VPN World

MENOG 16
Istanbul-Turkey

By Ziad Zubidah

Network Security Specialist

What is this Van used for?!

Armed Van

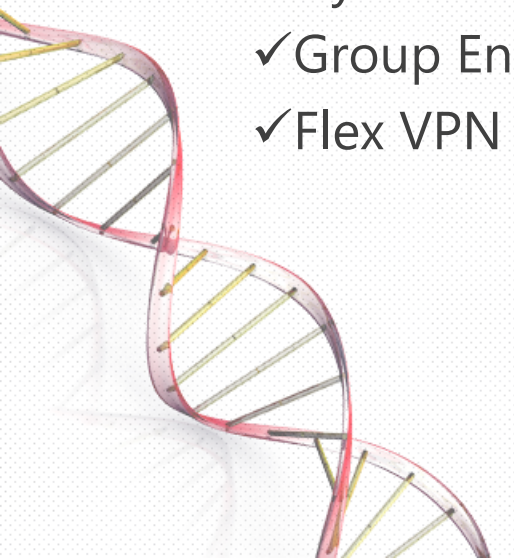
- It used in secure transporting for valuable goods from one place to another. It is bullet – resistant armed truck used to carry cache for banks

- These vehicles used the same infrastructure of public transportation, So, These vehicles are designed to resist attempts at robbery and hijacking. Bullet-resistant glass and reinforced shells and cabs are designed to resist bullets from most handguns and rifles. In addition, it driven by well trained armed security guard

Armed Van

AGENDA

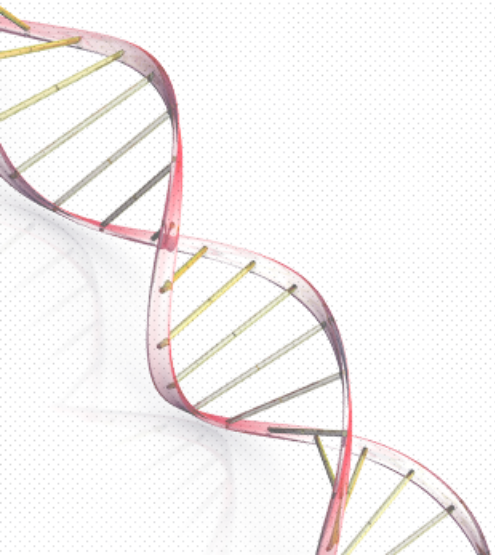
- **VPN Fundamentals**
  - ✓ What is VPN
  - ✓ VPN Protocols
  - ✓ IPsec
  - ✓ Tunnel Negotiation
  - ✓ VPN Topologies
- **Site-To-Site VPN**
  - ✓VTI Site-To-Site VPN
  - ✓Dynamic Multi-Point VPN
  - ✓Group Encrypted Transport VPN
  - ✓Flex VPN



AGENDA

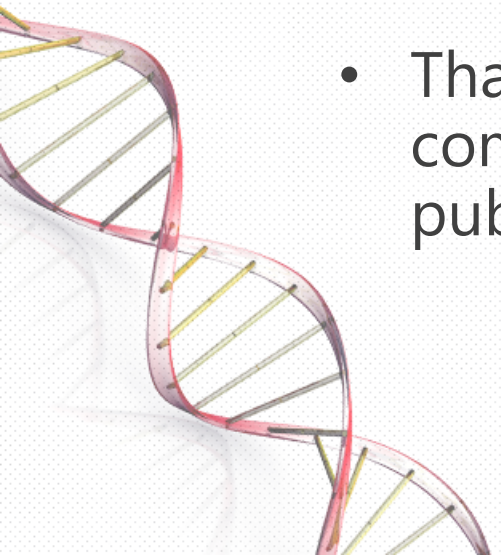
- **Remote Access VPN**
  - ✓TLS and SSL
  - ✓Full Tunnel Remote Access VPN
  - ✓Clientless Remote Access VPN
  - ✓IPsec Remote Access VPN

- **Public Key Infrastructure**
- **DEMO – Virtual LAB**



Virtual Private Network (VPN)

