nethesis

VPN con NethSecurity NG 7

Davide Marini

Molto usate perchè

- Permettono di lavorare su LAN remote senza limitazioni
- Sono sicure (traffico cifrato)
- Supporto per tutti i client (host to net)

Ricordarsi sempre degli aspetti legati alla sicurezza

- Le macchine che accedono in vpn di default possono vedere tutta la LAN remota
- Buona pratica creare regole di firewall sugli host che si connettono limitandone operatività alle sole operazioni strettamente necessarie

nethesis

OpenVPN

- Sicura
- Semplice da configurare e utilizzare
- Supporto multipiattaforma

Windows: openvpn.net (https://openvpn.net/index.php/download/community-downloads.html)

Linux : openvpn.net (https://openvpn.net/index.php/download/community-downloads.html)

Mac: Tunnelblick (https://tunnelblick.net/)

iOS: OpenVPN Connect (https://itunes.apple.com/it/app/openvpn-connect/id590379981?mt=8)

Android: OpenVPN Connect (https://play.google.com/store/apps/details?id=net.openvpn.openvpn&hl=it=

Modalità: Routed o Bridged?

All'attivazione del server OpenVPN RoadWarrior si aggiunge un'ulteriore interfaccia a quelle presenti su NethSecurity.

Il traffico vpn passerà su questa interfaccia *speciale* che può essere di 2 tipi:

- **tun** (modalità routed)
- **tap** (modalità bridged)

La modalità consigliata è la routed (interfaccia *tun*)

- Traffico vpn lavora su una classe di rete propria
- Instradamento molto chiaro gestito con regole di routing
- Facilità ad individuare traffico vpn e creare regole di firewall
- Non richiede modifiche alla rete green
- Solo il traffico destinato alle green remote (tutte le green)viene instradato nel tunnel VPN, il resto del traffico continua a passare FUORI dal tunnel

VPN Host to Net  Routed

netheSIS

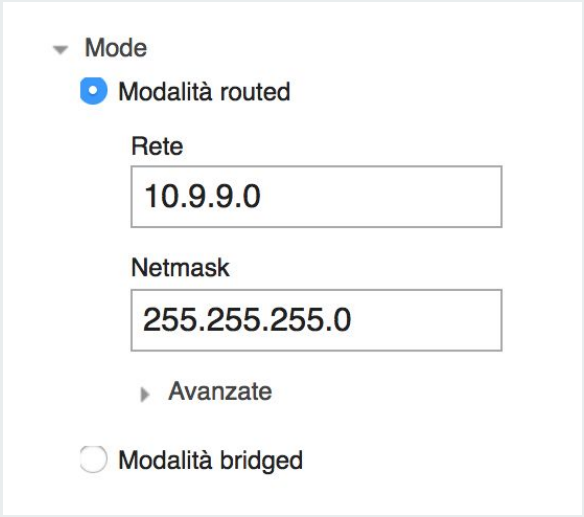
```
[root@nsec-primary ~]# ifconfig
en0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.41  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a35:71ff:fe07:2380  prefixlen 64  scopeid 0x20<link>
        ether 08:35:71:07:23:80  txqueuelen 1000  (Ethernet)
        RX packets 862504238  bytes 228311965408 (212.6 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1235116944  bytes 1176849470026 (1.0 TiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0xf7d00000-f7d20000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 216967508  bytes 175757926851 (163.6 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 216967508  bytes 175757926851 (163.6 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tunrw: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.9.9.1  netmask 255.255.255.255  destination 10.9.9.2
        inet6 fe80::68c6:9248:20a6:b1b9  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3  bytes 144 (144.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

VPN Host to Net Routed

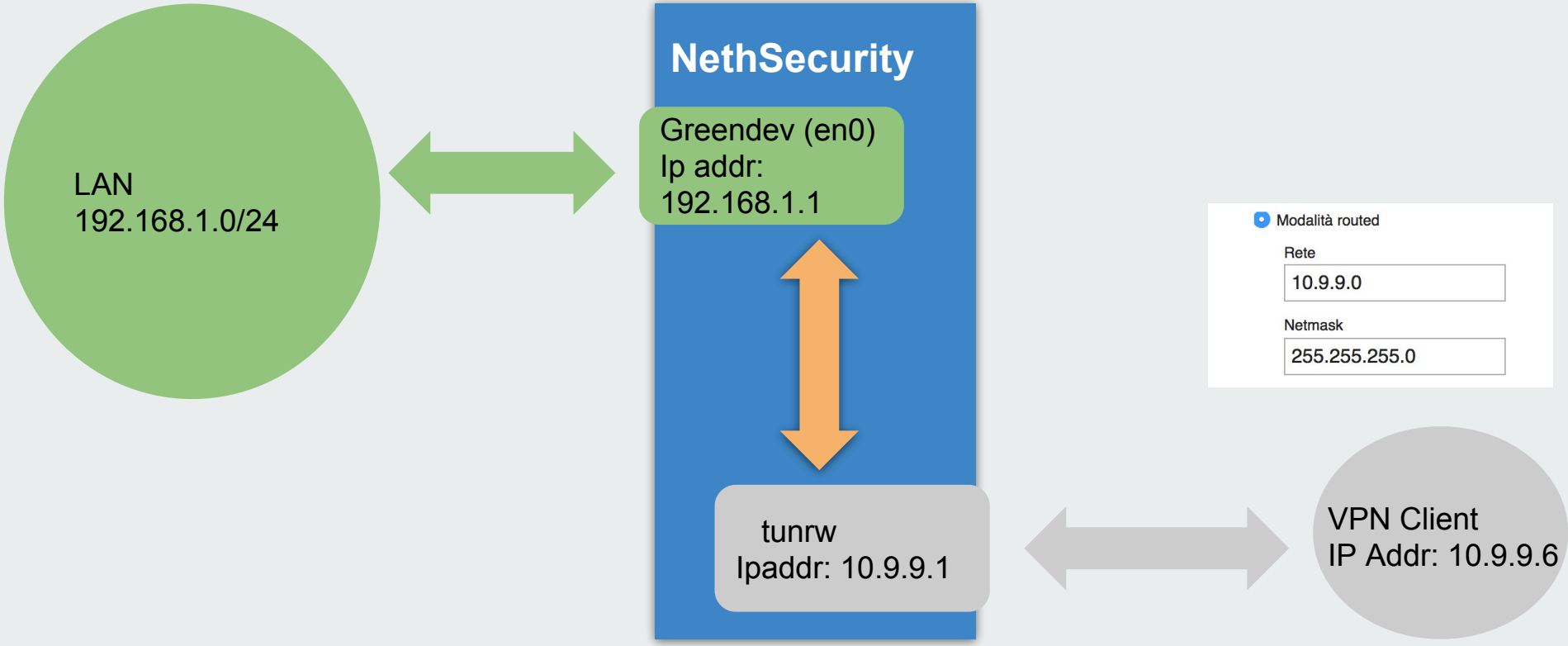
```
tunrw: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.9.9.1  netmask 255.255.255.255  destination 10.9.9.2
        inet6 fe80::68c6:9248:20a6:b1b9  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3  bytes 144 (144.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



- Il traffico vpn passa tutto su tunrw
- Tutti gli host che si connettono prendono un ip della classe stabilita nel pannello di configurazione

- La classe scelta deve essere:
  - Una rete privata (rfc-1918)
  - Deve essere diversa da tutte le altre reti gestite dal firewall

Schema instradamento RoadWarrior Routed (indiretto)



Affinchè funzioni tutto correttamente è necessario che:

