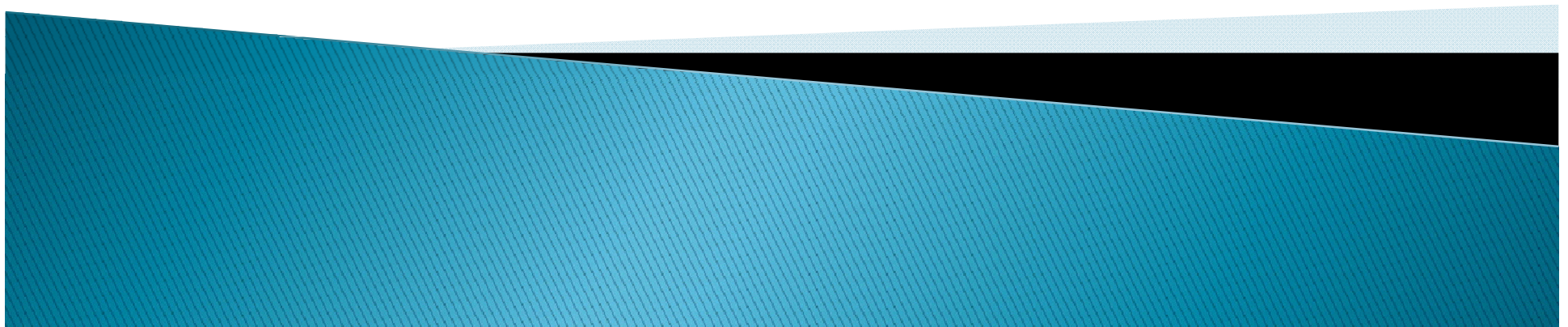
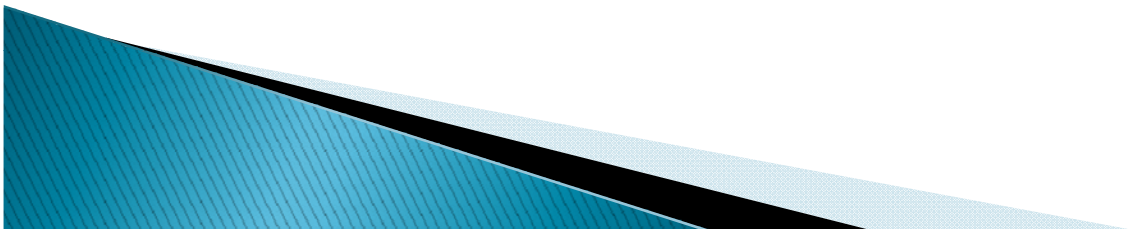


Virtual Private Networks



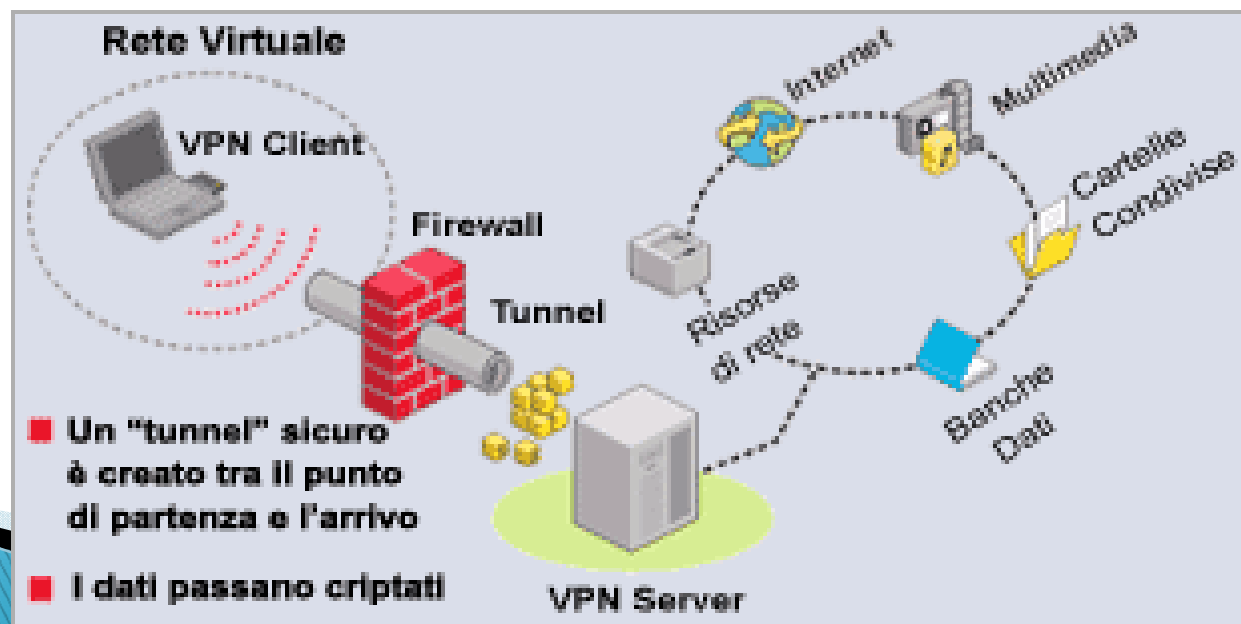
Problema

- ▶ 1. I domini di collisione sono insicuri
- ▶ 2. I dipendenti hanno spesso necessità di accedere remotamente alle risorse di rete aziendali
 - Il traffico via Internet è molto più vulnerabile all'eavesdropping di quello che circola in una rete interna aziendale.
- ▶ 3. Più filiali remote possono avere esigenza di accedere alle stesse risorse

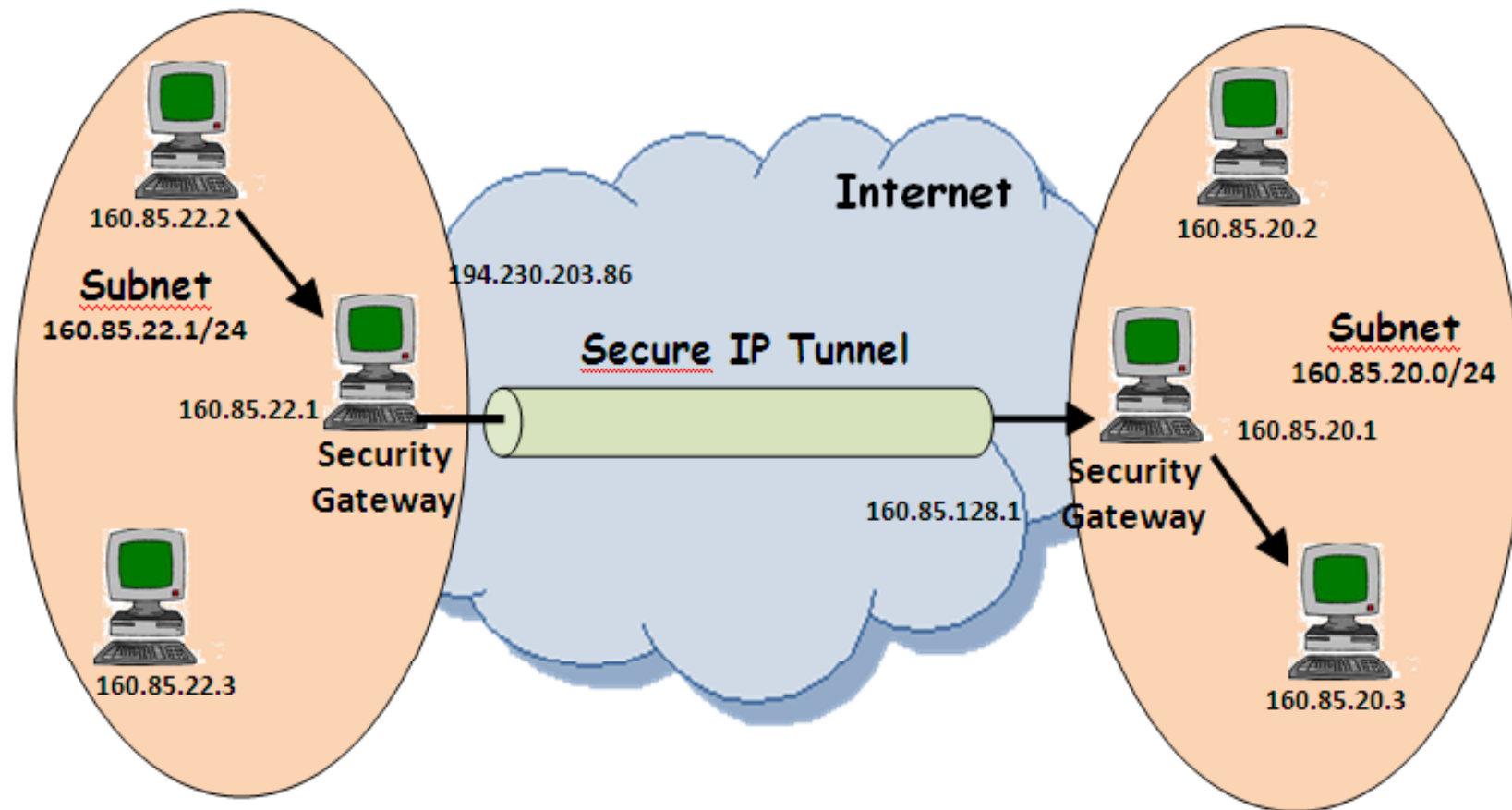


Quindi?

