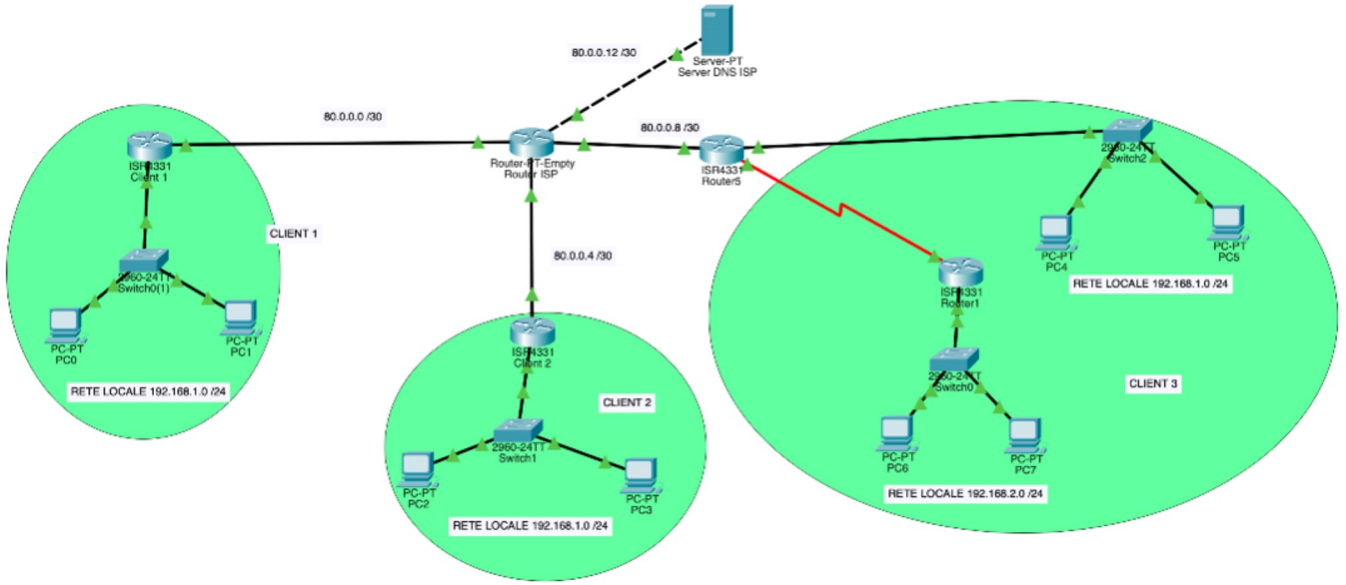
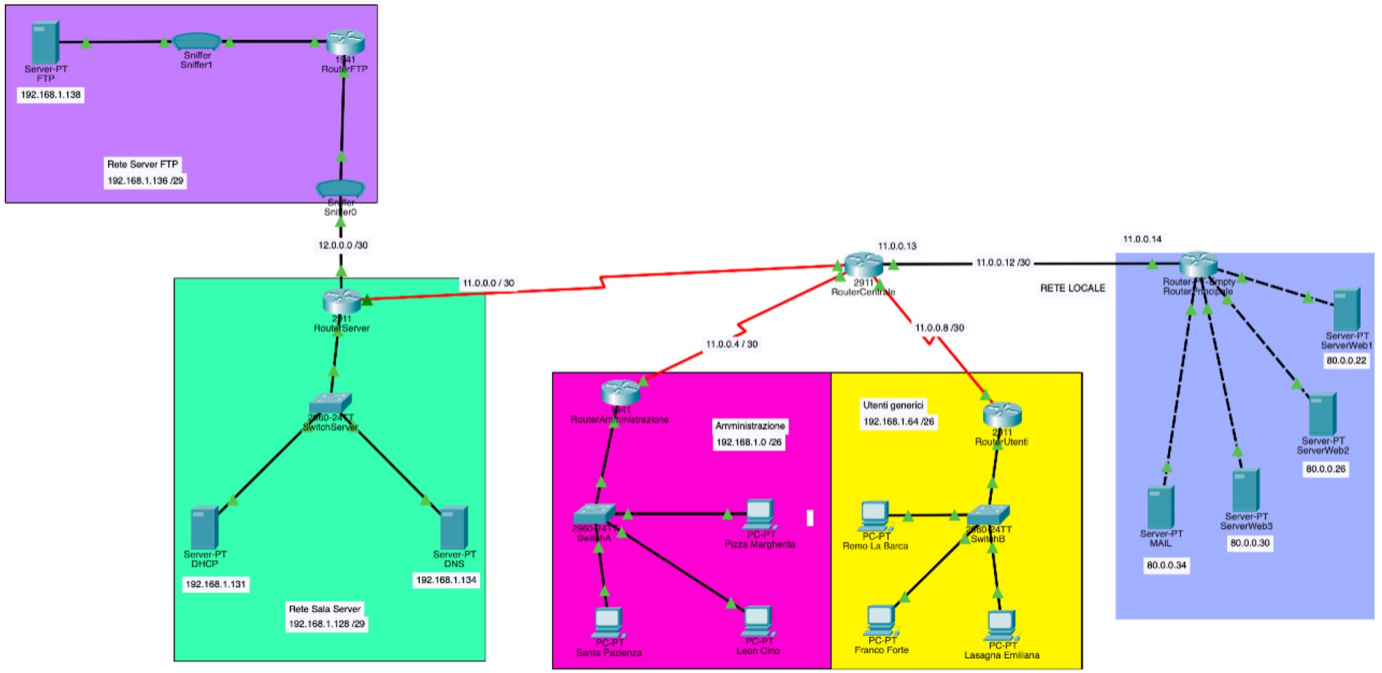
Lazzareschi, Mariani, Pardini, Pucci - 5BIF