1. Il tunnel sia UP
2. Nel client esista una regola di routing apposita per raggiungere la LAN remota (creata automaticamente da OpenVPN)

Se il tunnel non si attiva correttamente

Lanciare la VPN sul client e verificare nei log

Da interfaccia web :

- Visualizza log
- Selezionare /var/log/openvpn/openvpn.log
- Usare opzione *segui*

Da console ssh

```
tail -f /var/log/openvpn/openvpn.log
```

- Quando il client prova a connettersi devono apparire delle righe nel log
- Se non appaiono righe significa che non arriva traffico al firewall
- Verificare che il client riesca ad uscire su internet
- Verificare che il firewall sia raggiungibile e che la porta **1194 UDP** (default modificabile) sia stata inoltrata verso il firewall

Esempio di log con tunnel correttamente stabilito

```
Thu Mar  1 11:44:34 2018 87.19.66.29:59607 TLS: Initial packet from [AF_INET]87.19.66.29:59607 (via [AF_INET]93.57.48.68%en2),
sid=a8dec640 4eb57764
Thu Mar  1 11:44:34 2018 87.19.66.29:59607 VERIFY OK: depth=1, CN=NethServer, O=Nethesis srl, ST=SomeState,
OU=SomeOrganizationalUnit, emailAddress=root@nethsecurity7.nethesis.it, C=--, L=Pesaro
Thu Mar  1 11:44:34 2018 87.19.66.29:59607 VERIFY OK: depth=0, C=--, ST=SomeState, L=Pesaro, O=Nethesis srl, OU=SomeDepartment,
CN=davidem, emailAddress=admin@nethsecurity7.nethesis.it
Thu Mar  1 11:44:34 2018 87.19.66.29:59607 peer info: IV_VER=2.3.10
Thu Mar  1 11:44:34 2018 87.19.66.29:59607 peer info: IV_PLAT=mac
Thu Mar  1 11:44:34 2018 87.19.66.29:59607 peer info: IV_PROTO=2
Thu Mar  1 11:44:34 2018 87.19.66.29:59607 Outgoing Data Channel: Cipher 'BF-CBC' initialized with 128 bit key
Thu Mar  1 11:44:34 2018 87.19.66.29:59607 Outgoing Data Channel: Using 160 bit message hash 'SHA1' for HMAC authentication
Thu Mar  1 11:44:34 2018 87.19.66.29:59607 Incoming Data Channel: Cipher 'BF-CBC' initialized with 128 bit key
Thu Mar  1 11:44:34 2018 87.19.66.29:59607 Incoming Data Channel: Using 160 bit message hash 'SHA1' for HMAC authentication
Thu Mar  1 11:44:34 2018 87.19.66.29:59607 Control Channel: TLSv1.2, cipher TLSv1/SSLv3 ECDHE-RSA-AES256-GCM-SHA384, 2048 bit RSA
Thu Mar  1 11:44:34 2018 87.19.66.29:59607 [ davidem] Peer Connection Initiated with [AF_INET]87.19.66.29:59607 (via
[AF_INET]93.57.48.68%en2)
Thu Mar  1 11:44:34 2018 davidem/87.19.66.29:59607 MULTI_sva: pool returned IPv4=10.9.9.6, IPv6=(Not enabled)
Thu Mar  1 11:44:34 2018 davidem/87.19.66.29:59607 MULTI: Learn:   10.9.9.6 -> davidem/87.19.66.29:59607
Thu Mar  1 11:44:34 2018 davidem/87.19.66.29:59607 MULTI:   primary virtual IP for davidem/87.19.66.29:59607: 10.9.9.6
Thu Mar  1 11:44:36 2018 davidem/87.19.66.29:59607 PUSH: Received control message: 'PUSH_REQUEST'
Thu Mar  1 11:44:36 2018 davidem/87.19.66.29:59607 SENT CONTROL [davidem]: 'PUSH_REPLY,dhcp-option DOMAIN nethesis.it,dhcp-option
DNS 10.9.9.1,dhcp-option WINS 10.9.9.1,dhcp-option NBDD 10.9.9.1,dhcp-option NBT 2,route 192.168.100.0 255.255.255.0,route
192.168.1.0 255.255.255.0,route 10.9.9.1,topology net30,ping 20,ping-restart 120,ifconfig 10.9.9.6 10.9.9.5,peer-id 0' (status=1)
```

Tunnel UP

TEST PRINCIPALE

ping IP green del firewall

Se il ping va a buon fine significa che il tunnel è correttamente funzionante (abbiamo attraversato il firewall e arriviamo sulla green).

*Il ping ad host della rete **diversi dall'IP green** del firewall non è significativo del buon funzionamento della VPN*

Tunnel UP ma l'IP green del firewall non si raggiunge

- **Verificare configurazione di rete del client:**
  - Deve esistere un'interfaccia con uno degli ip della subnet della VPN
- **Verificare la tabella di routing del pc**
  - Deve esserci una regola di routing apposita per raggiungere la rete remota che usa come gateway un ip della rete della Roadwarrior
- **Verificare i log nel client**

- **Verificare se arriva traffico all'interfaccia tunrw del firewall**
  - Nel client:
    - `ping 192.168.1.1` (green del firewall)
  - Nel firewall (console ssh):
    - `tcpdump -p -nn -i tunrw`

Esempio di comunicazione corretta col firewall

```
[root@nsec-primary ~]# tcpdump -p -nn -i tunrw
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tunrw, link-type RAW (Raw IP), capture size 262144 bytes
11:48:42.681333 IP 10.9.9.6 > 192.168.1.1: ICMP echo request, id 26384, seq 0, length 64
11:48:42.681369 IP 192.168.1.1 > 10.9.9.6: ICMP echo reply, id 26384, seq 0, length 64
```

Tunnel UP ma alcuni host non si raggiungono

- Verificare che le richieste siano correttamente inviate all'host
  - Entrano dall'interfaccia tunrw
  - Escono dall'interfaccia della green verso l'host conttato

```
[root@nsec-primary ~]# tcpdump -p -nn -itunrw icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tunrw, link-type RAW (Raw IP), capture size 262144 bytes
12:44:41.164353 IP 10.9.9.6 > 192.168.1.22: ICMP echo request, id 5395, seq 0, length 64

[root@nsec-primary ~]# tcpdump -p -nn -ien0 host 10.9.9.6 and icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:44:41.164383 IP 10.9.9.6 > 192.168.1.22: ICMP echo request, id 5395, seq 0, length 64
```

Si vede che l'host contattato riceve la richiesta ma non risponde

Tunnel UP ma alcuni host non si raggiungono

- Se l'host non risponde tipicamente questo accade perchè:
  - C'è un personal firewall/AV che blocca le richieste provenienti da altre reti
  - L'host contattato ha un altro default gateway (risposte non inviate a NethSecurity)

Esempio di corretta comunicazione

```
[root@nsec-primary ~]# tcpdump -p -nn -i tunrw icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tunrw, link-type RAW (Raw IP), capture size 262144 bytes
12:44:41.164353 IP 10.9.9.6 > 192.168.1.22: ICMP echo request, id 5395, seq 0, length 64
12:44:41.164599 IP 192.168.1.22 > 10.9.9.6: ICMP echo reply, id 5395, seq 0, length 64

[root@nsec-primary ~]# tcpdump -p -nn -i en0 host 10.9.9.6 and icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:44:41.164383 IP 10.9.9.6 > 192.168.1.22: ICMP echo request, id 5395, seq 0, length 64
12:44:41.164576 IP 192.168.1.22 > 10.9.9.6: ICMP echo reply, id 5395, seq 0, length 64
```

