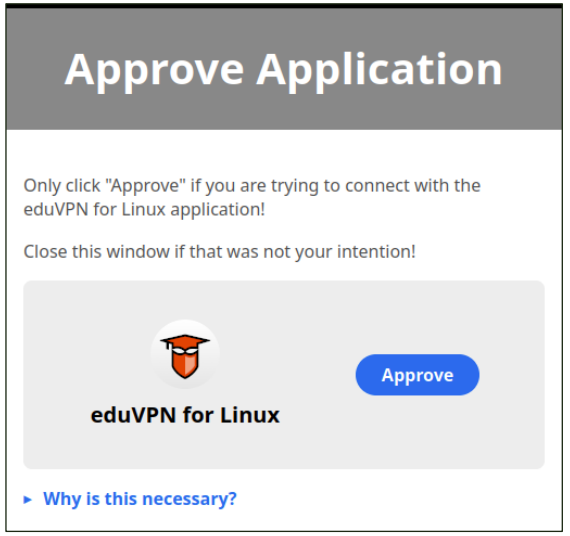
Autenticazione

- OpenVPN con username/password
- Non tutta l'utenza ha le capacita' per gestire certificati
- Vorremmo che la VPN supportasse MFA

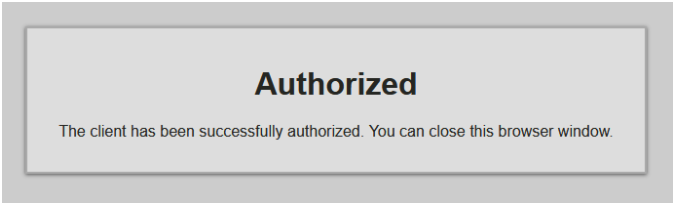
Le istruzioni (1)