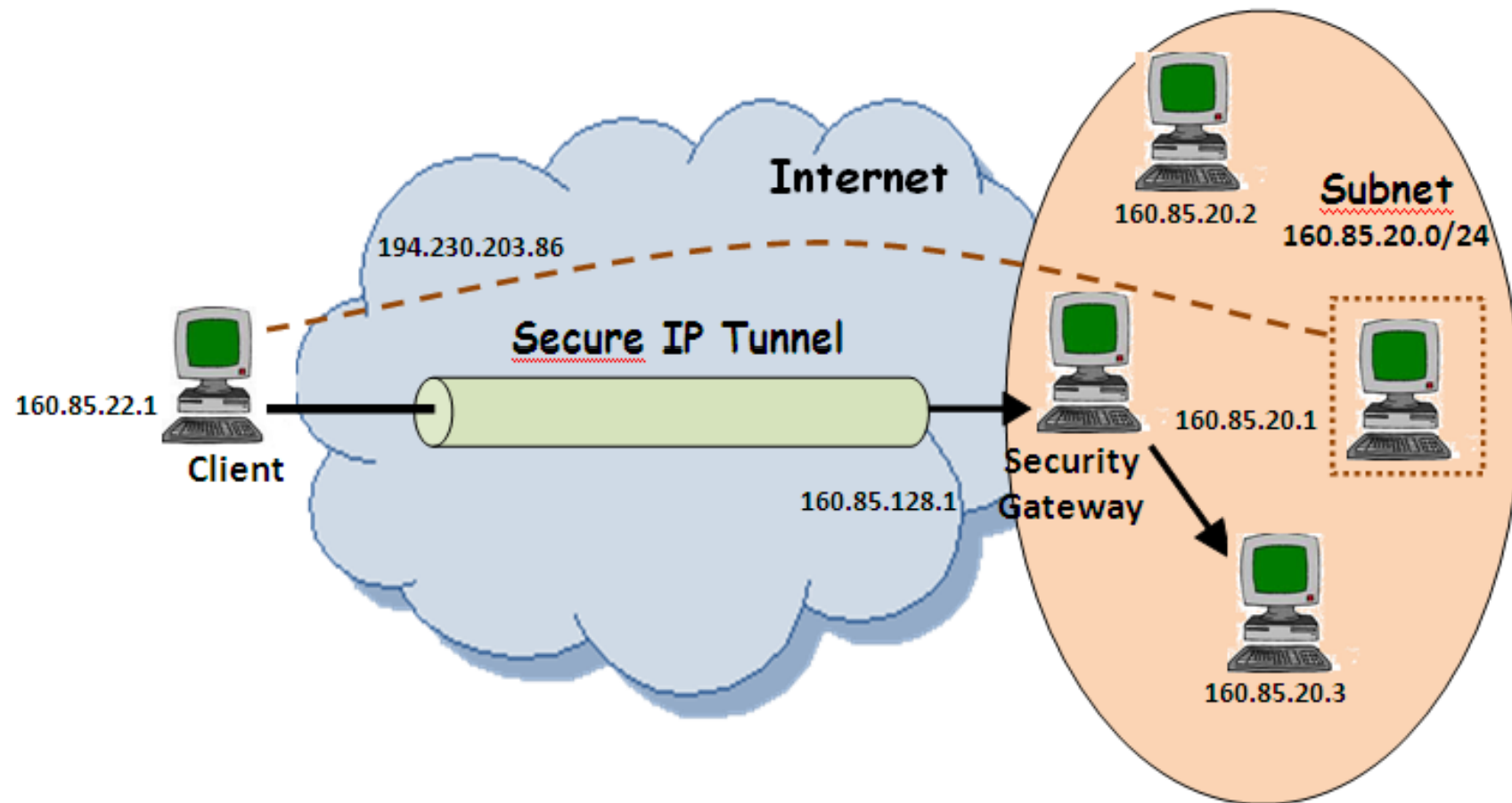
- ▶ **Idea:** creare un dominio di collisione *artificiale* che utilizza una rete fisica sottostante (internet) come supporto di trasmissione e attraverso un protocollo di *tunneling* consente di incapsulare i dati da trasmettere (crittografandoli)
- ▶ **Obiettivo:** ottenere una subnet sicura e trasparente con un costo minimo