Tunnel UP ma alcuni host non si raggiungono

Se l'host che si sta cercando di contattare non è collegato alla rete o è spento :

```
[root@nsec-primary ~]# tcpdump -p -nn -i tunrw icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tunrw, link-type RAW (Raw IP), capture size 262144 bytes
12:44:41.164353 IP 10.9.9.6 > 192.168.1.22: ICMP echo request, id 5395, seq 0, length 64
12:44:42.164353 IP 10.9.9.6 > 192.168.1.22: ICMP echo request, id 5395, seq 0, length 64

[root@nsec-primary ~]# tcpdump -p -nn -i en0 host 10.9.9.6 and icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:44:41.164383 ARP, Request who-has 192.168.1.22 tell 192.168.1.1, length 28
12:44:41.164576 ARP, Request who-has 192.168.1.22 tell 192.168.1.1, length 28
```

Richieste ARP del firewall che chiede qual è l'host con l'ip 192.168.1.22

Modalità bridged (interfaccia *tap*)

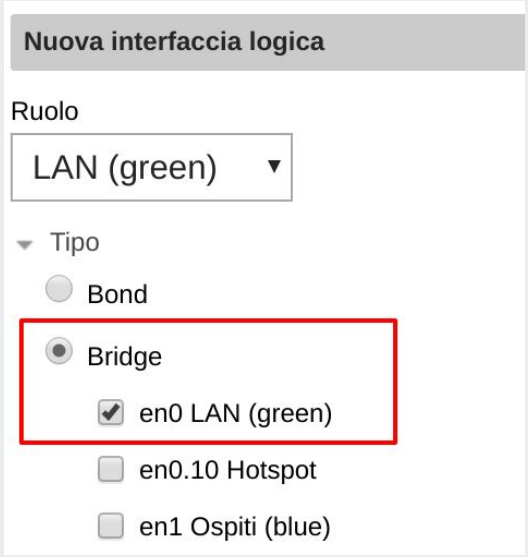
Necessaria nei casi in cui sia necessario accedere a macchine remote con configurazioni di rete che ne impediscano l'accesso da remoto
Es: i client hanno

- Default gateway differente da Nethsecurity
- personal firewall o antivirus che impediscono l'accesso da reti differenti dalla LAN (il traffico VPN in modalità routed arriva da una rete differente dalla LAN remota)

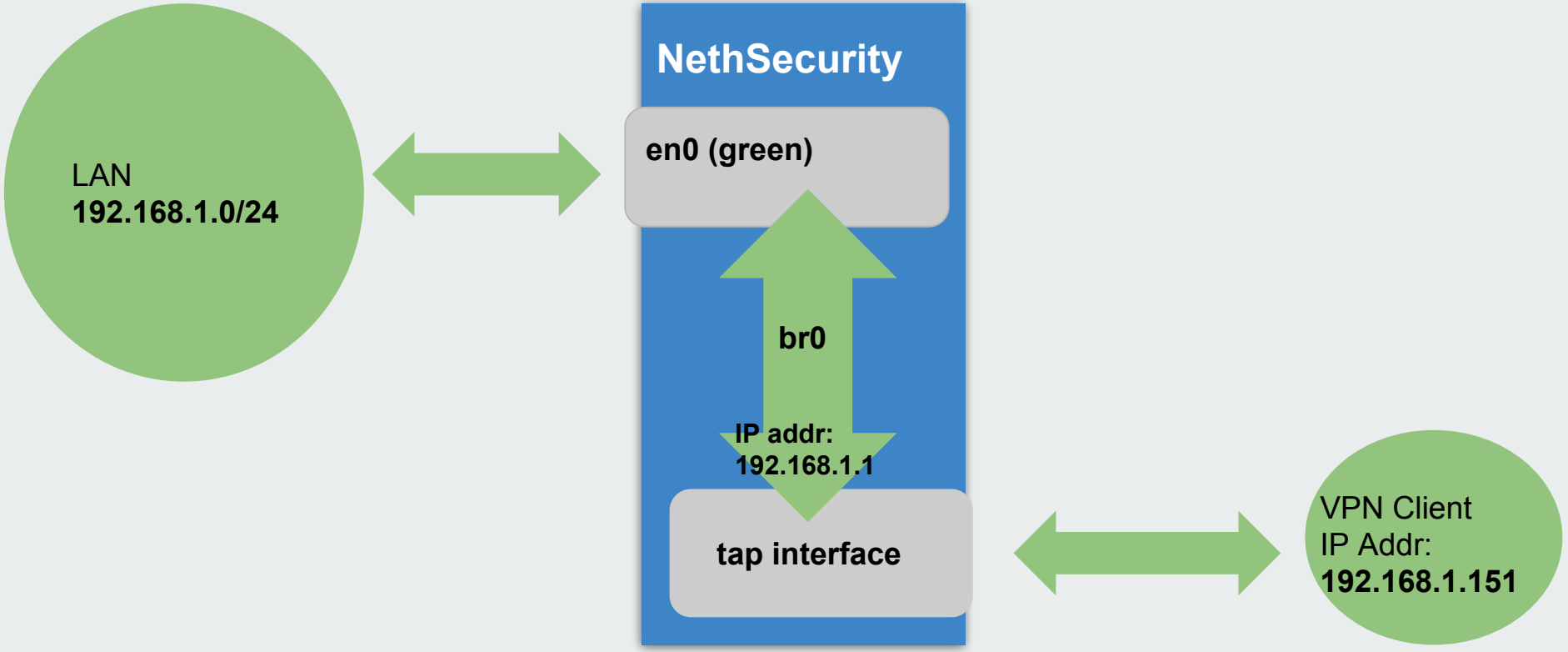
- I device che si collegano prendono un IP della rete green, assegnato all'interno di un range ben definito
- Per poter creare la VPN è necessario definire prima un'interfaccia Bridge che lavora sulla green (o su una delle green)
- La VPN bridged consente di sfogliare la rete perchè può comunicare con dei messaggi broadcast

Necessario creare prima un bridge (br0) sulla green

- Da Menu *Rete* creare nuova interfaccia logica **bridge**



VPN Host to Net Bridged (instradamento diretto)



Se il tunnel non si attiva correttamente

Lanciare la VPN sul client e verificare nei log

Da interfaccia web :

- Visualizza log
- Selezionare /var/log/openvpn/openvpn.log
- Usare opzione *segui*

Da console ssh

```
tail -f /var/log/openvpn/openvpn.log
```

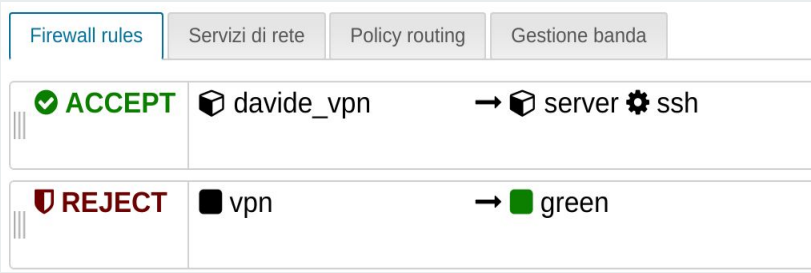
- Quando il client prova a connettersi devono apparire delle righe nel log
- Se non appaiono righe significa che non arriva traffico al firewall
- Verificare che il client riesca ad uscire su internet
- Verificare che il firewall sia raggiungibile e che la porta 1194 **UDP** (default modificabile) sia stata inoltrata verso il firewall

La modifica della modalità di funzionamento da Routed a Bridged o viceversa impone di **scaricare nuovamente i file di configurazione.**