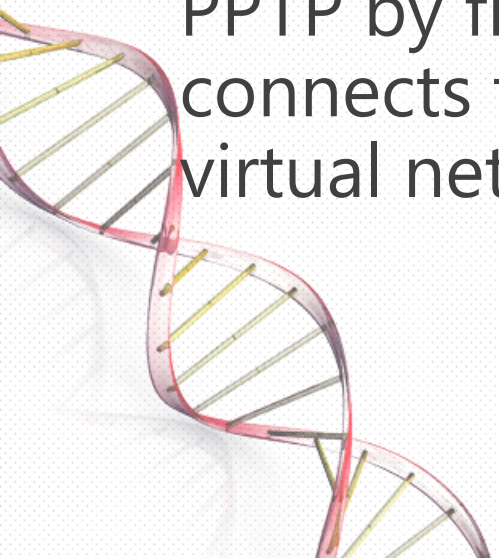
- A virtual private network (VPN) provides a secure communication between two points across a public network, such as the Internet.
- The traffic that flows between these two points passes through shared resources such as routers, switches, and other network equipment that make up the public WAN.
- That's why we should secure VPN communication while passing through the public network



VPN Protocols

- **PPTP (Point-to-Point Tunneling Protocol)**

Point-to-Point Tunneling Protocol (PPTP) is a Layer 2 tunneling protocol which allows a remote client to use a public IP network in order to communicate securely with a private network. Remote users can access a private network via PPTP by first dialing into their local ISP. PPTP connects to the target network by creating a virtual network for each remote client.