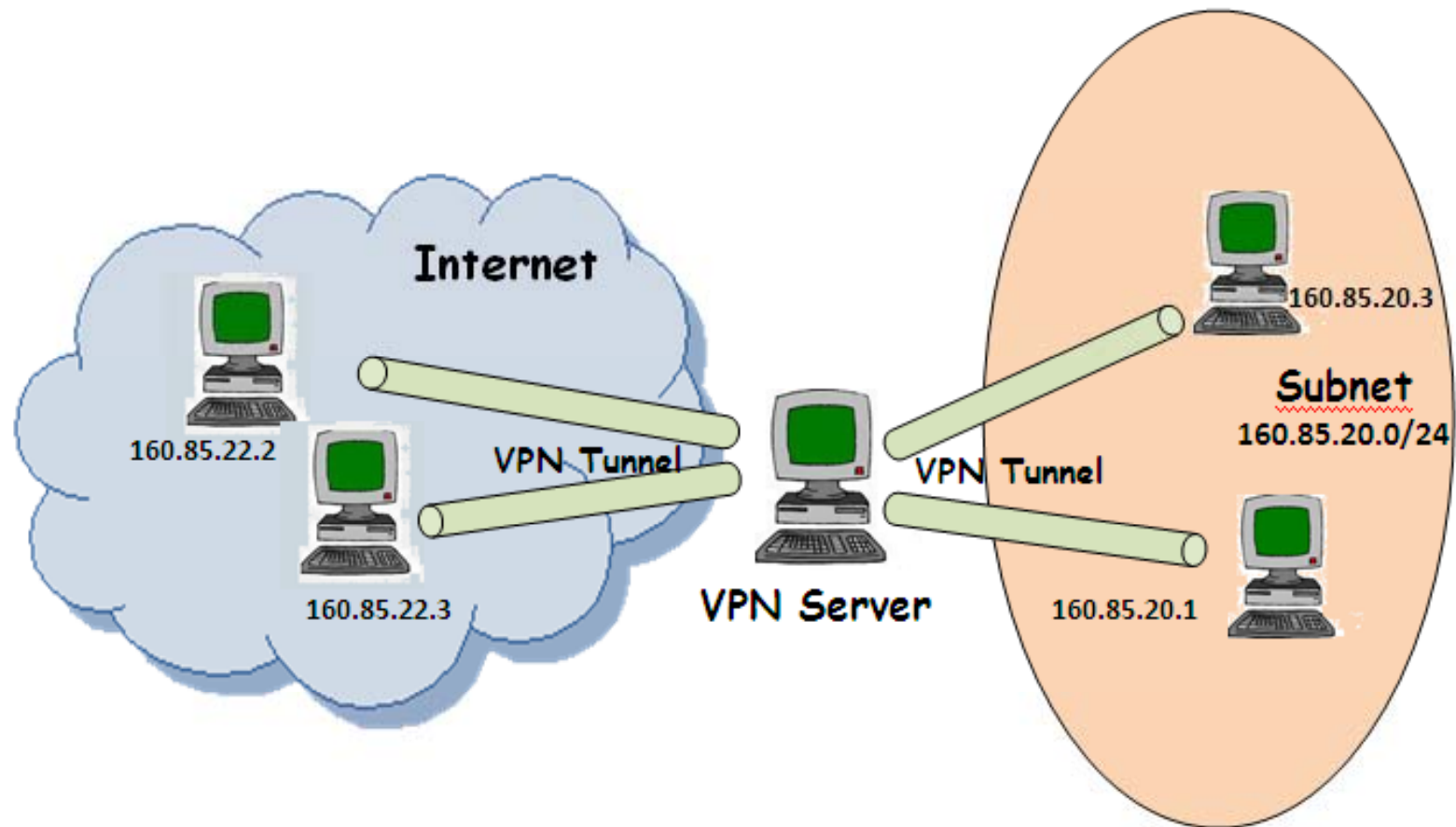
VPN LAN-2-LAN



VPN for Roadwarriors



Many-to-many Secured VLAN



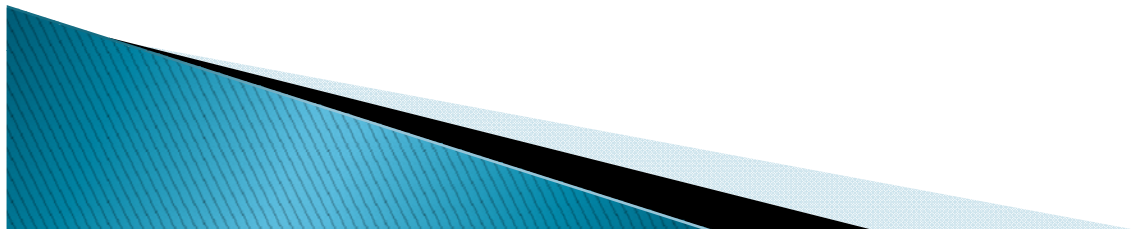
Cos'è una Virtual Private Network?

- Il termine è generico, può descrivere diverse configurazioni di reti e protocolli...
- **Virtuale**: è una rete *artificiale* che si poggia su una sottostante rete fisica
- **Privata**: i dati viaggiano incapsulati o non visibili dal traffico della rete sottostante
- Funziona come una “pipe all'interno di una pipe”, dove quella esterna è costituita dalla connessione della rete sottostante
 - Internet può essere usata come piattaforma di comunicazione
 - Instaura dei canali puramente logici e sicuri tra le varie sezioni



Caratteristiche di una VPN

- ▶ Cifratura dei dati
 - Conversazioni riservate
- ▶ Verificabilità dell'identità di ogni stazione
 - Meccanismi di autenticazione
- ▶ Le sezioni remote risultano *logicamente* appartenenti alla stessa rete locale della sede centrale
 - Gli utenti possono accedere a tutte le applicazioni e banche dati della sede centrale, come se si trovassero fisicamente sulla stessa LAN



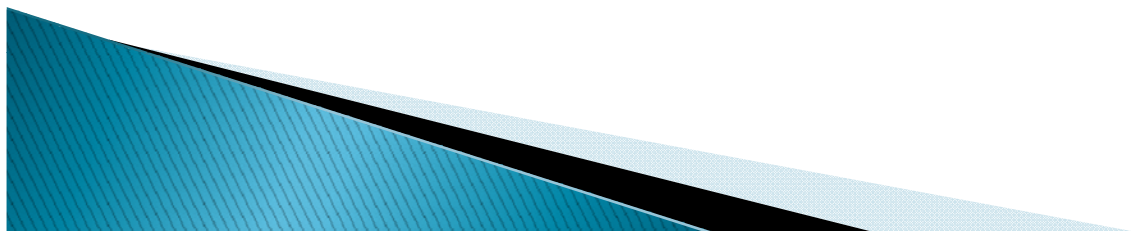
Vantaggi di una VPN?

- ▶ Riduzione dei costi (grazie all'utilizzo di Internet)
 - Connessione di sedi remote senza i costi di una linea dedicata
- ▶ Scalabilità
 - Aggiungere un numero potenzialmente illimitato di nuove sezioni
- ▶ Sicurezza e protezione dei dati che viaggiano sulla rete
- ▶ Possibilità di far accedere alla rete aziendale anche utenti esterni all'azienda

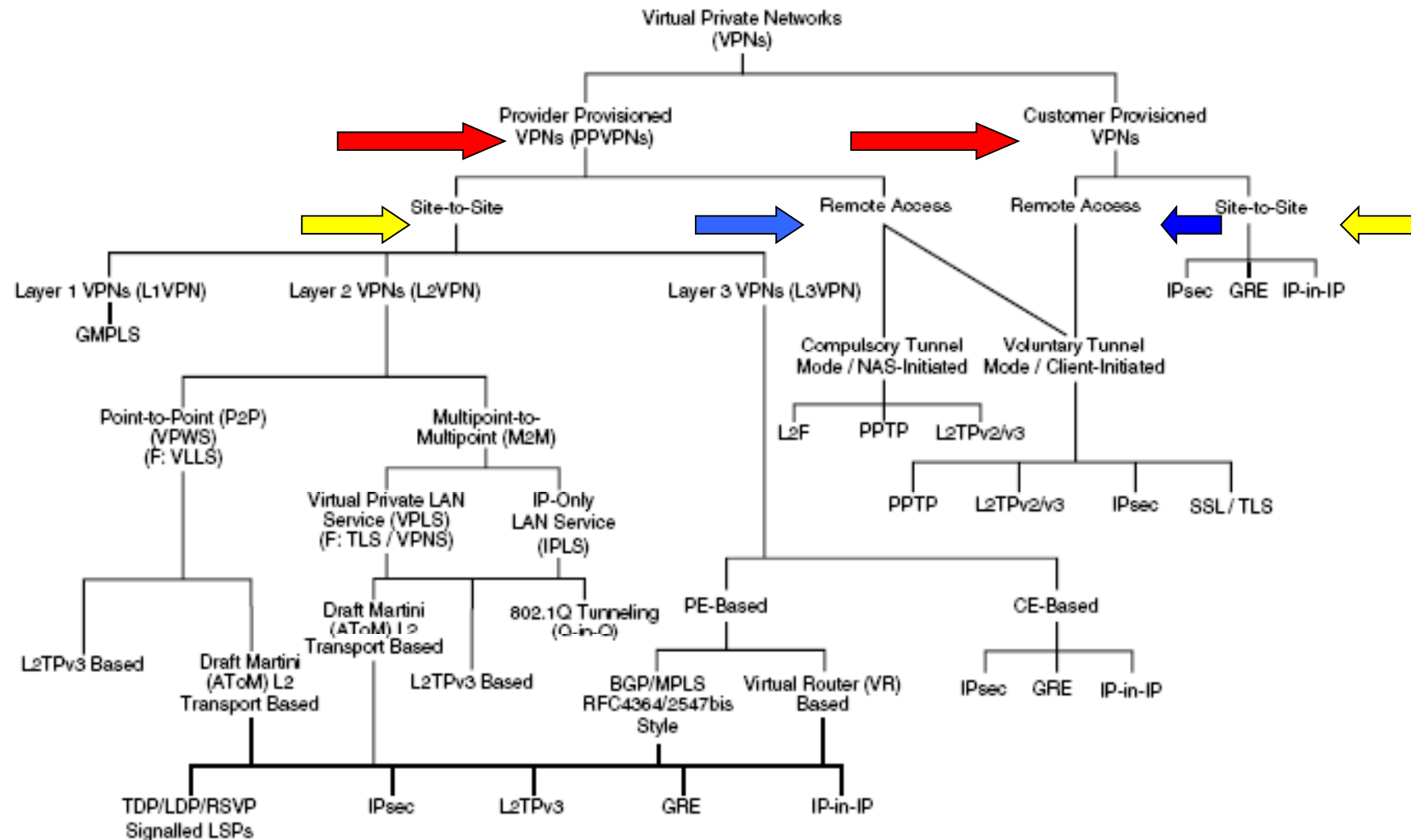


Classificazione (in base a ..)

