VPN univr

ubuntu

```
sudo apt install network-manager-vpnc network-manager-vpnc-gnome
```

arch

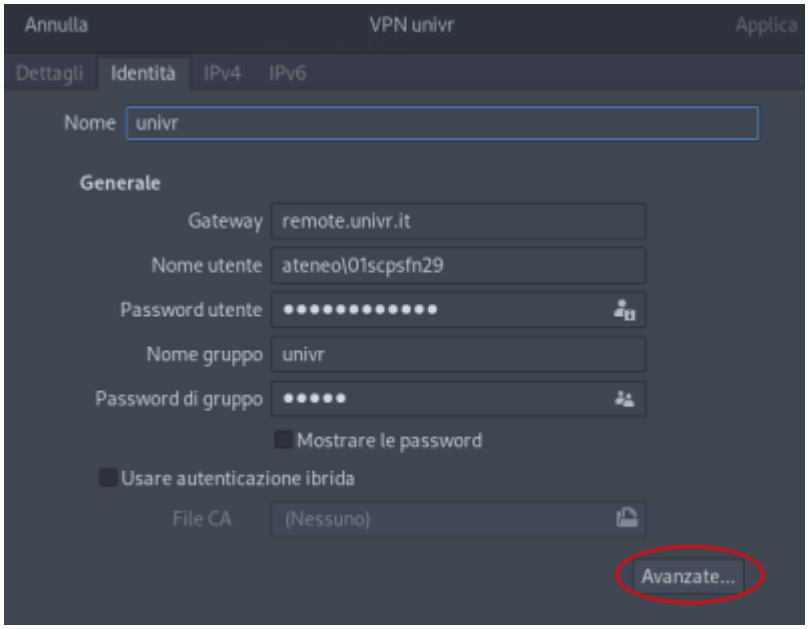
```
paru networkmanager-vpnc
```

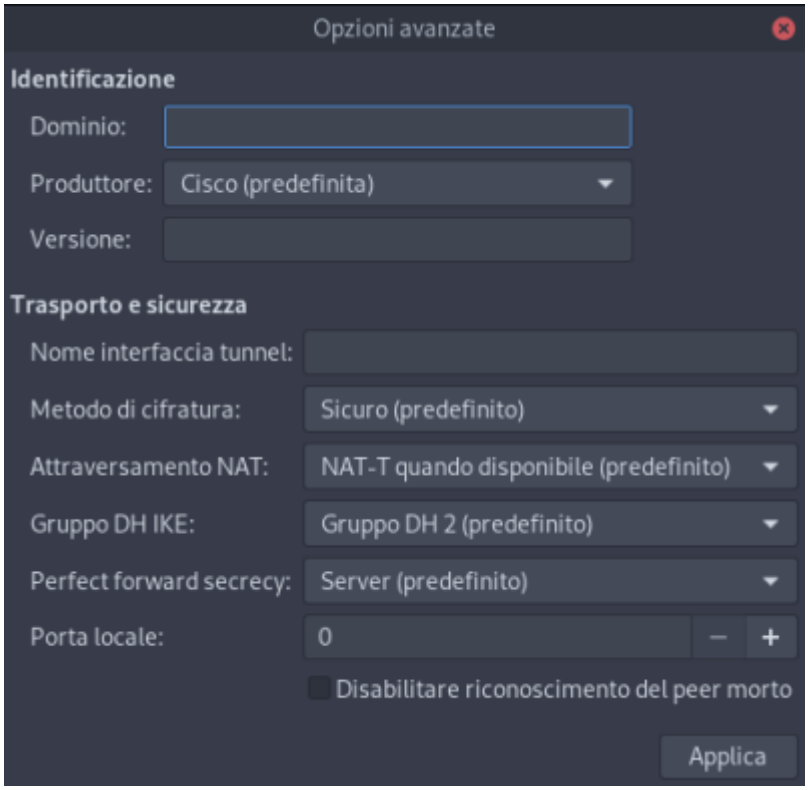
network manager

```
yay -S networkmanager-vpnc
```

add VPN cisco compatible from network manager:

- gateway: remote.univr.it
- username: ateneo\01scpsfn29
- password: xxx
- group: univr
- group password: univr