Questo poichè il client che si connette deve sapere in anticipo se attivare un tipo di interfaccia tun o tap.
Questa informazione è contenuta nel file di configurazione

Creazione regole di firewall

- Associazione utente-> indirizzo ip
  - http://helpdesk.nethesis.it/solution/articles/3000038186-e-possibile-assegnare-un-ip-statico-ad-un-utente-openvpn-
- Creazione oggetto host con indirizzo ip
- Creazione di regole di firewall sull'indirizzo ip definito



Vs

Agisce su tutto il traffico VPN :
RoadWarrior, Net to Net (OpenVPN e IPsec)

Agisce SOLO su traffico VPN RoadWarrior

- Instradare tutto il traffico su vpn
  - http://helpdesk.nethesis.it/solution/articles/3000075397-come-instradare-tutto-il-traffico-sulla-vpn-host-to-net-
- Instradare traffico verso reti ulteriori
  - Tutte le *Rotte Statiche* vengono aggiunte alla vpn
    - Es: aggiungere rete Blue (di default instradata solo Green)
- Passare DNS e WINS
- Rete da raggiungere identica a quella di provenienza
  - http://helpdesk.nethesis.it/solution/articles/3000071281-openvpn-roadwarrior-host-to-net-con-rete-sorgente-e-destinazione-uguali

Perchè IPsec

PRO

- Standard de facto implementato su tutti gli apparati di rete
  - Scelta *quasi* obbligata per interfacciare NethSecurity con apparati di terze parti

CONTRO

- Backup del tunnel automatico con MultiWAN non gestito

Perchè OpenVPN

PRO

- Protocollo moderno, non richiede IP pubblico su entrambi gli apparati solo sul lato Server
- Permette di gestire il backup automatico della VPN in presenza di MultiWAN
- Semplice da configurare

CONTRO

- Net to Net supportata nativamente da pochi dispositivi

2 Modalità : **p2p** e **subnet**

Entrambe le modalità permettono di creare una net 2 net tra 2 sedi in modo semplice e rapido.

p2p:

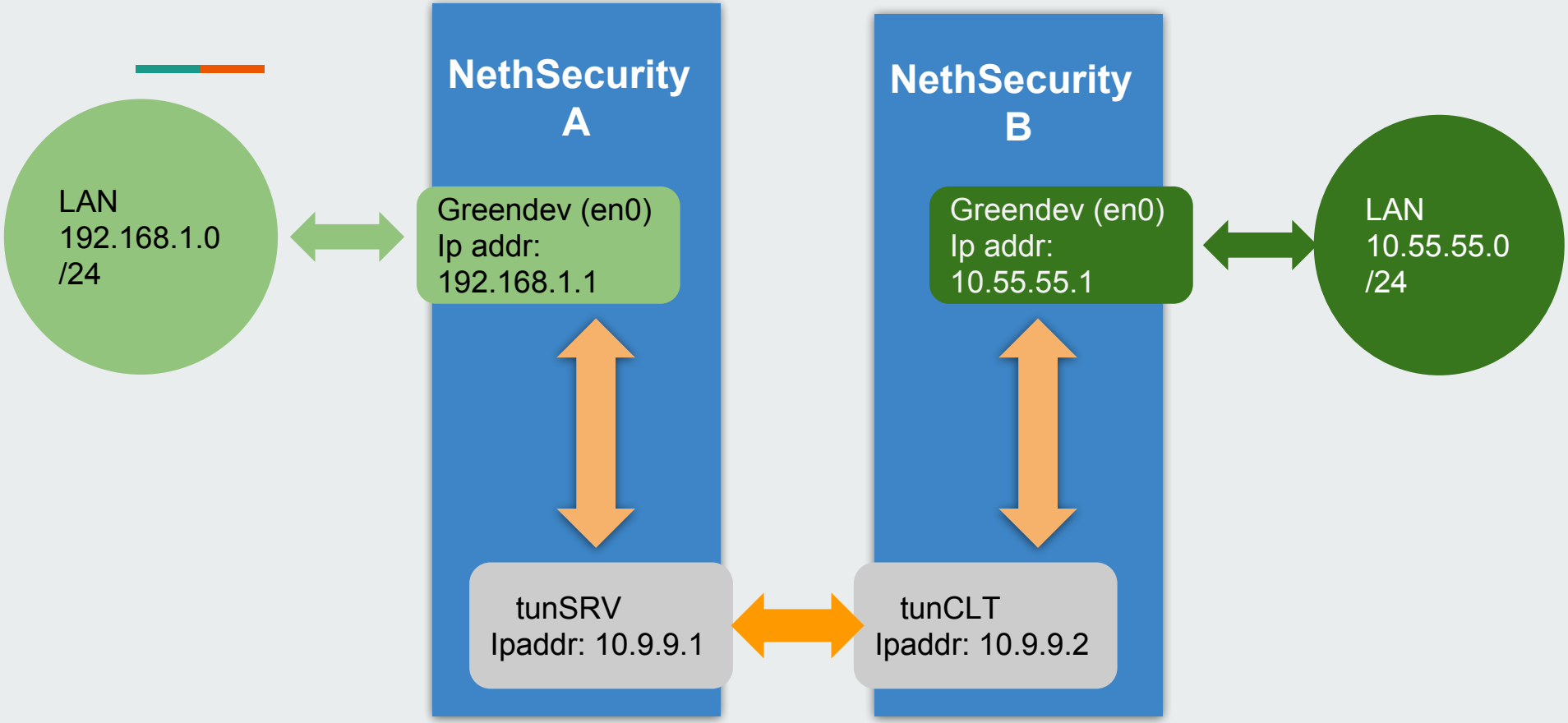
- Usa una chiave precondivisa (PSK)
- Compatibile con OpenVPN net to net su NethSecurity 1.5.0
- Ogni tunnel lavora su una porta differente e mette in comunicazione 2 soli firewall, ognuno ha un ip corrispondente al ptp (point to point)

Subnet:

- Simile alla modalità Roadwarrior
- Utilizza dei certificati
- Teoricamente più tunnel possono essere stabiliti con lo stesso server

VPN Net to Net Il traffico passa su interfaccia dedicata

nethesis

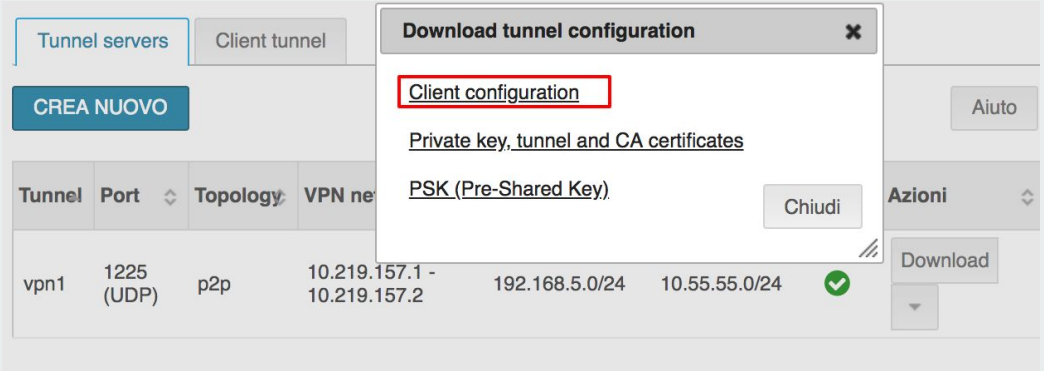


VPN Net to Net : OpenVPN - Configurazione Server

Configurazione molto semplice con pochi parametri, il sistema cerca di configurare automaticamente tutti i parametri possibili in modo da evitare errori.