- ▶ Protocolli di *tunneling* utilizzati
- ▶ Localizzazione del “tunnel termination”
 - lato utente o network provider
- ▶ Tipologia di accesso
 - site-to-site, remote access connectivity
- ▶ Livello di sicurezza garantito
- ▶ Livello OSI che si espone verso la rete di connessione
 - Layer 2 circuits, Layer 3 network connectivity

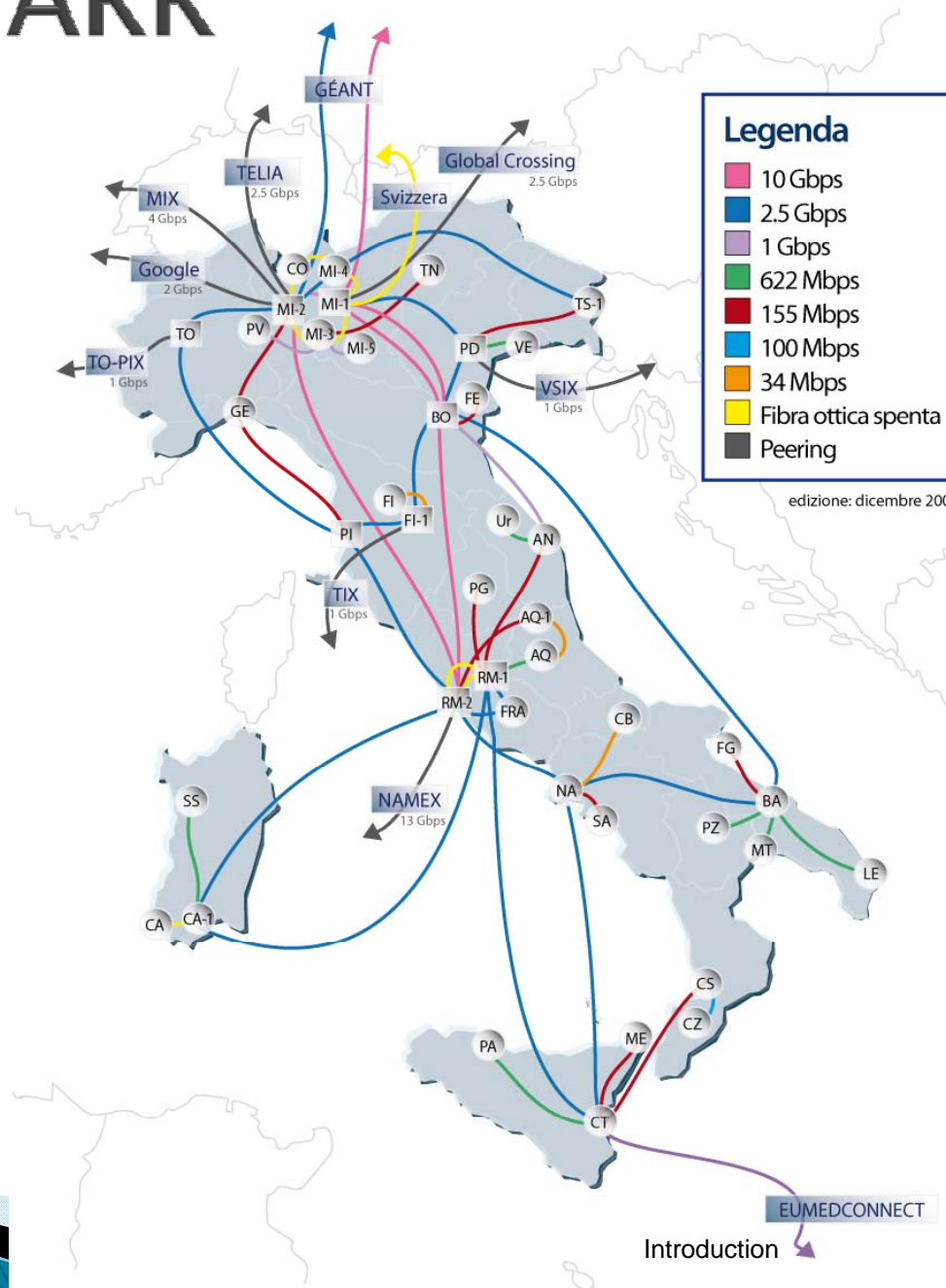


Classificazione



La rete GARR

Topologia di backbone di GARR-G



Introduction

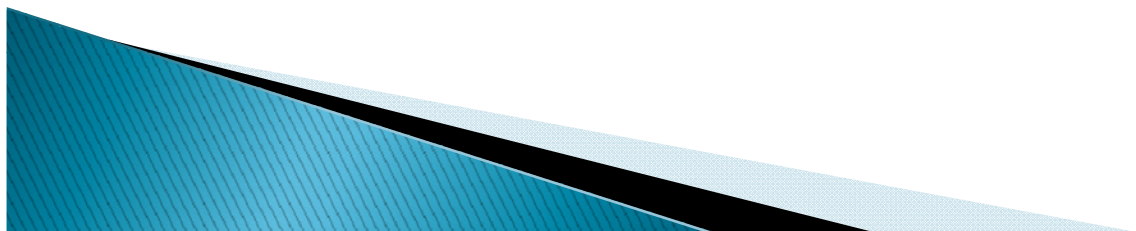
Classificazione tradizionale

- ▶ **Intranet VPN:** collega uffici periferici o sedi di una società
- ▶ **Remote access VPN:** collega sede centrale di una società con utenti remoti o mobili
- ▶ **Extranet VPN:** collega la sede centrale con partners, clienti, fornitori
- ▶ Ciascuna tipologia ha diversi requisiti in termini di sicurezza e tecnologia
 - Intranet VPN: protezione informazioni, performance delle risposte, scalabilità
 - Remote VPN access: autenticazione forte, sistema efficiente di gestione centralizzata degli account
 - Extranet VPN: utilizzo piattaforme standard e aperte



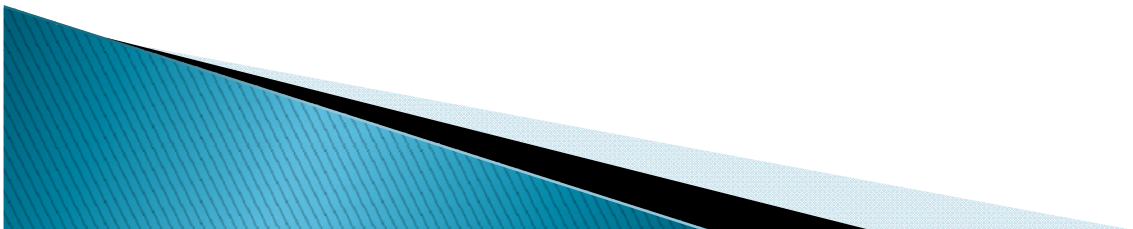
Secure VPN

- ▶ Meccanismi di autenticazione per gli endpoints del tunnel (durante la fase di setup del tunnel)
- ▶ Cifratura del traffico in transito
- ▶ Il traffico viene criptato e questo crea un un *“Tunnel”* tra due reti/host
- ▶ Le “Secure VPN” hanno uno o più tunnel e ogni tunnel ha due estremità



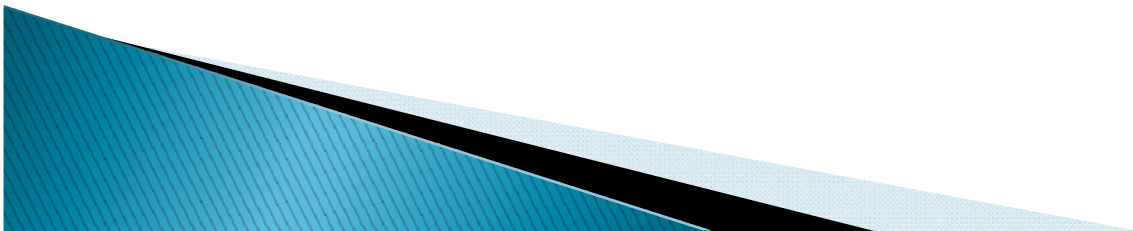
Secure VPNs

- ▶ Una VPN per essere definita una secure VPN deve garantire:
 - un sistema di autenticazione
 - i dati devono viaggiare criptati
 - il livello di cripting dei dati deve essere elevato e modificabile nel tempo