Indice

1.1
Rete esterna



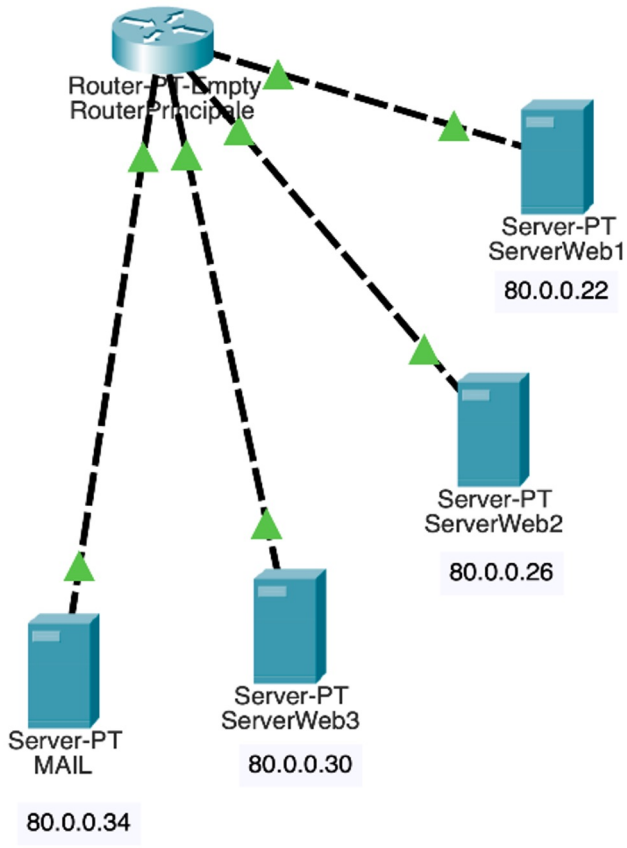
1.2
Rete aziendale



Servizi esposti

L’azienda permette l’accesso da reti esterne ai propri server web e mail

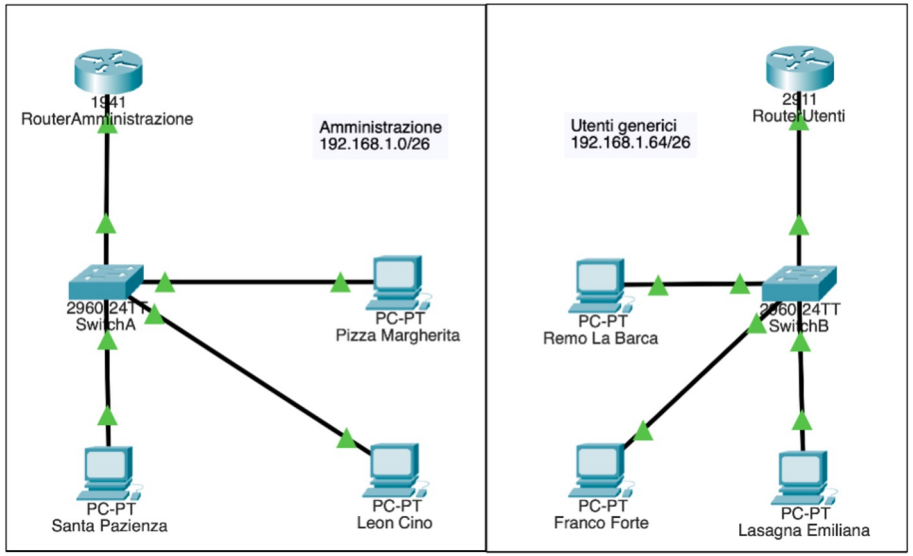
Nome Server	IP pubblico
ServerWeb1	80.0.0.22
ServerWeb2	80.0.0.26
ServerWeb3	80.0.0.30
Server Mail	80.0.0.34



Rete amministrazione e client

La rete aziendale prevede due sottoreti per i client