- Configurare lato Server (quello in cui abbiamo l'IP pubblico, che può essere anche nattato)

- Esportare il file di configurazione e caricarlo nella sezione Client dell'altro Firewall



VPN Net to Net : OpenVPN failover con MultiWAN

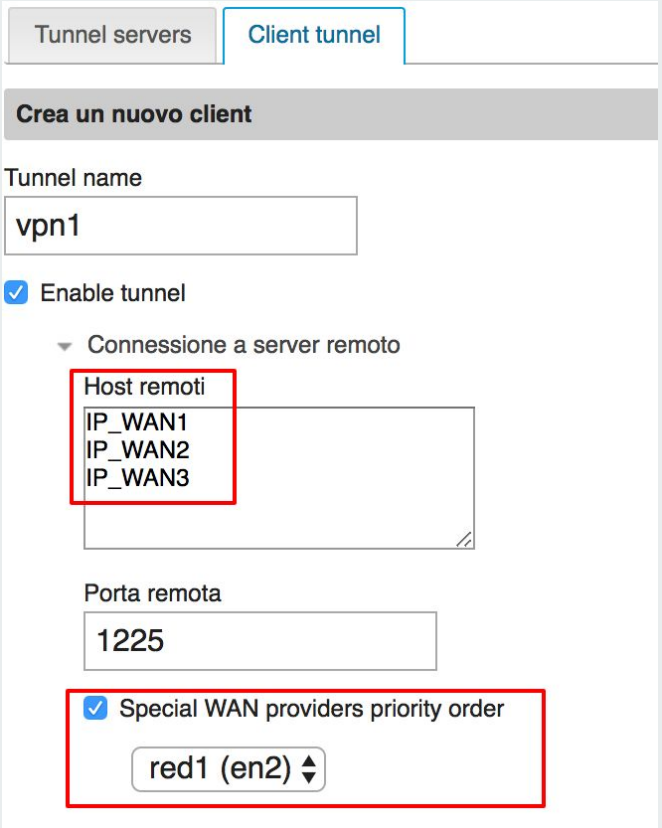
Se il server è collegato a più connettività è possibile fare in modo che il tunnel vpn si sposti sulla connettività secondaria quando la principale cade.

Indicare gli IP pubblici del server nell'ordine di utilizzo desiderato

VPN Net to Net : OpenVPN failover con MultiWAN

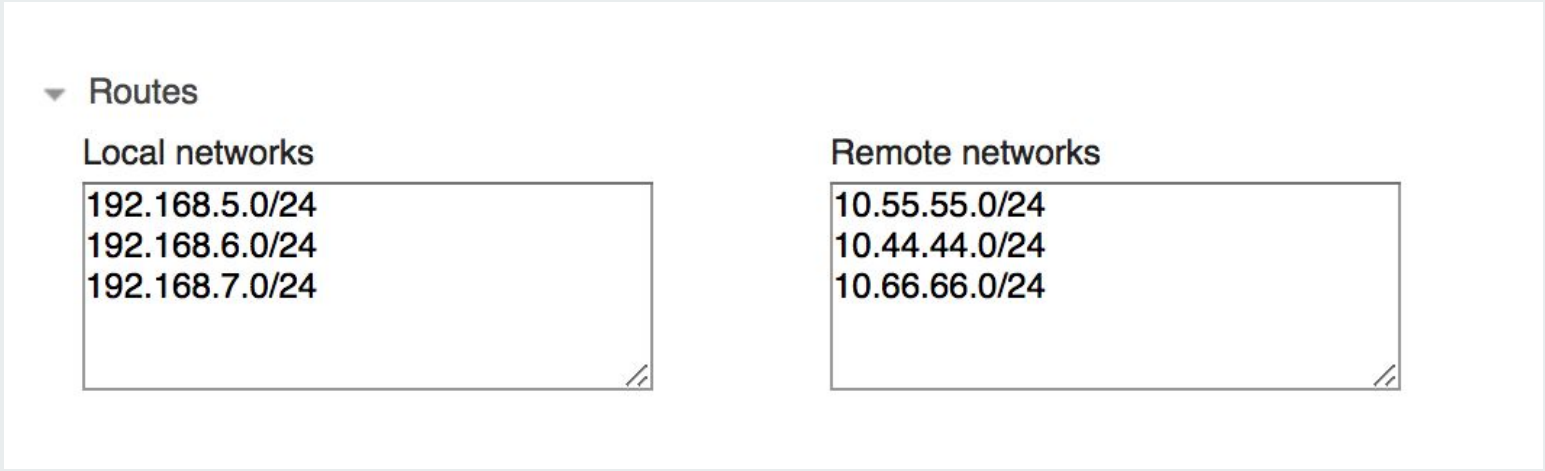
L'importazione del file sul client ne configura già correttamente gli IP da contattare

Se il client ha una MultiWAN è possibile scegliere l'ordine preferenziale di utilizzo delle RED



VPN Net to Net : In presenza di più reti locali o remote

E' sufficiente indicare le reti locali e remote raggiungibili tramite il tunnel



VPN Net to Net : OpenVPN - Analisi dei Log

nethesis

Analisi dei log da console ssh - Riferimento : nome_vpn

Es: nome_vpn = ***vpn1***

- Nome tunnel: tun**vpn1**
- Verifica log :

  ```
  # journalctl -u openvpn@vpn1
  ```

  Per vedere il log mentre viene scritto

  ```
  # journalctl -f -u openvpn@vpn1
  ```

- Analisi del traffico da console ssh:

  ```
  #tcpdump -p -nn -i tunvpn1
  ```

VPN Net to Net : IPsec - Configurazione

- IPsec utilizza le porte 500 UDP e 4500 UDP ed i protocolli AH e ESP, se il firewall non dispone di un IP Pubblico sulla propria RED è necessario inoltrare correttamente questo traffico dal router

- Per configurare la VPN IPsec è necessario che i parametri di rete (ip pubblici locale e remoto, reti locali, ID locale e remoto) siano **invertiti** tra le 2 sedi