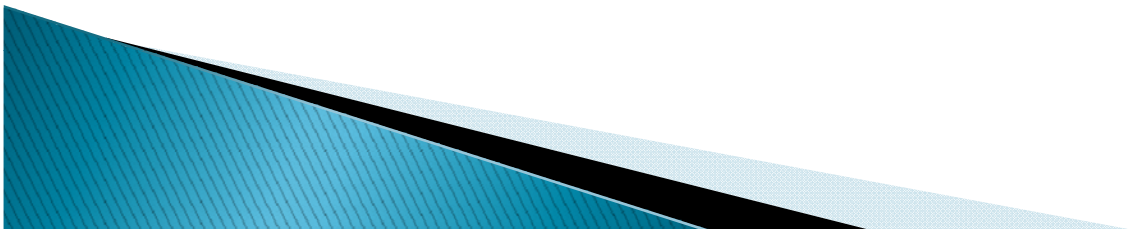
Secure VPNs

- Sono usate:
 - Per proteggere il traffico quando internet è la rete di appoggio o se il livello di sicurezza offerto dalla rete sottostante differisce da quello richiesto dal traffico interno alla VPN
 - In uno scenario di accesso remoto, dove un client VPN (utente finale) si connette in modo sicuro ad un remote office network
 - Ad esempio, offrono utilità di accesso remoto ad impiegati di una organizzazione



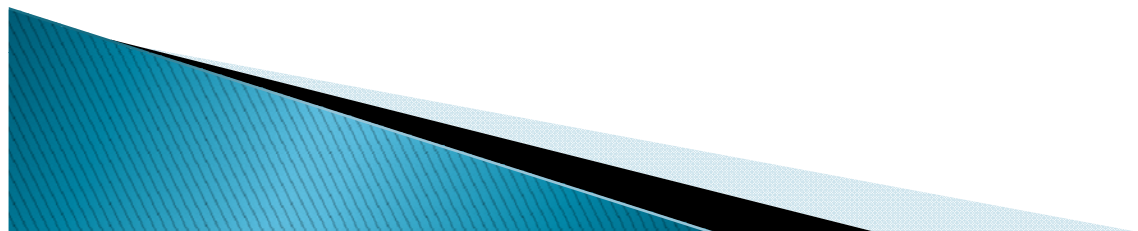
Secure VPNs

- ▶ Tecnologie e protocolli utilizzati (non tutti standard IETF) :
 - SSH Tunneling
 - SSL/TLS VPN (con SSL/TLS)
 - OpenVPN
 - PPTP/SSTP (con MPPE).
 - IPsec 'puro'
 - Ipsec+L2TP



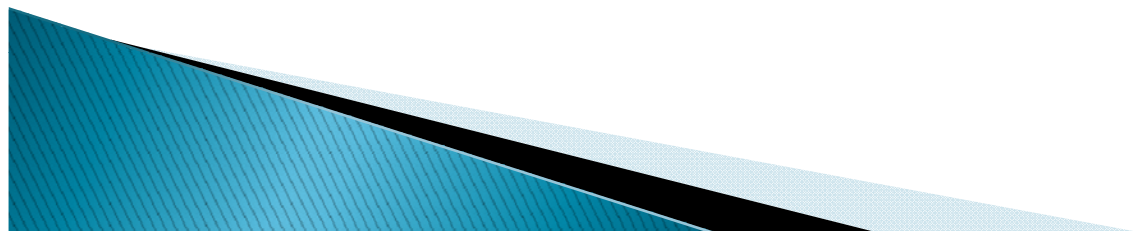
Security Protocols (Secure VPN)

- **IPsec (Internet Protocol Security)**
 - Sviluppato per Ipv6, ma usato anche per IPv4
 - Obiettivo di introdurre sicurezza:
 - Cifratura del traffico: traffico letto solo dai destinatari
 - Integrità
 - Autenticazione dei peers

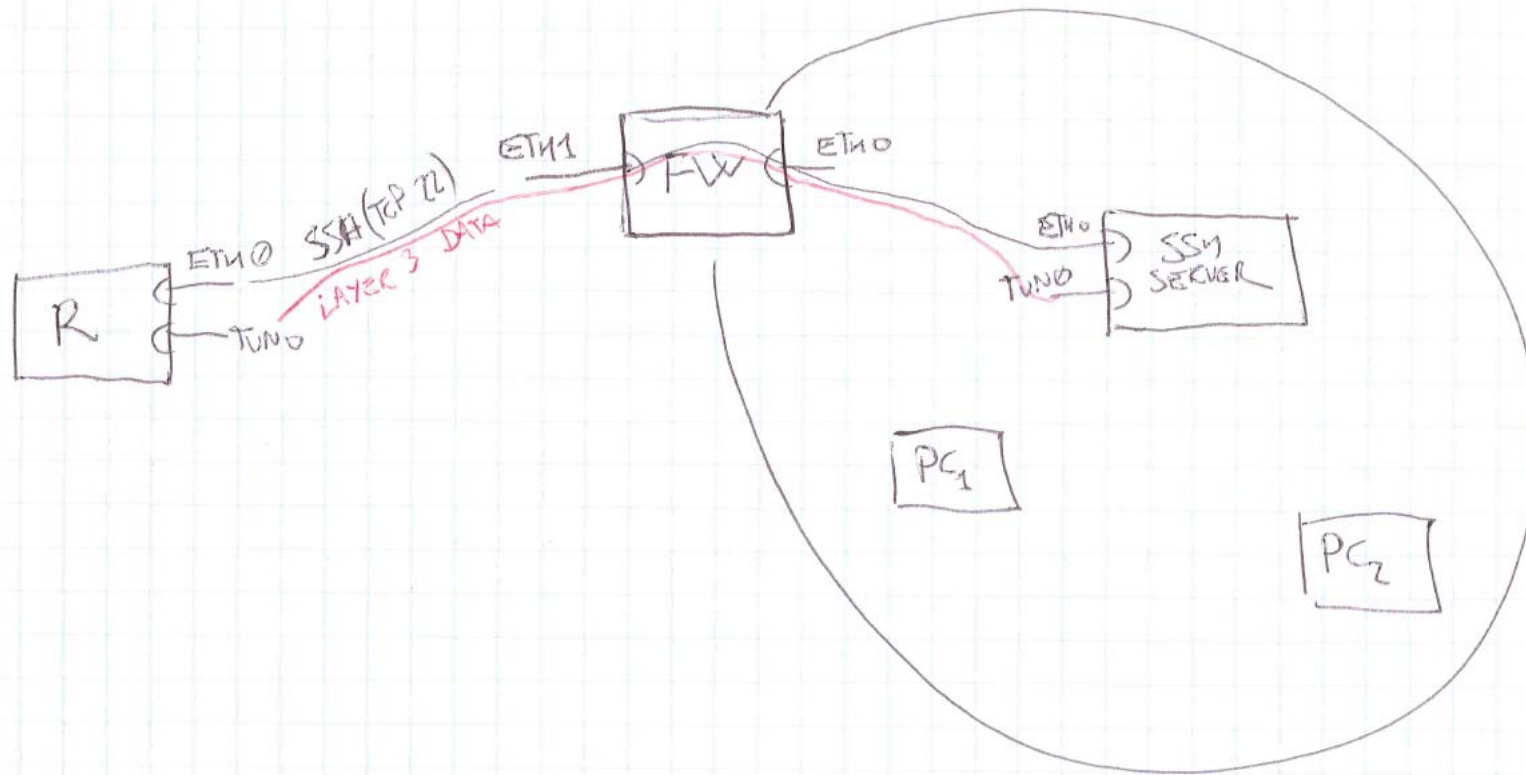


Security Protocols (Secure VPN)

- IPsec (Internet Protocol Security)
 - Standard:
 - Encapsulating Security Payload (ESP): fornisce autenticazione, confidenzialità e controllo di integrità del messaggio;
 - Authentication Header (AH): garantisce l'autenticazione e l'integrità del messaggio ma non offre la confidenzialità
 - Internet key exchange (IKE): implementa lo “*scambio delle chiavi*” per realizzare il flusso crittografato
 - AH autentica l'intero pacchetto, mentre IP, mentre ESP solo i dati