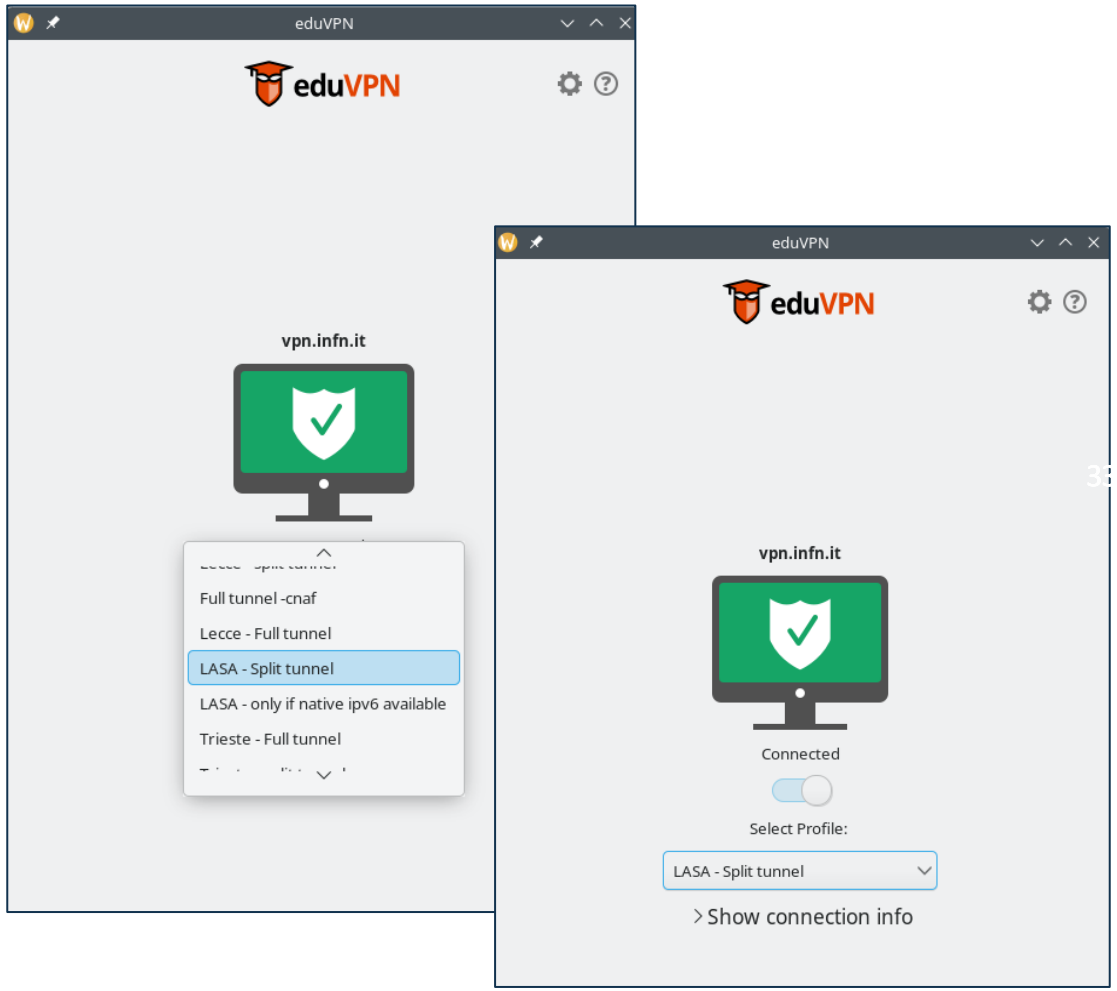








Le istruzioni (2)



Scarico l'applicazione per la mia piattaforma preferita

In "Trova la tua istituzione" scrivo il nome del server

a meno di registrazione Istituzione

OIDC+SAML

User/pass + totp	X509 + totp	SPID	CIE	Krb5+totp

Componenti del servizio

- **vpn-user-portal**
  - API e pagina web
  - Supporta configurazioni in HA
- **vpn-daemon**
  - Interagisce con vpn-user-portal via API http
  - Configura wireguard e/o openvpn server
  - Fornisce informazioni a vpn-user-portal
- **Proxyguard**
  - "Proxy WireGuard UDP connections over HTTP(S)"

Il portale (1)

- Contattato dai client
- Interagisce con le sedi
- Detiente le definizione dei profili
- Reverse proxy per proxyguard... per ora
- Syncthing ->sincronizzazione multimaster

3 VM su Business continuity che operano in active-active

Database galera + memcached per sessioni + haproxy db

Syncthing per sincronizzazione file, permessi e acl posix

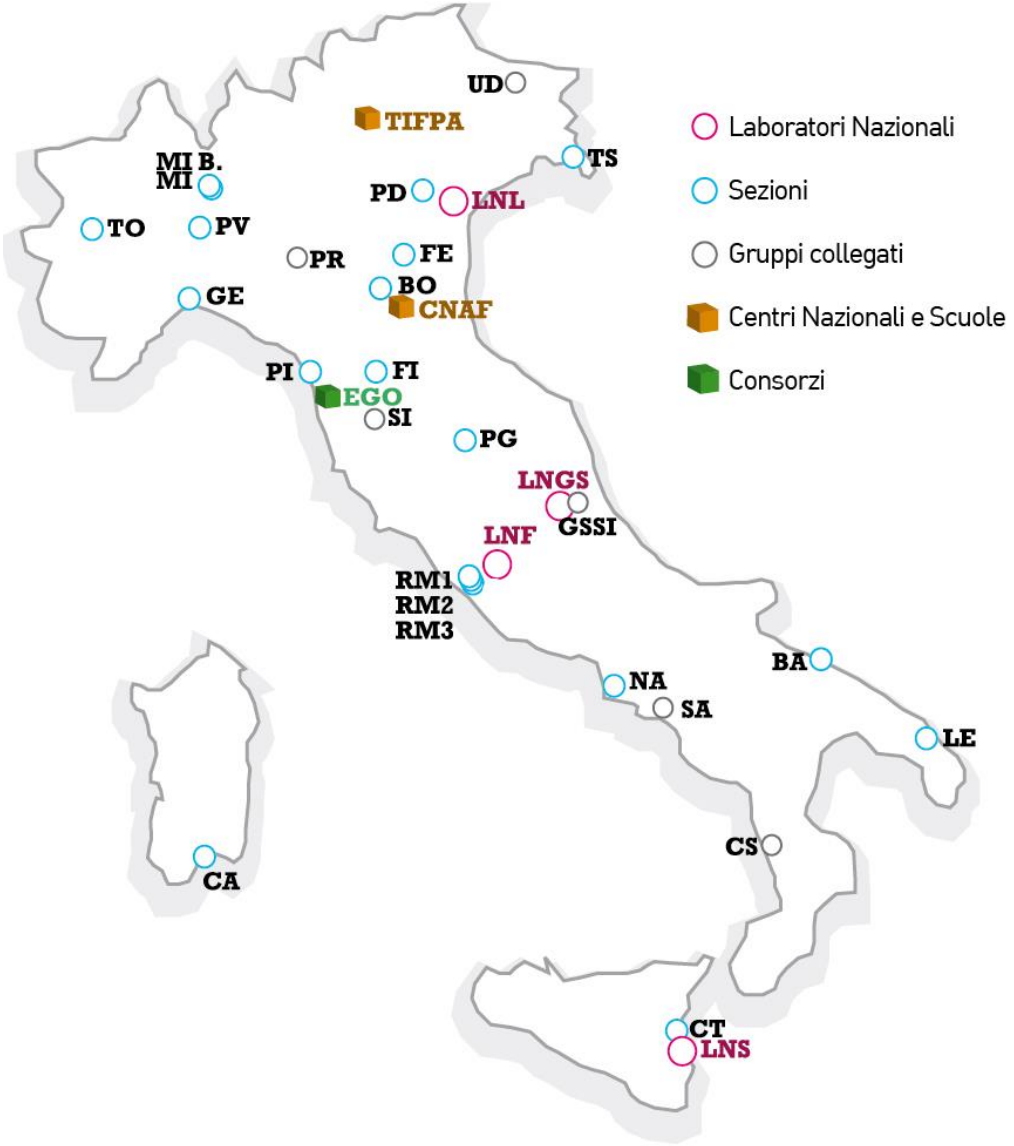
Il portale (2)