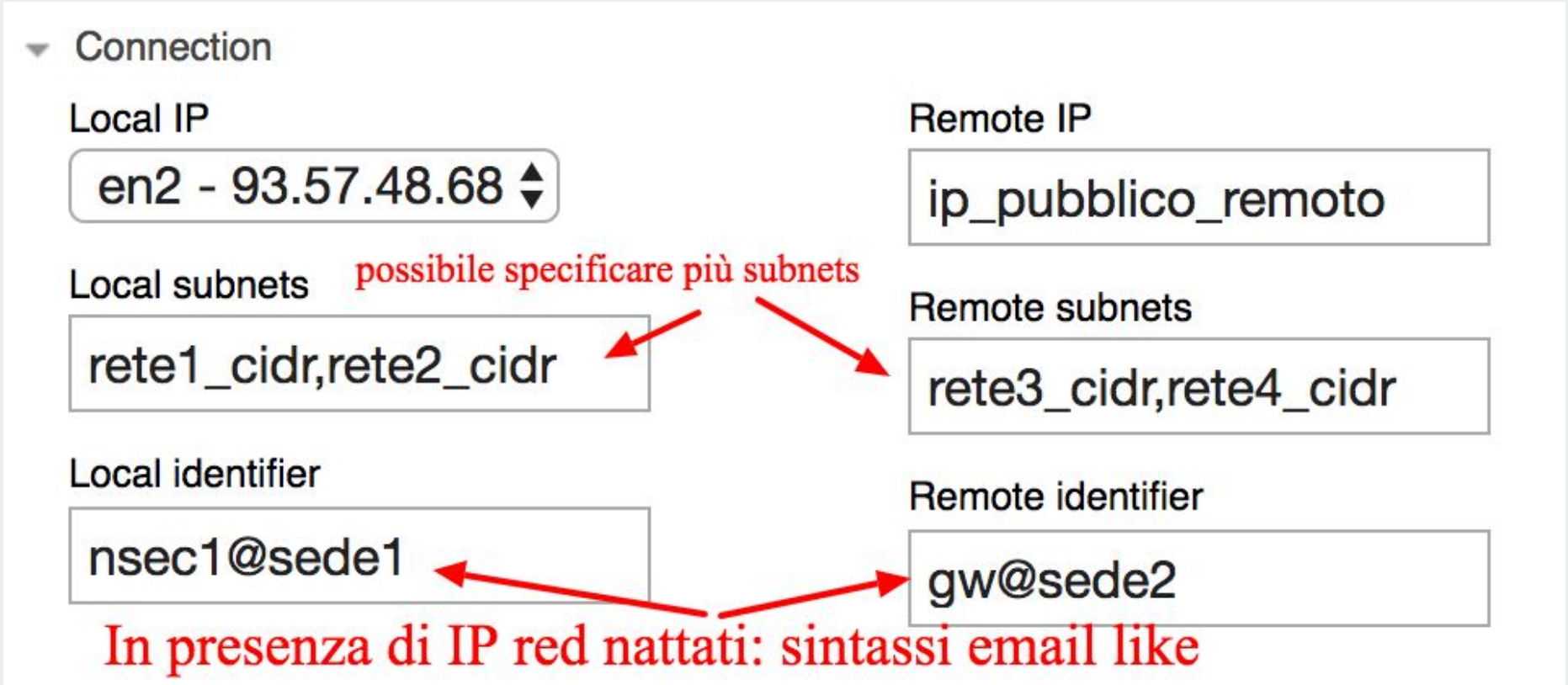
- Tutti gli altri parametri devono essere identici tra le 2 sedi

VPN Net to Net : IPsec - Configurazione

nethesis

VPN Net to Net : IPsec - Configurazione

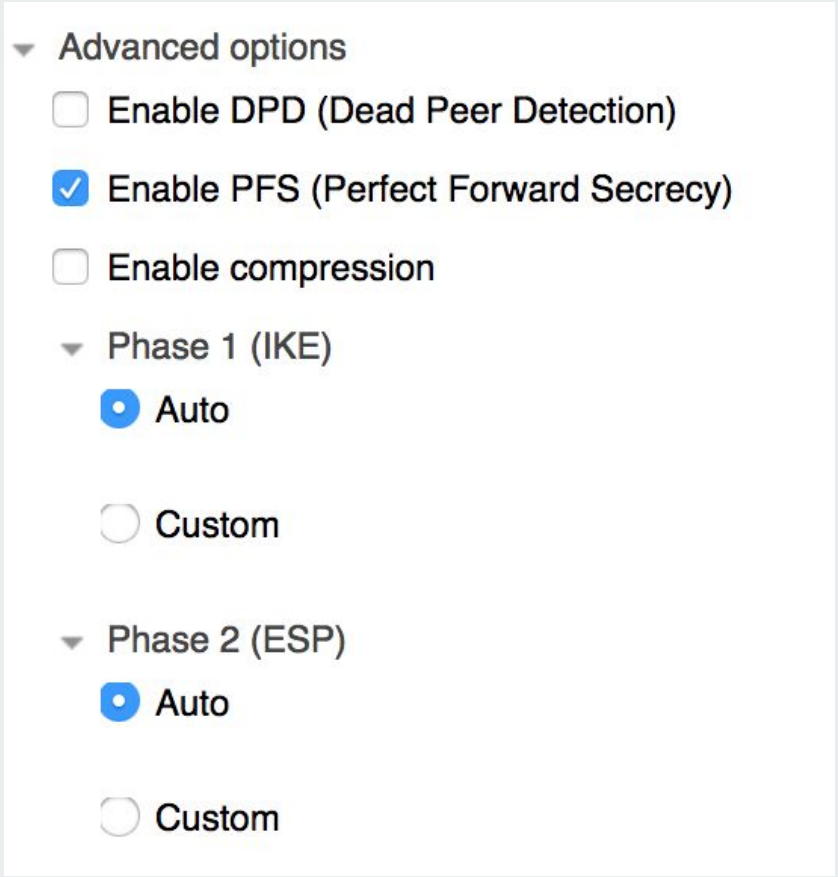
nethesis



VPN Net to Net : IPsec - Configurazione

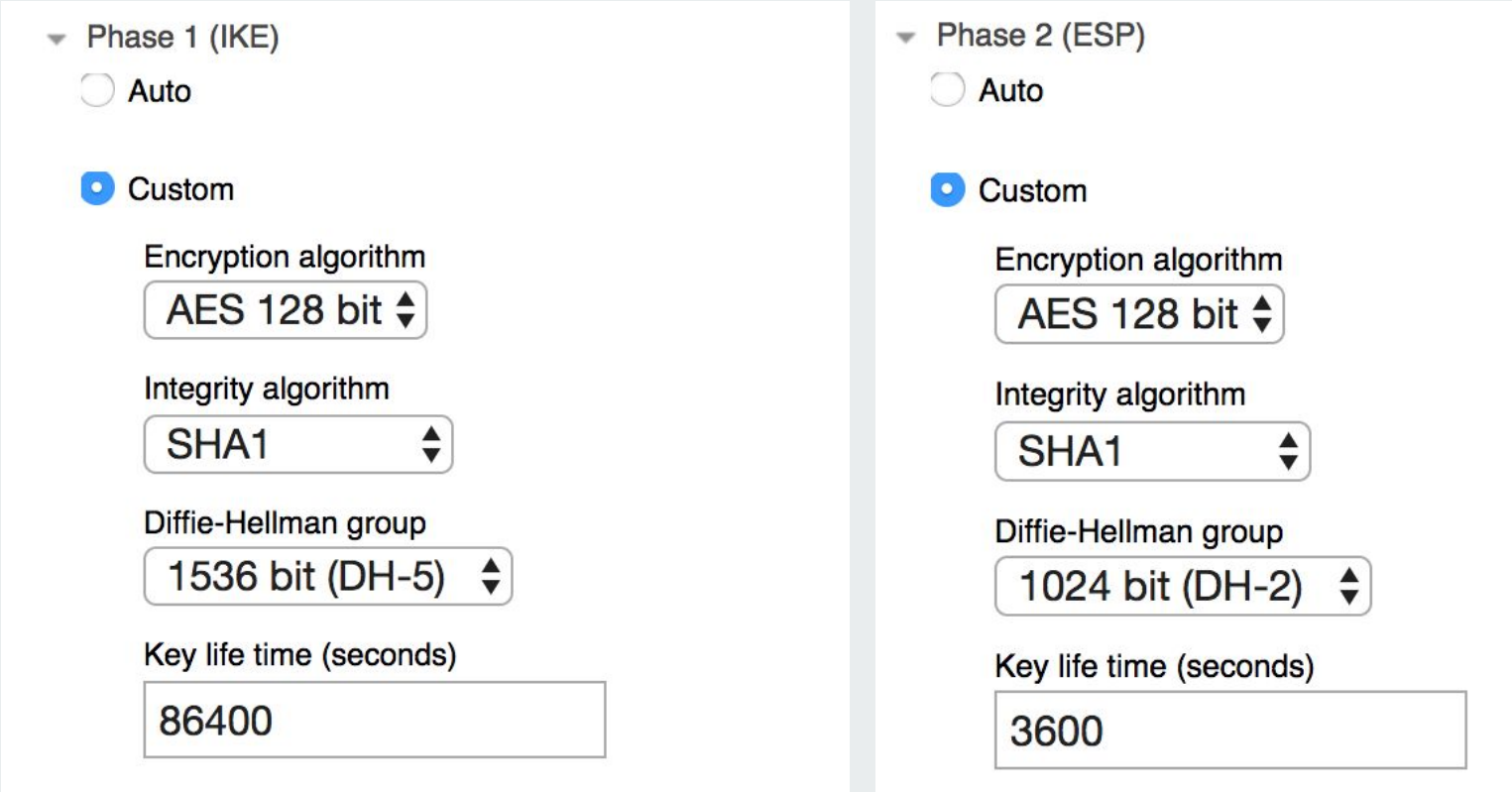
nethesis

Se la VPN è tra 2 NethSecurity NG è Possibile lasciare la modalità *Auto* per Phase 1 e 2



VPN Net to Net : IPsec - Configurazione

Se la VPN è con un apparato differente è necessario esplicitare tutti i parametri.