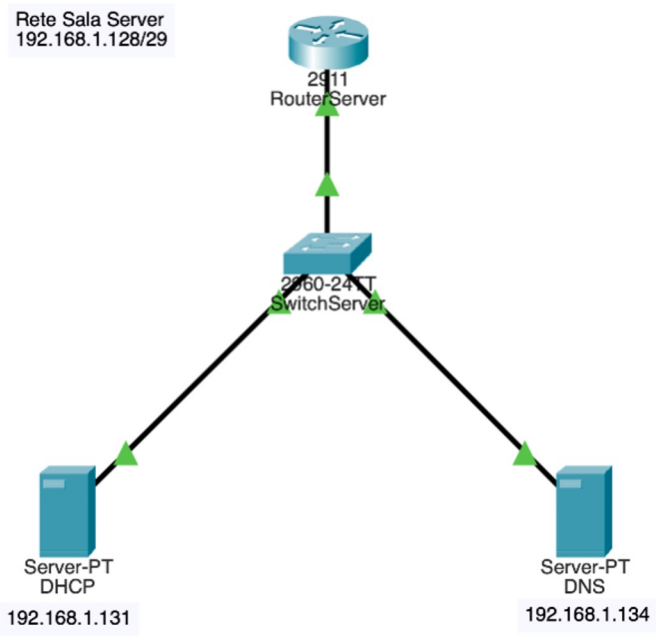
Nome rete	Indirizzo di rete
Amministrazione	192.168.1.0 /26
Utenti generici	192.168.1.64 /26



Rete server

Indirizzo di rete: 192.168.1.128/29
È composta da due server:

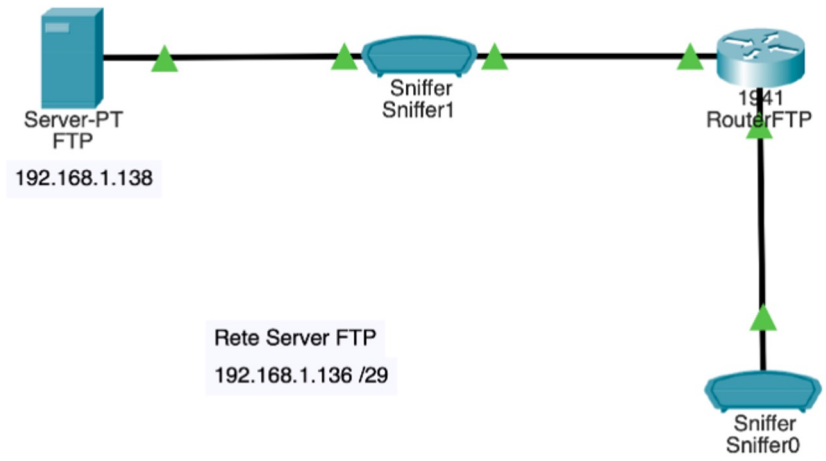
Nome server	Indirizzo IP
DHCP	192.168.1.131
DNS	192.168.1.134



Rete server FTP

Indirizzo di rete: 192.168.1.136/29
È composta da due server:

Nome server	Indirizzo IP
FTP	192.168.1.138



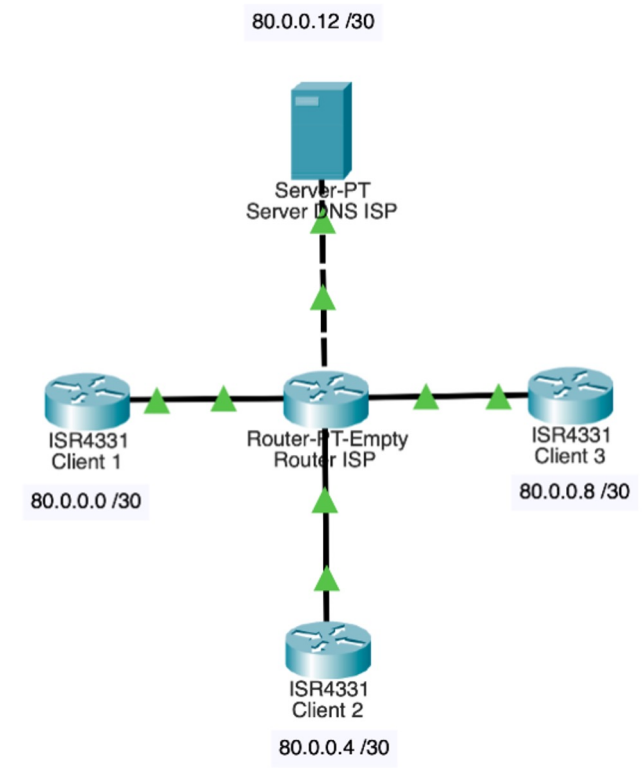
02

Subnetting

Maschera fissa

L’ISP effettua il subnetting a maschera fissa /30 del blocco di indirizzi a sua disposizione: 80.0.0.0

Rete	Indirizzo IP
Client 1	80.0.0.0/30
Client 2	80.0.0.4/30
Client 3	80.0.0.8/30
Server DNS	80.0.0.12/30



Maschera variabile

All’interno della rete aziendale si ricorre al subnetting a maschera variabile per creare reti di dimensione congrua a quella necessaria.
Nello specifico:

- **Sala server** e **Sala server FTP** hanno come maschera 255.255.255.248
- Rete amministrazione e utenti generici hanno invece come subnet 255.255.255.192

Nome rete	Indirizzo IP
Amministrazione	192.168.1.0 /26
Utenti generici	192.168.1.64 /26
Sala Server	192.168.1.128 /29
Sala Server FTP	192.168.1.136 /29

03

Routing

Routing

Le rotte sono state impostate nel seguente modo:

OSPF

- Router FTP
- Router Server
- Router Centrale
- Router Amministrazione
- Router Utenti
- Router Principale

RIP

- Router principale
- Router secondario

Statico

- Router Client 1
- Router Client 2
- Router Client 3

04

Servizi

DHCP Aziendale

Il server DHCP interno all'azienda ha come indirizzo 192.168.1.131 /29

Pool name	Default gateway	DNS Server	Start IP address	Subnet Mask	Max User
Client 1	192.168.1.1	192.168.1.134	192.168.1.2	255.255.255.192	61
Client 2	192.168.1.65	192.168.1.134	192.168.1.66	255.255.255.192	61

Nei router è poi stato configurato l'ip helper-address.

```
Router (config-int) # ip helper-address 192.168.1.131
```

DNS Aziendale

Il server DNS interno all'azienda ha come indirizzo 192.168.1.134 /29 e al suo interno sono stati configurati i seguenti record:

Name	Type	Detail
smtp.robertone.it	A Record	80.0.0.34
pop.robertone.it	A Record	80.0.0.34
robertone.it	A Record	80.0.0.22
robertone.it	A Record	80.0.0.26
robertone.it	A Record	80.0.0.30

Server FTP

Il server FTP ha indirizzo IP statico 192.168.1.138 /29. L'accesso a quest'ultimo è consentito solo dalla rete dell'amministrazione tramite VPN e ACL come descritto nei punti seguenti.

Username	Password	Permissions
cisco	cisco	RWDNL
leoncino	pippo	RWDNL
pizzamargherita	pippo	RWDNL
santapazienza	pippo	RWDNL

Server email

Il server mail ha indirizzo IP statico 80.0.0.34 /30 e offre servizi SMTP e POP3.