VPN Protocols

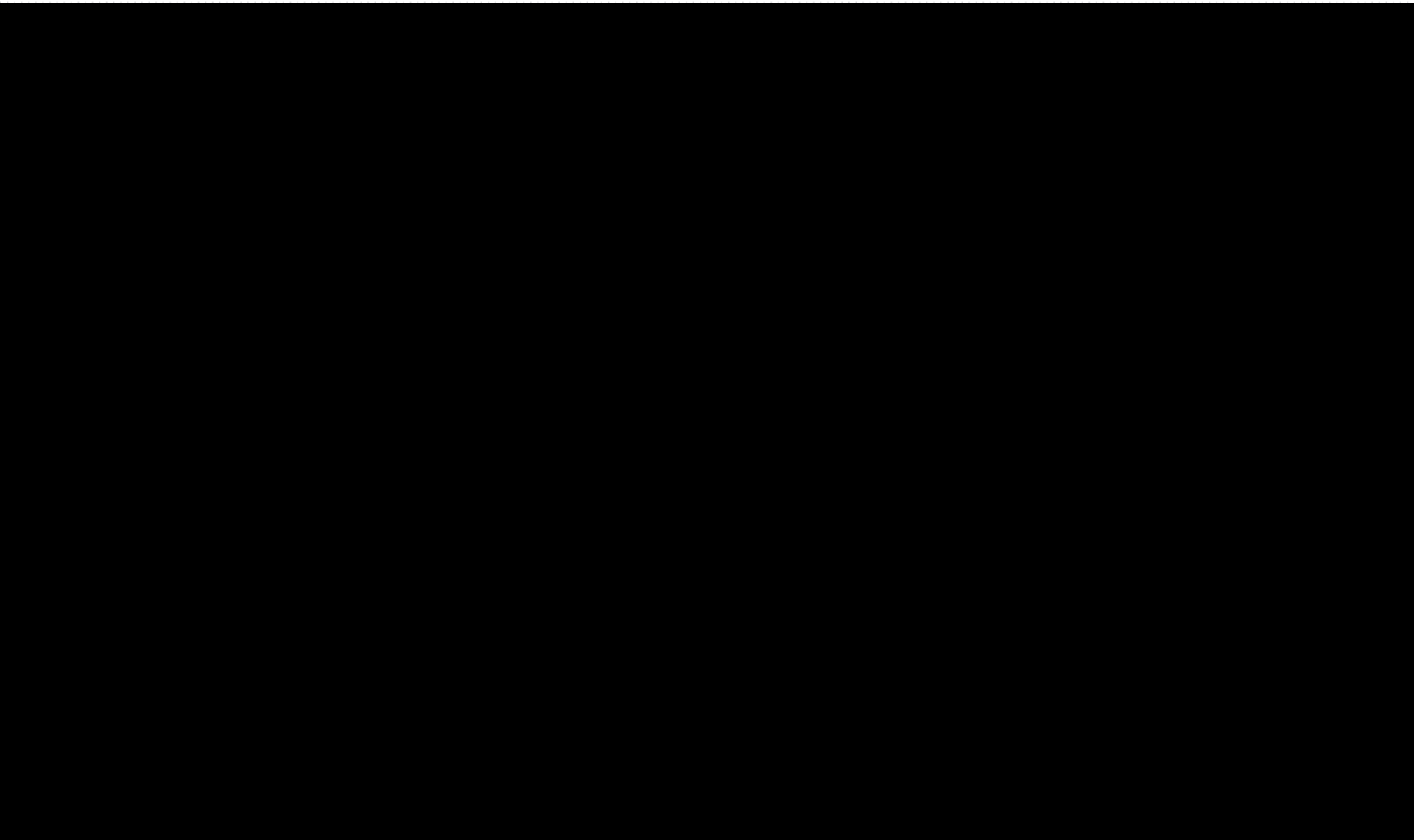
- **L2TP (LAYER 2 TUNNELING PROTOCOL)**

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support VPNs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy

Because of that, L2TP is often implemented along with IPsec.

VPN Protocols

- What is Generic Routing Encapsulation (GRE)?



Internet Protocol security (IPsec)

- Internet Protocol security (IPsec) is a security framework contain protocols for cryptographically securing communications over the IP Layer.

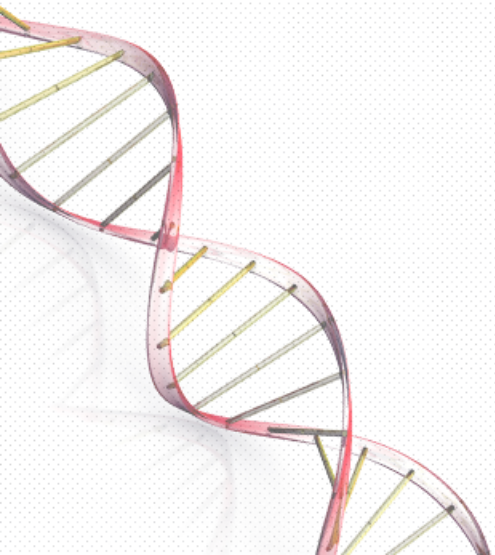
- It has two main protocols:
  - ✓ Authentication Header (AH)
  - ✓ Encapsulation Security Payload (ESP)

  - In addition to one protocol used for Key Management – Internet Key Exchange (IKE) Protocol

IPsec Protocols

1. Authentication Header (AH) : A security protocol for authenticating the source of an IP packet and verifying the integrity of its content.

1. Encapsulating Security Payload (ESP) : A security protocol for encrypting the IP packet, It can both encrypt and authenticate, encrypt only, or authenticate only.

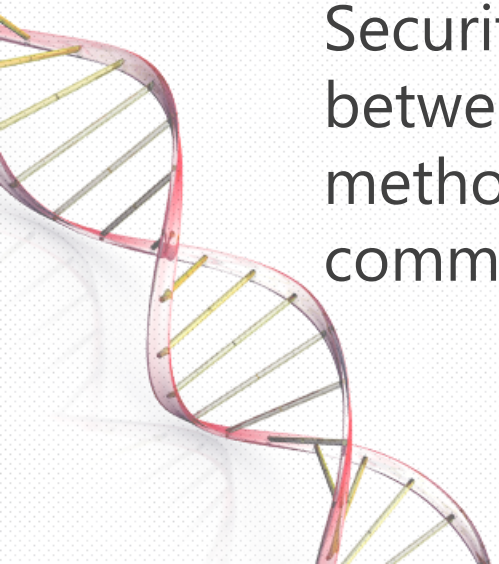


IPsec Key Management

IPsec supports the automated generation and negotiation of keys and security associations (SA) using the Internet Key Exchange (IKE) protocol.