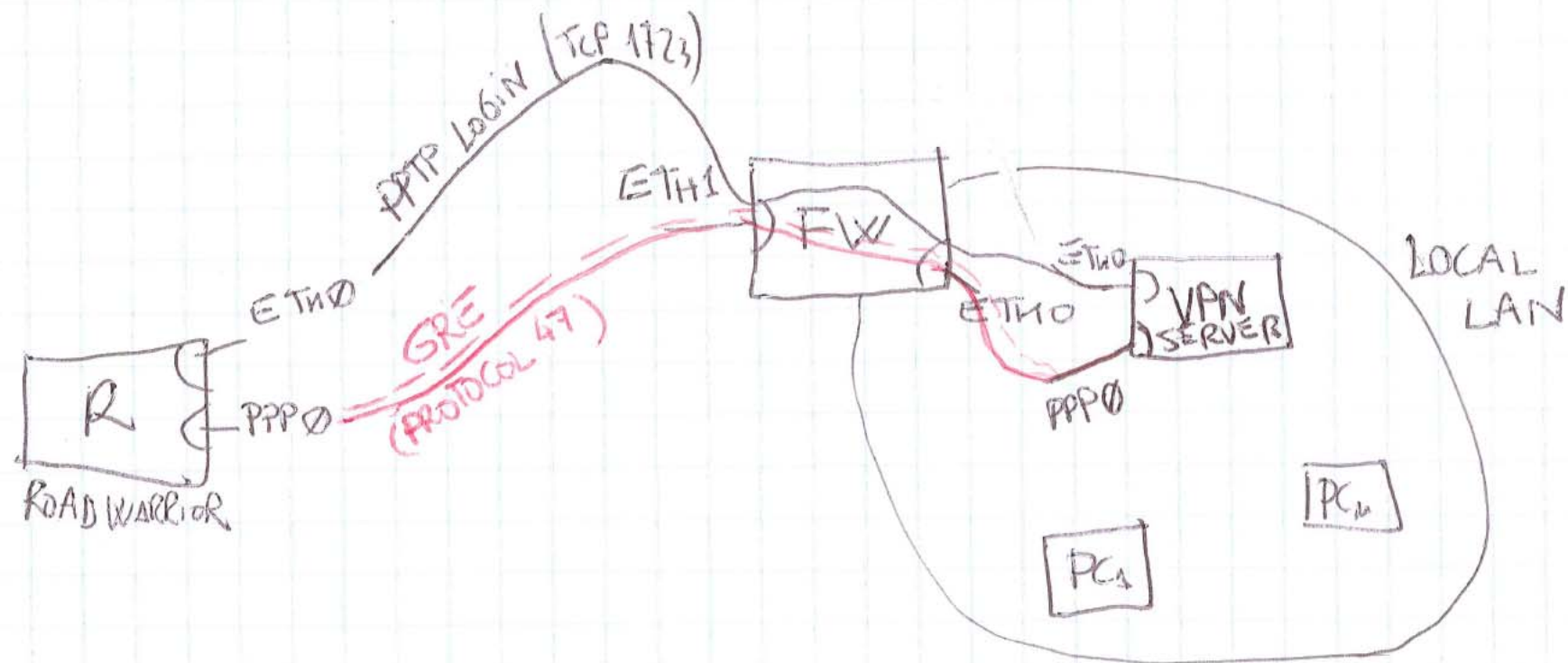


VPN con SSH Tunnel



```
iptables -A FORWARD -i eth1 -p tcp -dport 22 -j ACCEPT
iptables -A FORWARD -i eth0 -p tcp -sport 22 \
-m state -state ESTABLISHED, RELATED -j ACCEPT
```

VPN PPTP+GRE

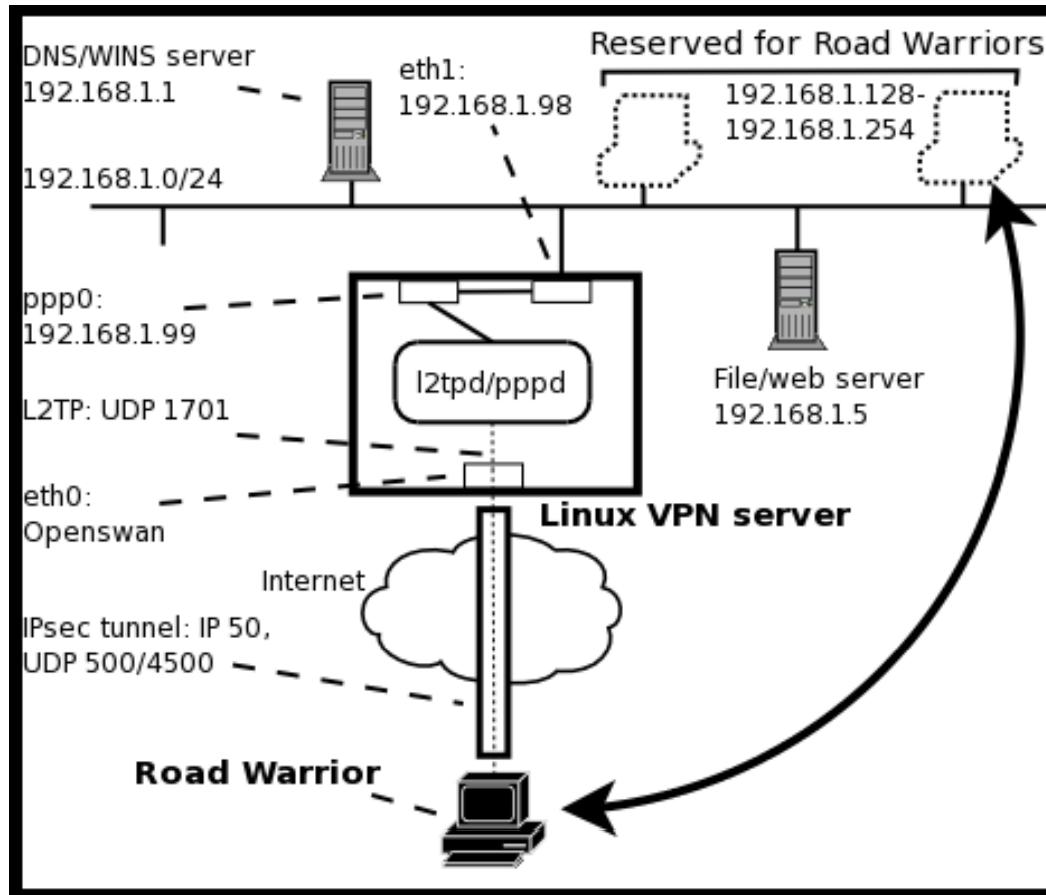


```
iptables -A FORWARD -p 47 -j ACCEPT
```

```
iptables -A FORWARD -i eth1 -p tcp --dport 1723 \
-m state -state ESTABLISHED, RELATED -j ACCEPT
```

```
iptables -A FORWARD -i eth0 -p tcp --sport 1723 \
-m state -state ESTABLISHED, RELATED -j ACCEPT
```