IKEv1 vs IKEv2

NethSecurity NG di default utilizza IKEv1

IKEv2 è permessa

Se l'altro apparato inizia una connessione utilizzando IKEv2 NethSecurity la permetterà

VPN Net to Net : IPsec - Troubleshooting

nethesis

Errori comuni :

- **Golden Rule**: essere molto scrupolosi e ricontrollare tutti i parametri di configurazione, nessuno escluso
- **Id remoto e Locale non coincidenti**
  - Nei log : `INVALID_ID`

    ```
    fw1 pluto[6769]: "ro-mi_ipsec-tunnel/1x1" #7117: no suitable connection for peer '192.168.6.78'
    fw1 pluto[6769]: "ro-mi_ipsec-tunnel/1x1" #7117: sending encrypted notification INVALID_ID_INFORMATION to 88.77.66.55:51261
    ```

  - Verificare che nell'altro apparato sia selezionata la sintassi *Email* (tipicamente può essere: IP, Email, FQDN)
- **Verificare che le reti locale e remota siano invertite negli apparati** e rispecchino le reti usate
- **Se il tunnel è stabilito ma il traffico non passa**: verificare il parametro *Compressione* nelle Avanzate
- E' buona norma condurre sempre i test da un client della rete, non dagli apparati di rete stessi

Analisi dei log da console ssh :

- VPN correttamente instaurata

```
# journalctl -u ipsec
```

```
Feb 22 13:11:39 nsec-roma.it pluto[28414]: "roma-milano_ipsec-tunnel/1x1" #1171: the peer proposed:
192.168.10/24:0/0 -> 192.168.66.0/24:0/0
Feb 22 13:11:39 nsec-roma.it pluto[28414]: "roma-milano_ipsec-tunnel/1x1" #1172: responding to Quick Mode
proposal {msgid:b6cc8caa}
Feb 22 13:11:39 nsec-roma.it pluto[28414]: "roma-milano_ipsec-tunnel/1x1" #1172:     us:
192.168.10/24===93.57.48.68<%en2>[@roma]
Feb 22 13:11:39 nsec-roma.it pluto[28414]: "roma-milano_ipsec-tunnel/1x1" #1172:   them:
2.229.91.58<2.229.91.58>[@milano]===192.168.66.0/24
Feb 22 13:11:39 nsec-roma.it pluto[28414]: "roma-milano_ipsec-tunnel/1x1" #1172: keeping refhim=0 during rekey
Feb 22 13:11:39 nsec-roma.it pluto[28414]: "roma-milano_ipsec-tunnel/1x1" #1172: transition from state
STATE_QUICK_R0 to state STATE_QUICK_R1
Feb 22 13:11:39 nsec-roma.it pluto[28414]: "roma-milano_ipsec-tunnel/1x1" #1172: STATE_QUICK_R1: sent QR1,
inbound IPsec SA installed, expecting QI2 tunnel mode {ESP=>0xf7c
Feb 22 13:11:39 nsec-roma.it pluto[28414]: "roma-milano_ipsec-tunnel/1x1" #1172: transition from state
STATE_QUICK_R1 to state STATE_QUICK_R2
Feb 22 13:11:39 nsec-roma.it pluto[28414]: "roma-milano_ipsec-tunnel/1x1" #1172STATE_QUICK_R2: IPsec SA
established tunnel mode {ESP=>0xf7c531a3 <0xf617676c xfrm=AES_128-
```

nethesis

Analisi dei log da console ssh :

- Verifica dei log mentre le parti cercano di stabilire la VPN

```
# journalctl -f -u ipsec
```

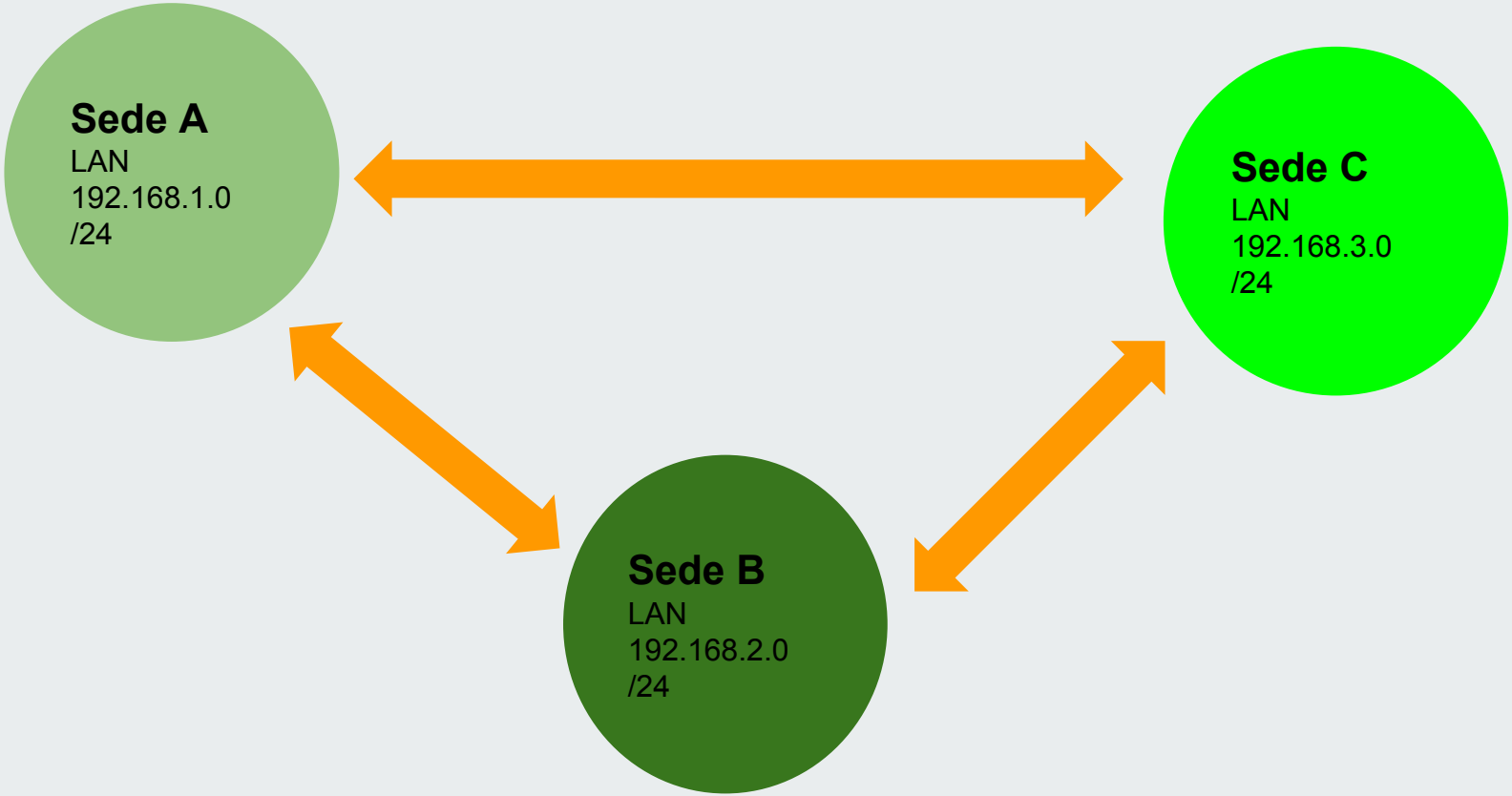
- Analisi del traffico passante su tunnel ipsec

```
# iptables -t mangle -I POSTROUTING -m policy --pol ipsec --dir out -j NFLOG --nflog-group 5
# tcpdump -s 0 -n -i nflog:5
```