Sono state configurati le seguenti mail.

Username	Password	E-Mail
santapazienza	pippo	santapazienza@robertone.it
leoncino	pippo	leoncino@robertone.it
pizzamargherita	pippo	pizzamargherita@robertone.it
lasagnaemiliana	pippo	lasagnaemiliana@robertone.it
francoforte	pippo	francoforte@robertone.it
remolabarca	pippo	remolabarca@robertone.it

05

NAT

Scopo e funzionamento del NAT

Il NAT è un protocollo che sta alla base del funzionamento di internet e permette di tradurre degli indirizzi locali in indirizzi globali e viceversa.
Ad esempio, ogni rete domestica dispone di più indirizzi locali (almeno uno per ogni host), ma un solo indirizzo pubblico.

L'uso del NAT inevitabilmente porta con sé il problema relativo a quale host (con indirizzo IP privato) recapitare un pacchetto indirizzato ad un determinato indirizzo pubblico.
Ciò viene gestito tramite delle politiche definite nel router di destinazione.

Configurazione del NAT

Quando un host (interno) invia un pacchetto a degli host esterni, l'indirizzo IP sorgente verrà sostituito con l'indirizzo IP pubblico assegnato dall'ISP. Così facendo, il router tiene traccia della trasformazione dell'IP ed è in grado di smistare i pacchetti di ritorno all'host interno che ha iniziato la comunicazione tramite la propria NAT Table.

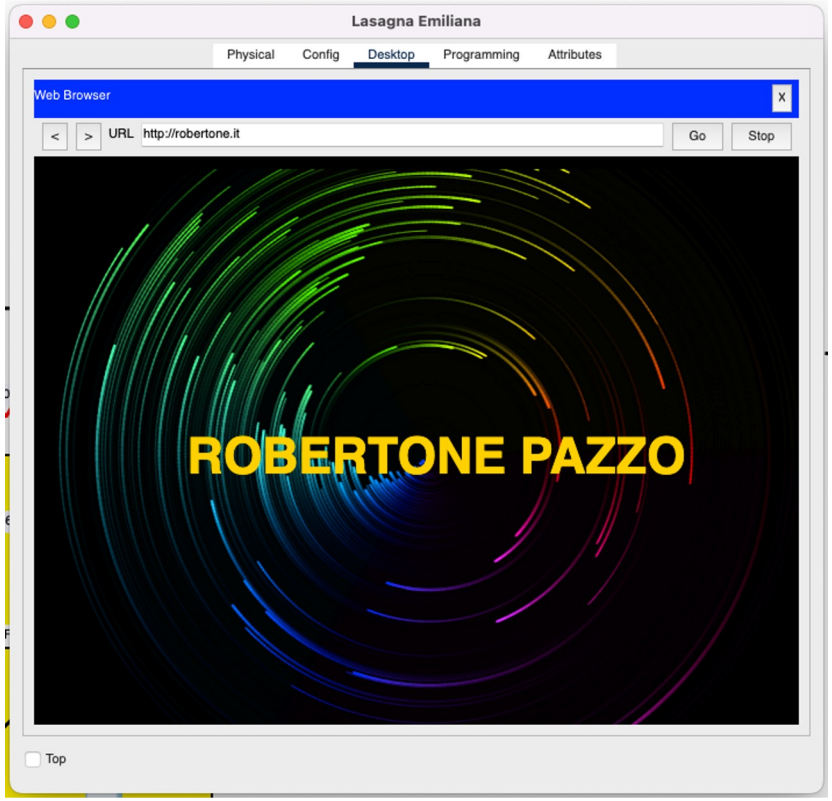
```
Router(config) # ip nat inside source list 1 interface ethernet 2/0 override

Router(config) # interface Ethernet 1/0
Router(config-if) # ip nat inside

Router(config) # interface Ethernet 2/0
Router(config-if) # ip nat outside
```

Server WEB

Il server Web distribuito è stato configurato impostando 3 record DNS con il medesimo dominio, ma con traduzioni in IP differenti.
Così facendo il server DNS risponde alle query DNS alternando i record secondo la politica round-robin.