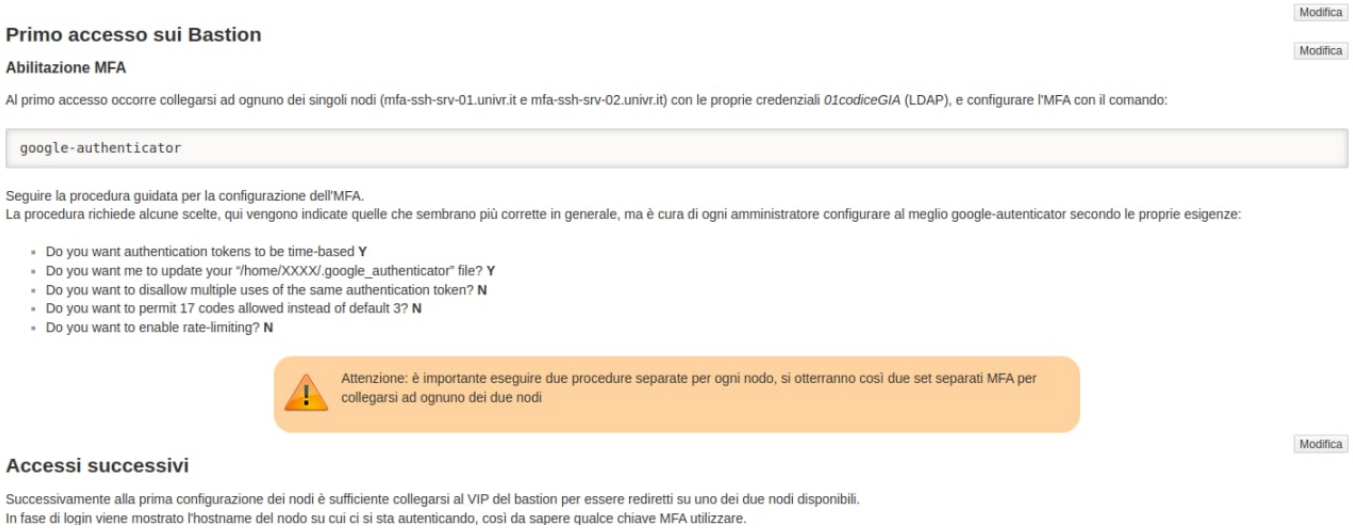


or create /etc/NetworkManager/system-connections/univr.nmconnection (chmod 600 and owned by root)

```
[connection]
id=univr
uuid=234f1f79-0a96-4be0-991e-75622ead54d0
type=vpn
autoconnect=false
permissions=user:scipio:;
timestamp=1630335537

[vpn]
IKE DH Group=dh2
IPSec ID=univr
IPSec gateway=remote.univr.it
IPSec secret-flags=0
Local Port=0
NAT Traversal Mode=natt
Perfect Forward Secrecy=server
Vendor=cisco
Xauth password-flags=0
Xauth username=xxx
ipsec-secret-type=save
xauth-password-type=save
service-type=org.freedesktop.NetworkManager.vpnc

[vpn-secrets]
IPSec secret=univr
Xauth password=xxx
```

```
[ipv4]
method=auto

[ipv6]
addr-gen-mode=stable-privacy
method=auto

[proxy]
```

bastion (jump box)



Modifica

Primo accesso sui Bastion

Modifica

Abilitazione MFA

Al primo accesso occorre collegarsi ad ognuno dei singoli nodi (mfa-ssh-srv-01.univr.it e mfa-ssh-srv-02.univr.it) con le proprie credenziali *01codiceGIA* (LDAP), e configurare l'MFA con il comando:

```
google-authenticator
```

Seguire la procedura guidata per la configurazione dell'MFA.
La procedura richiede alcune scelte, qui vengono indicate quelle che sembrano più corrette in generale, ma è cura di ogni amministratore configurare al meglio google-autenticator secondo le proprie esigenze:

- Do you want authentication tokens to be time-based **Y**
- Do you want me to update your "/home/XXXX/.google_authenticator" file? **Y**
- Do you want to disallow multiple uses of the same authentication token? **N**
- Do you want to permit 17 codes allowed instead of default 3? **N**
- Do you want to enable rate-limiting? **N**

Attenzione: è importante eseguire due procedure separate per ogni nodo, si otterranno così due set separati MFA per collegarsi ad ognuno dei due nodi

Modifica

Accessi successivi

Successivamente alla prima configurazione dei nodi è sufficiente collegarsi al VIP del bastion per essere rediretti su uno dei due nodi disponibili.
In fase di login viene mostrato l'hostname del nodo su cui ci si sta autenticando, così da sapere qualce chiave MFA utilizzare.

~/.ssh/config

```
Host umfa
  Hostname mfa-ssh-srv.univr.it
  User 01scpsfn29
  ForwardAgent yes

Host ucd
  Hostname cd-www-srv.univr.it
  User 01scpsfn29
  ProxyJump umfa

Host ustage
  Hostname stage-dev.univr.it
  User 01scpsfn29
  ProxyJump umfa
```

Oppure, al posto di google auth, si può usare keepassxc utilizzando totp e la "secret key"