Versione attuale di tcpdump (tcpdump-4.9.0-5.el7.x86_64) non funziona correttamente con i link di tipo NFLOG

esportare su altro sistema e analizzare con wireshark o versioni differenti di tcpdump

Come collegare tra di loro in VPN più di 2 sedi?



VPN Net to Net : VPN tra più sedi

nethesis

E' necessario creare un tunnel tra ogni coppia di sedi, es: sedi A-B-C

1. Tunnel A-B
2. Tunnel B-C
3. Tunnel A-C

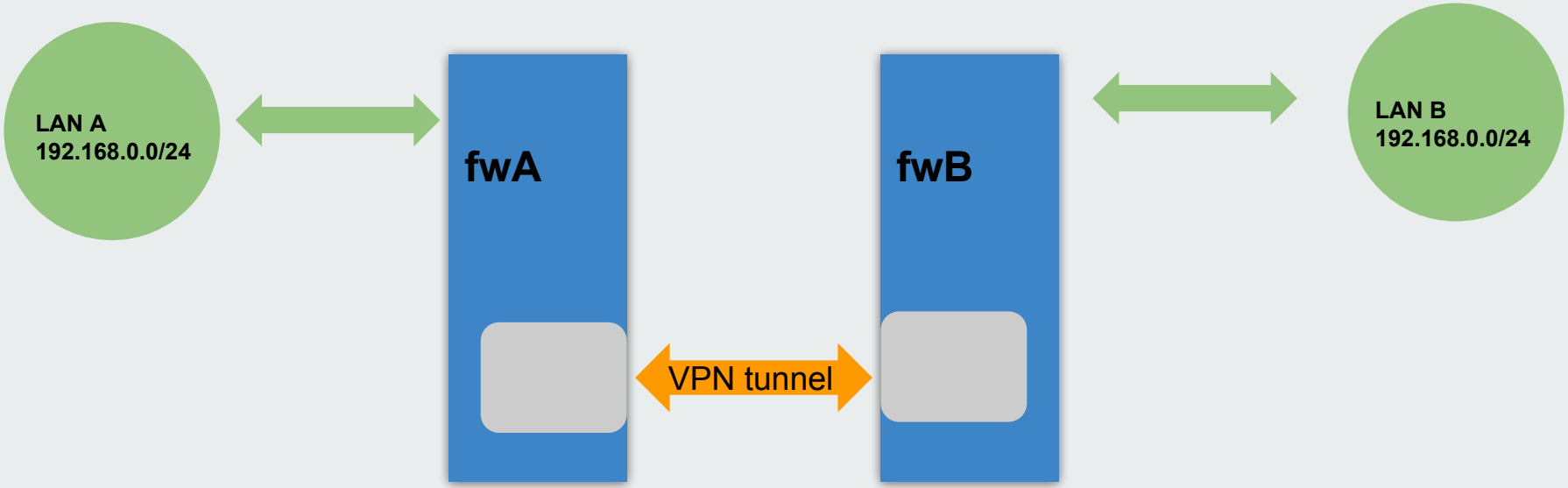
In questo modo:

- Il transito tra le 2 sedi è diretto
  - più rapido
  - non consuma banda della sede intermedia
  - non soggetto a problemi se la sede intermedia ha malfunzionamenti

La configurazione è valida sia per OpenVPN che per IPsec

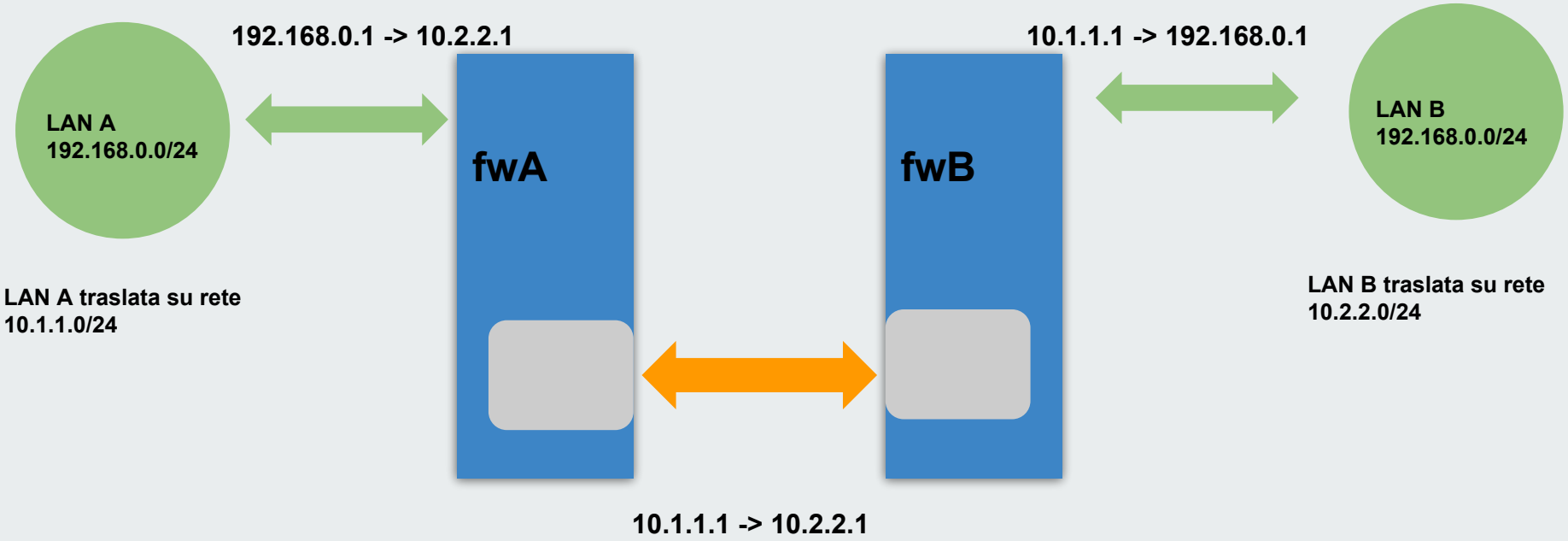
VPN Net to Net : Problemi

Rete Locale e rete Remota uguali



- Rete da raggiungere identica a quella di provenienza
  - http://helpdesk.nethesis.it/solution/articles/3000075550-vpn-net-to-net-con-rete-locale-e-remota-coincidenti

Rete Locale e rete Remota uguali -> NAT delle Reti



Grazie per l'attenzione