- vpn.infn.it -- DNS —-> vpn-0{1..3}.infn.it
- Tempi di riavvio bassi
- Galera e syncthing possono tornare operativi con calma
- Efficace, ma migliorabile

```
frontend galera
    bind *:3307
    mode tcp
    default_backend galera_backend
...
backend galera_backend
    mode tcp
    server vpn-01.infn.it vpn-01.infn.it:3306 check
    server vpn-02.infn.it vpn-02.infn.it:3306 check backup
    server vpn-03.infn.it vpn-03.infn.it:3306 check backup
```

I nodi

- Eseguono vpn-daemon
- Dislocati nelle sedi dell'Istituto
- Veri server VPN:
  - Wireguard
  - ~~openvpn~~ => non lo usiamo
  - proxyguard-server
- Proxyguard-server viene (per ora) contattato tramite reverse proxy (vpn.infn.it)



Enrollment di una sede

1. Scrivere a eduvpn-support

2. Aggiunta nodi di sede al portale e generazione segreti
   1. Script python edita inventory.yml, genera secrets e produce un tar
   2. Tar viene cifrato con gpg e scambiato
   3. Ansible playbook aggiorna setup portali
3. Inserimento di profili (in json) per la sede

4. Scambio segreti e lancio playbook Ansible in sede (config nodi)
5. Verifica funzionamento

Tipicamente validiamo un profilo con NAT e poi...

Sede che vai, infrastruttura di logging che trovi

- Logging decentralizzato
- Syslog-ng
- Vpn-0{1..3}.infn.it
  -> vpn-log.infn.it
  -> nodo.sede.infn.it
- mTLS

```
# Inoltro log dai portali al nodo pertinente

destination d_eduvpn-02.sede.infn.it {
        network("eduvpn-02.sede.infn.it" port(6514)
        transport("tls")
        tls( ca-file("/etc/syslog-ng/security/ca.crt"))
    );
};

filter f_eduvpn-02.sede.infn.it {
        match("eduvpn-02.sede.infn.it",
value("MESSAGE"));
};

log {
        source(s_portals);
        filter(f_eduvpn-02.sede.infn.it);
        destination(d_eduvpn-02.sede.infn.it);
        };
```

Sede che vai, ACL che trovi

Profili:

- Full tunnel e/o split tunnel
  - Per tutti?
  - Per amministrazione?
  - Solo dipendenti e associati?
  - ACL basate su attributi SAML
    - Locality, isMemberOf, eduPersonEntitlement

- GODiVA:
  - Identity and Access Management System dell'INFN
  - gruppi logici, eccezioni, deleghe

eduPersonEntitlement:
urn:mace:infn.it:g:infn:**eduvpn**

:**pi** (delega a sede)

:ammin

Sede che vai, rete che trovi (1)

- NAT
- NAT condizionale:
  - routing su ip interni
  - SNAT verso resto del mondo

```
ip saddr 10.11.0.0/16
        ip daddr != { 10.0.0.0/8,... ,168.0.0/16 }
        oifname "ens192" masquerade
```

Sede che vai, rete che trovi (2)

Policy routing:

- Profili che *escono* da NIC differenti

```
# ip rule
0:      from all lookup local
32759:  from 10.133.10.0/24 lookup pisavpn
...
32764:  from 10.133.6.0/24 lookup ammin
32766:  from all lookup main
32767:  from all lookup default

# ip route show table ammin
default via xxx.xxx.xxx.xxx dev eth2
10.133.6.0/24 dev wg0 scope link
```

Sede che vai, rete che trovi (3)