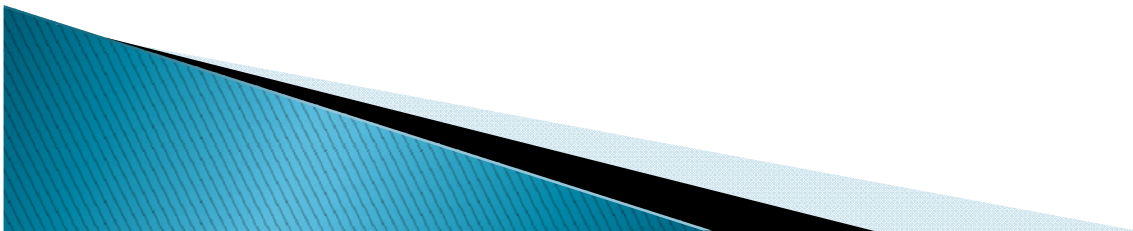
Tunneling con IPsec



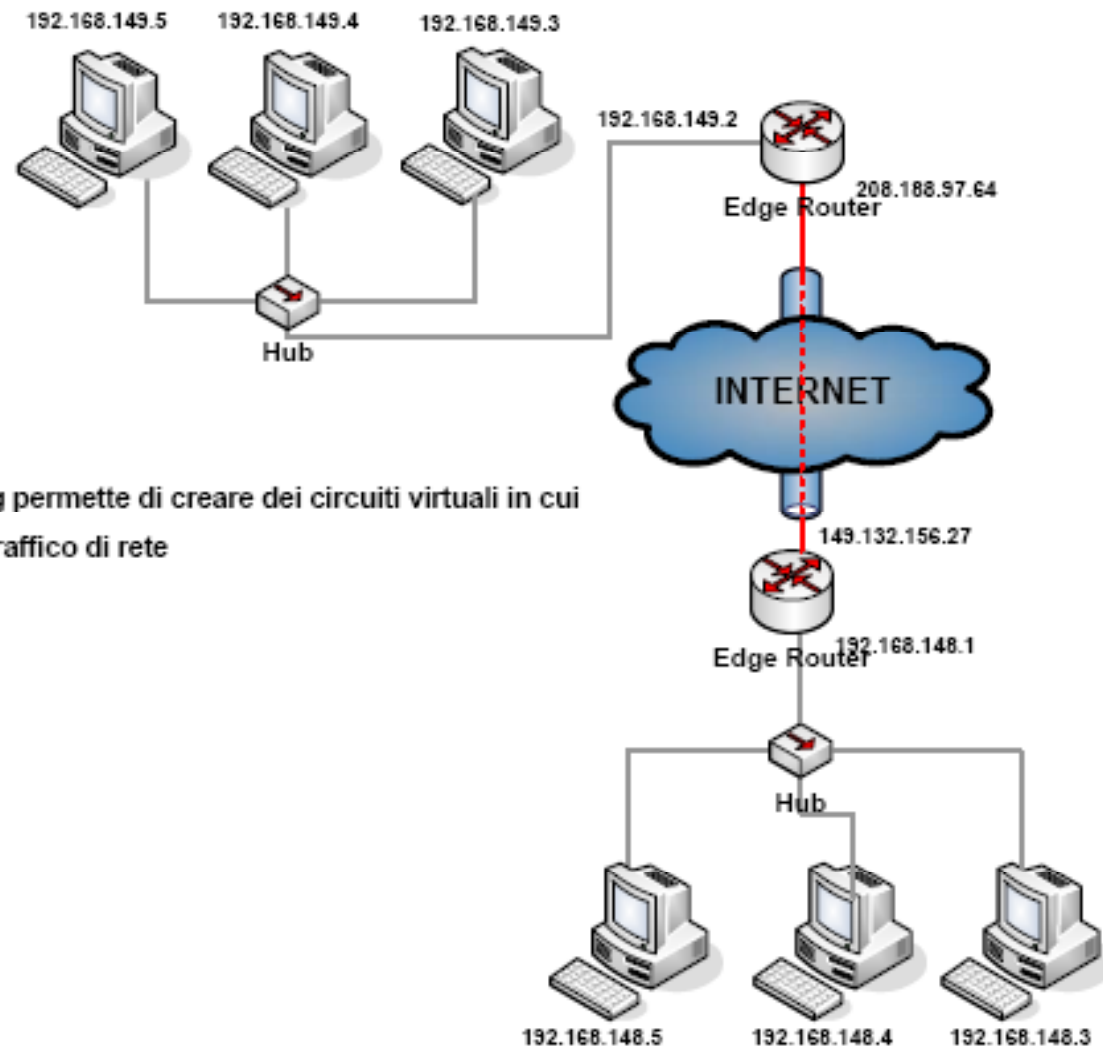
```
iptables -A FORWARD -p esp -j ACCEPT
iptables -A FORWARD -i eth1 -p udp --dport 500 \
    -m state -state ESTABLISHED, RELATED -j ACCEPT
iptables -A FORWARD -i eth0 -p udp --sport 500 \
    -m state -state ESTABLISHED, RELATED -j ACCEPT
```


Tunnelling: altre tecnologie

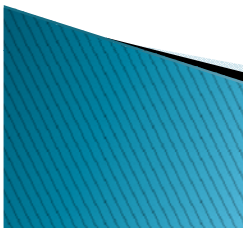
- ▶ insieme di protocolli di rete per cui un protocollo viene incapsulato in un altro o dello stesso livello o di livello superiore.




Tunnelling: altre tecnologie



Il tunneling permette di creare dei circuiti virtuali in cui viaggia il traffico di rete



Tunnelling: altre tecnologie

- ▶ Protocolli usati per il Tunneling:
 - L2TP (Layer 2 Tunneling Protocol)
 - MPLS (Multi-Protocol Label Switching)
 - GRE (Generic Routing Encapsulation)
 - PPTP(Point-to-Point Tunneling Protocol)
 - Ipsec
 - IEEE 802.1 Q (Ethernet VLANs)
- 

Tunnelling: altre tecnologie

Point to Point Tunneling Protocol (PPTP)	<p>Sviluppato da Microsoft, è un'estensione del Point to Point Protocol (PPP) che incapsula IP, IPX, NetBEUI all'interno dei pacchetti IP.</p> <p>Prevede un meccanismo (proprietario e opzionale) di cifratura</p>
Layer 2 Forwarding (L2F)	<p>Sviluppato da Cisco viene utilizzato per il "tunnelling" di protocolli di tipo link (HDLC, asynchronous HDLC, SLIP).</p> <p>Non prevede la cifratura dei dati</p>
Layer 2 Tunneling Protocol (L2TP)	<p>Frutto di un accordo fra Microsoft e Cisco, permette il "tunneling" del traffico PPP su diversi network. Serve a fornire un multi-protocol dial-up service per i provider ISP ed i POP.</p> <p>Come L2F, anche L2TP non prevede cifratura</p>
Socksv5	Alternativa di Nec a L2TP

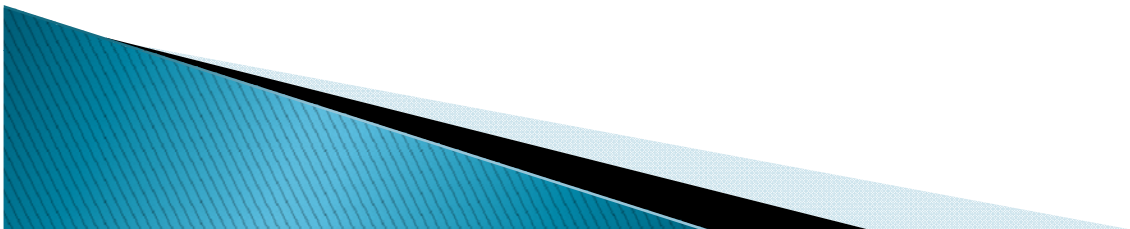
Security Protocols (Secure VPN)

- Transport Layer Security (SSL/TLS)
 - Usato per il tunneling del traffico dell'intera rete (SSL/TLS VPN) o per rendere sicura una connessione individuale
 - SSL (alla base per offrire accesso remoto ai servizi VPN).
 - Vantaggio di SSL VPN è che può essere acceduta anche da postazioni
 - che limitano l'accesso a siti web SSL-based senza il supporto di IPsec.
 - VPNs SSL-based possono risultare vulnerabili a *denial-of-service* rivolti alle connessioni TCP, essendo non autenticate
 - Garantisce confidenzialità e affidabilità delle comunicazioni su rete pubblica
 - Protegge da intrusioni, modifiche o falsificazioni



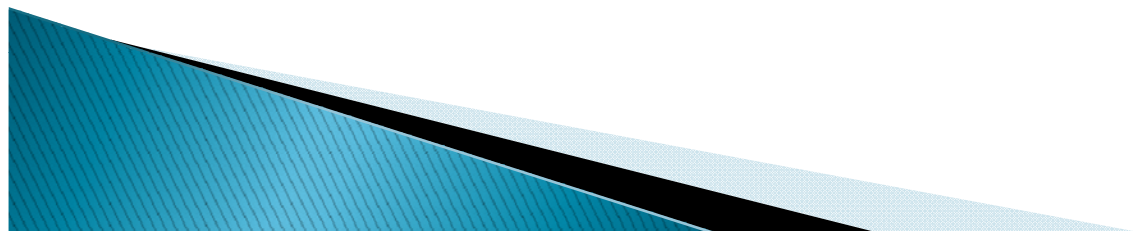
Security Protocols (Secure VPN)

- ▶ **Datagram Transport Layer Security (DTLS)**
 - Cisco AnyConnect VPN.
 - DTLS risolve il problema del tunneling su TCP, analogamente a SSL/TLS
- ▶ **Microsoft Point-to-Point Encryption (MPPE)**
 - usato con PPTP
 - PPTP (point-to-point tunneling protocol):
 - Cifratura dei dati
 - Sviluppato da Microsoft, assicura autenticazione, cifratura e compressione dei dati.
 - Generic Routing Encapsulation (GRE): GRE crea un collegamento point-to-point virtuale e questo è fatto in maniera che nessuno dei due punti si debba preoccupare dell'infrastruttura su cui passa la comunicazione