Distribuzione tramite NAT

Disponendo di router fisici sarebbe stato possibile utilizzare politiche di NAT dinamico per tradurre l'indirizzo IP pubblico in indirizzi IP privati differenti distribuendo quindi il carico sui vari cloni.
I comandi che permettono di effettuare l'operazione in questione sono i seguenti.

```
Router(config) # ip nat pool POOL <primo-ip> <ultimo-ip> netmask
<subnetmask> type rotary

 Router(config) # ip nat outside destination <indirizzo-pubblico> pool
POOL
```

ACL Standard

È stata configurata una ACL sulla porta GigabitEthernet 0/1 del router RouterFTP per regolare l'accesso al server FTP. In particolar modo, si stabilisce che vi possano accedere solamente gli host appartenenti alla rete relativa all'amministrazione.

```
RouterFTP (config) # access-list 9 permit 192.168.1.0 0.0.0.63
RouterFTP (config) # interface GigabitEthernet0/1
RouterFTP (config-if) # ip access-group 9 in
```

ACL Estesa

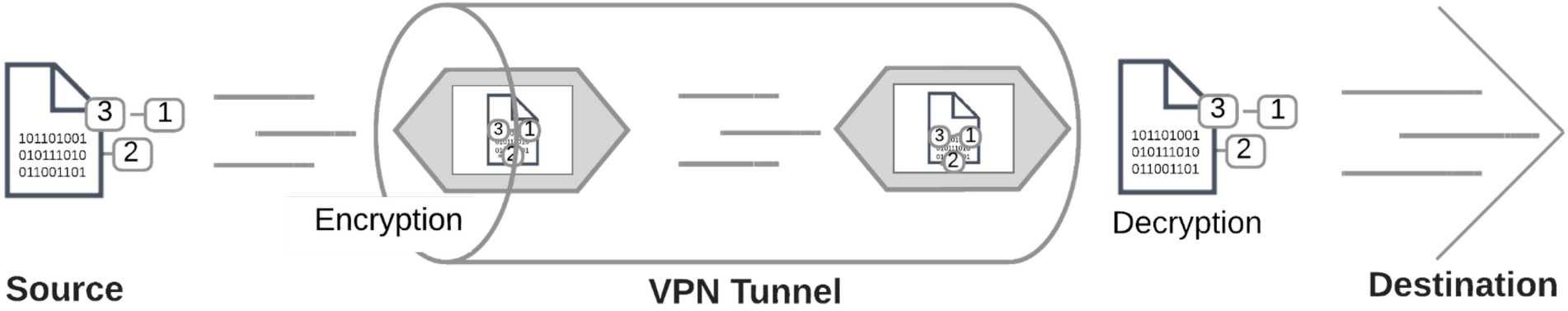
Per regolare poi l'accesso dall'esterno ai server mail e web è stata impostata un'ACL che accetta solamente il traffico (dell'appropriato protocollo) rivolto verso i server della DMZ.

```
RouterPrincipale (config) # ip access-list extended SoloSRV
RouterPrincipale (config-ext-nacl) # permit tcp any host 80.0.0.34 eq pop3
RouterPrincipale (config-ext-nacl) # permit tcp any host 80.0.0.34 eq smtp
RouterPrincipale (config-ext-nacl) # permit tcp any host 80.0.0.24 eq www
RouterPrincipale (config-ext-nacl) # permit tcp any host 80.0.0.26 eq www
RouterPrincipale (config-ext-nacl) # permit tcp any host 80.0.0.26 eq www
RouterPrincipale (config-ext-nacl) # permit tcp any host 80.0.0.30 eq www
```

06

VPN

VPN



Una VPN è una connessione privata tra dispositivi che viene creata avvalendosi di un canale di rete insicuro.

IPSEC

IPSEC è una suite di protocolli che autentica e cripta i pacchetti per fornire una comunicazione crittografata sicura tra due computer su una rete di protocollo Internet.

È composto da:

- protocolli che implementano lo scambio delle chiavi per la realizzazione del flusso crittografato: IKE
- protocolli che forniscono la cifratura del flusso di dati
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)

Modalità di funzionamento

Transport mode

- Connessione host to host.
- Prevede solo la cifratura del payload
- Gli host devono avere un software apposito per gestire la comunicazione

Tunnel mode

- Connessione gateway to gateway
- Prevede la cifratura di tutto il pacchetto
- I gateway devono avere un software apposito per gestire la comunicazione

Trasmissione con e senza VPN