Dual stack per i client

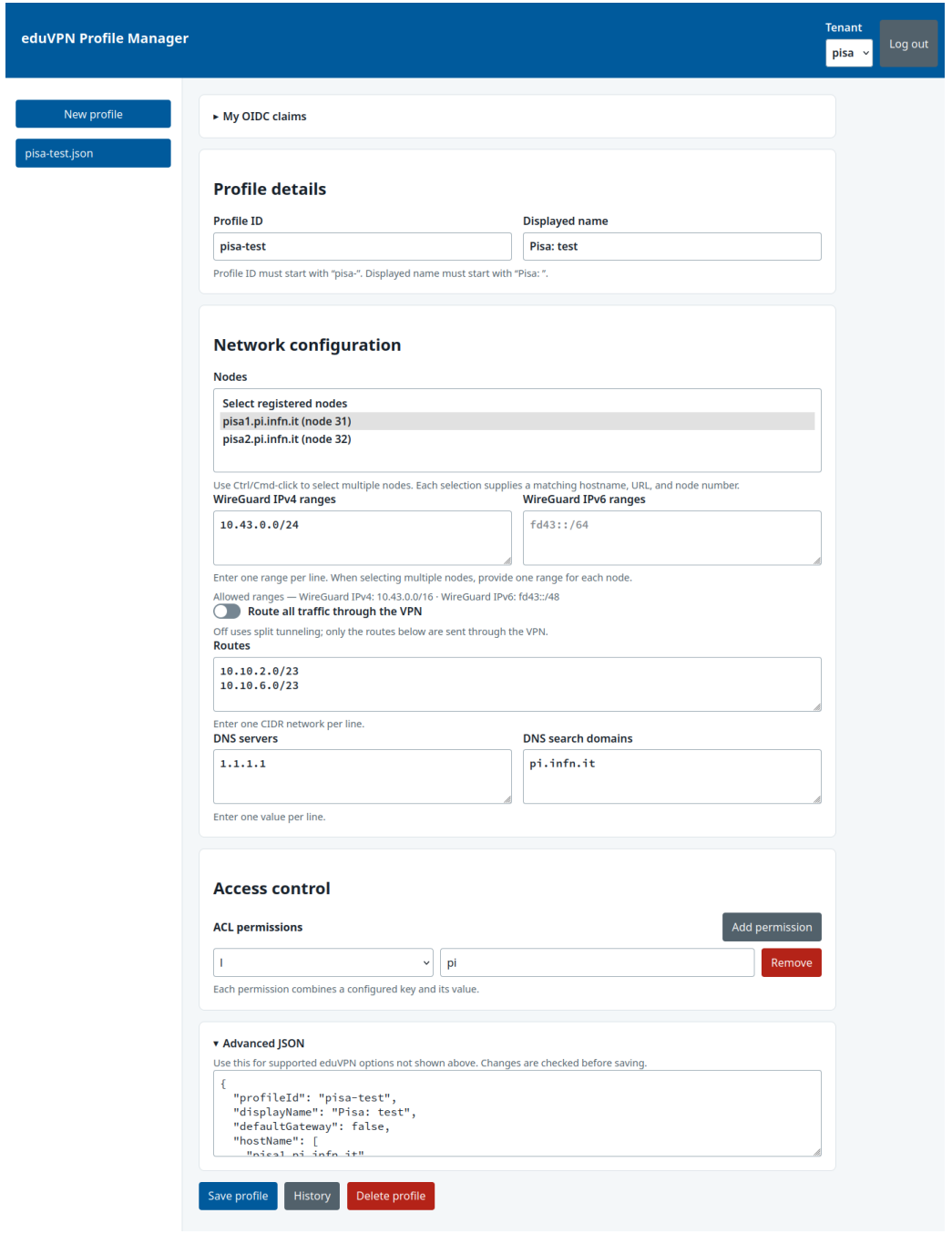
- Assegno al client un IPv6 GUA nel tunnel
- Il nodo fa da router per la subnet

Dual stack per nodi

- Endpoint wireguard risolto in Dual Stack con qualche caveat indipendente da eduVPN (https://gitlab.freedesktop.org/NetworkManager/NetworkManager/-/work_items/1939)

Sede che vai, autonomia che cerchi

- eduVPN non prevede un meccanismo di deleghe/ruoli:
  - O sei utente o sei admin
- Una sede INFN ha bisogno di autonomia nella gestione dei profili
- Abbiamo sviluppato un portale web (ancora in test) che permette
  - di delegare la gestione sulla base di entitlement
  - di semplificare la compilazione dei profili json
  - rollback in caso di errore.



Conclusioni e ringraziamenti

WORKSHOP GARR 2026

NET MAKERS

Domande?

www.partici.fi
8399528

francesco.laruina@infn.it

WORKSHOP GARR 2026
NET MAKERS