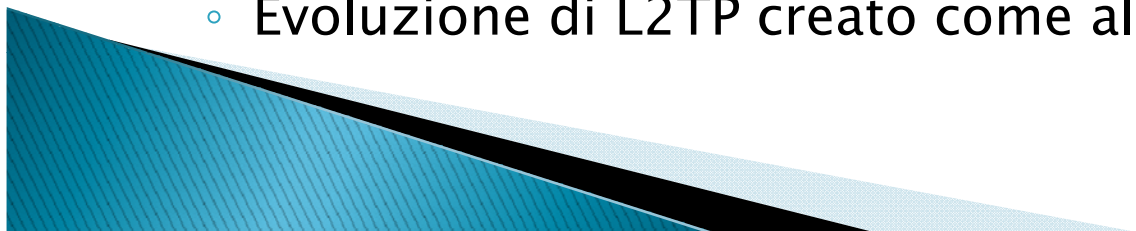
Security Protocols (Secure VPN)

- **Secure Socket Tunneling Protocol (SSTP) (Microsoft)**
 - Windows Server 2008, Windows Vista Service Pack 1.
 - SSTP tunnels PPP o traffico L2TP tramite un canale SSL 3.0
- **MPVPN (Multi Path Virtual Private Network).**
 - Sviluppato da Ragula Systems Development Company
- **SSH VPN -- OpenSSH**
 - offre tunneling VPN per rendere sicure connessioni remote a una rete



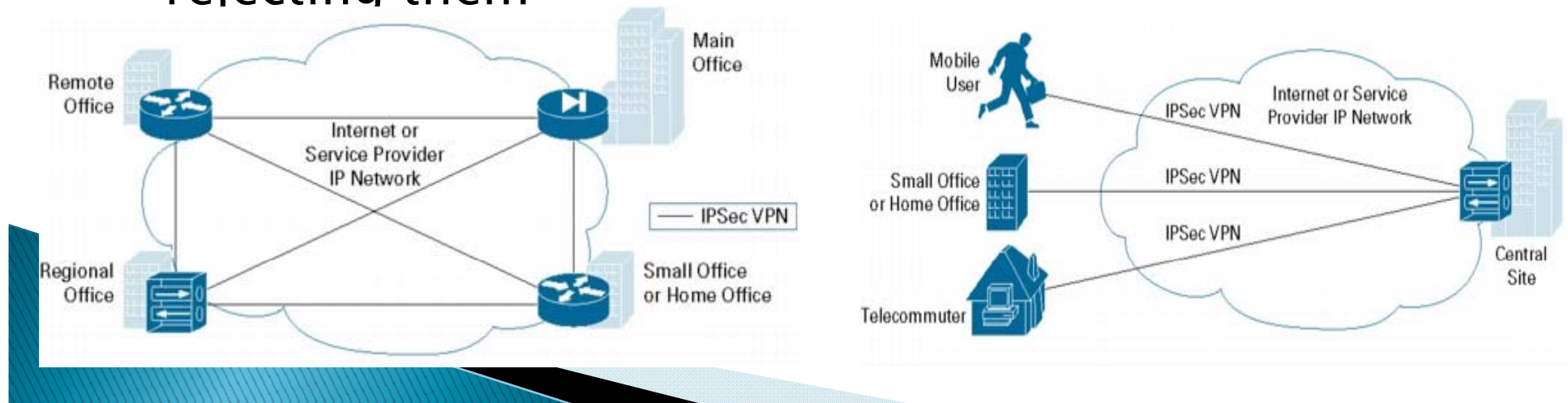
Security Protocols (Secure VPN)

- ▶ L2TP (Layer 2 Tunnelling Protocol)
 - Secure/Trusted VPN
 - Standard IETF
 - E' un protocollo a livello 5 (session) che agisce però come un protocollo di livello 2 (data link) usando pacchetti UDP per incapsulare i pacchetti L2TP e per mantenere una connessione Point-to-Point.
 - Deve essere associato ad un altro protocollo per implementare autenticazione, confidenzialità e integrità dei dati (solitamente IPSec).
- ▶ L2TPv3 (Layer 2 Tunnelling Protocol version 3)
 - Secure/Trusted VPN
 - Evoluzione di L2TP creato come alternativa a MPLS



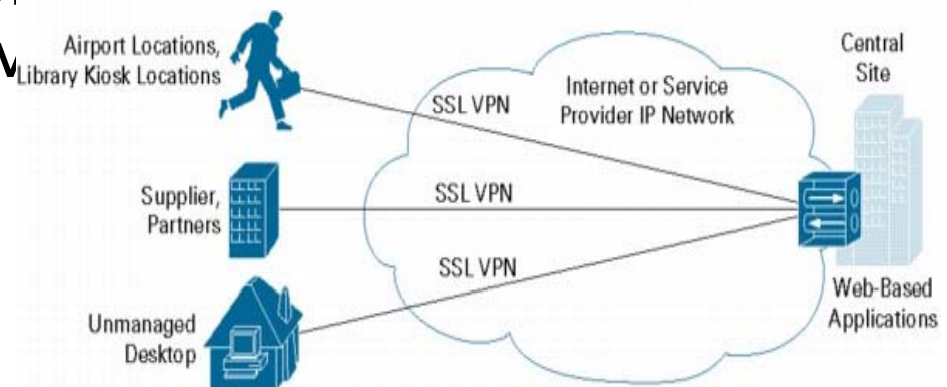
IPSec-based VPN

- ▶ Data confidentiality: Encrypts packets before transmission (ESP)
- ▶ Data integrity: Authenticates packets to help ensure that the data has not been altered during transmission
- ▶ Data origin authentication: Authenticates the source of received packets, in conjunction with data integrity service (Internet Key Exchange protocol)
- ▶ Antireplay: Detects aged or duplicate packets, rejecting them



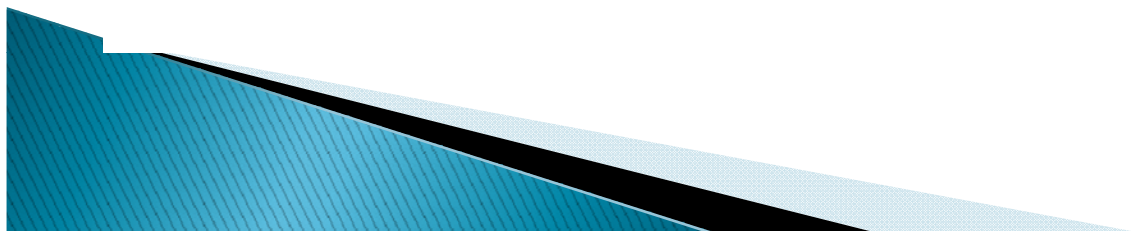
SSL-based VPN

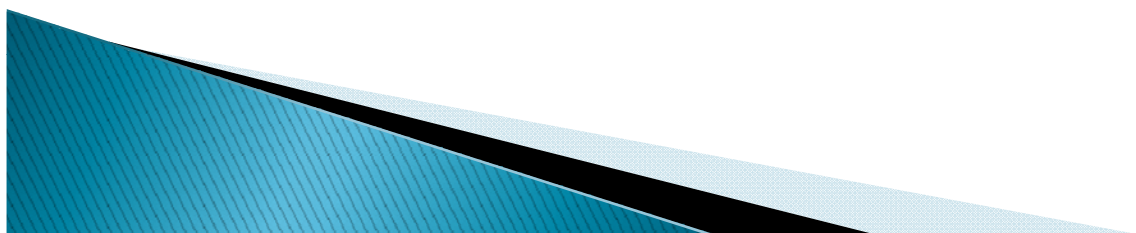
- ▶ Alternative to IPSec for remote-access VPNs
- ▶ SSL provides access special client software
- ▶ Secure connectivity by authenticating the communicating parties and encrypting the traffic
- ▶ SSL operates at the session layer and doesn't not support applications not coded for SSL
- ▶ SP can provide granular access control, limiting individual users' access to resources
- ▶ Include application proxies (SSL must be aware of each individual connection)
- ▶ SSL is computing-intensive (encryption processes)



Autenticazione

- Gli endpoints di un tunnel devono autenticarsi prima di poter stabilire un circuito VPN sicuro
 - *Tunnel End user created* possono usare passwords, biometrics, two-factor authentication, altri metodi di crittografia
 - *Network-to-network tunnels* fanno uso di passwords o certificati digitali, dato che devono essere memorizzati in modo permanente e non richiedono un intervento manuale per l'attivazione del tunnel





21/04/10