Security Association (SA)

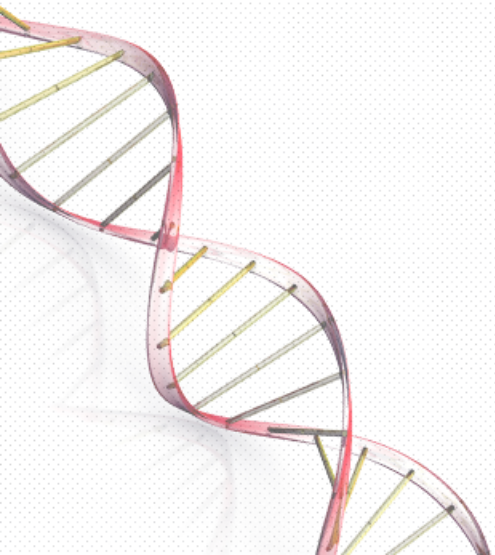
Security Association (SA) is an agreement between the VPN participants regarding the methods and parameters to use in securing a communication channel.



Tunnel Negotiation

To establish an Auto Key IKE IPsec tunnel, two phases of negotiations are required:

- Phase 1, the participants establish a secure channel in which to negotiate the IPsec SAs.
- In Phase 2, the participants negotiate the IPsec SAs for encrypting and authenticating user data.



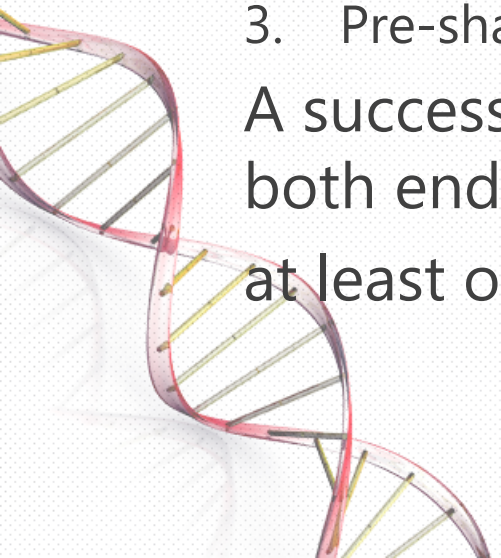
Tunnel Negotiation – Phase 1

- Phase 1 of tunnel negotiation consists of the exchange of proposals for how to authenticate and secure the channel.
- The participants exchange proposals for acceptable security services such as:

1. Encryption algorithms (DES and 3DES) and authentication algorithms (MD5,SHA-1 or SHA2).
2. A Diffie-Hellman group
3. Pre-shared key or certificates

A successful Phase 1 negotiation concludes when both ends of the tunnel agree to accept

at least one set of the security parameters .



Tunnel Negotiation – Phase 2

- After the participants a secure channel, they proceed to Phase 2, in which they negotiate the SAs to secure the data to be transmitted.

- The participants exchange security parameters included in the SA. A Phase 2 proposal also includes a security protocol; Encapsulating Security Payload (ESP) or Authentication Header (AH), and selected encryption and authentication algorithms. The proposal can also specify a DH group.

Tunnel Negotiation

- What is Diffie-Hellman key exchange algorithm?

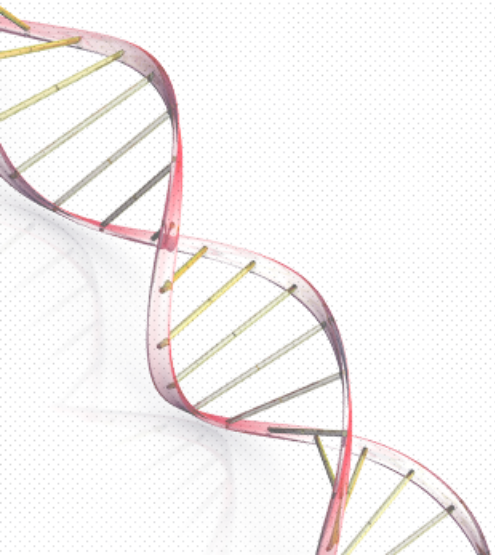
The Diffie-Hellman-Merkle
Key Exchange

VPN Topologies

- Point-to-Point VPN : two sites communicate directly with each other.
- Hub-and-Spoke VPN : Multiple remote sites (spokes) communicate securely with a central site (hub)
- Partial Mesh VPN: Some of the sites have connections with other sites
- Full Mesh VPN : In this topology type, every site communicates with every other device through a unique IPsec tunnel.

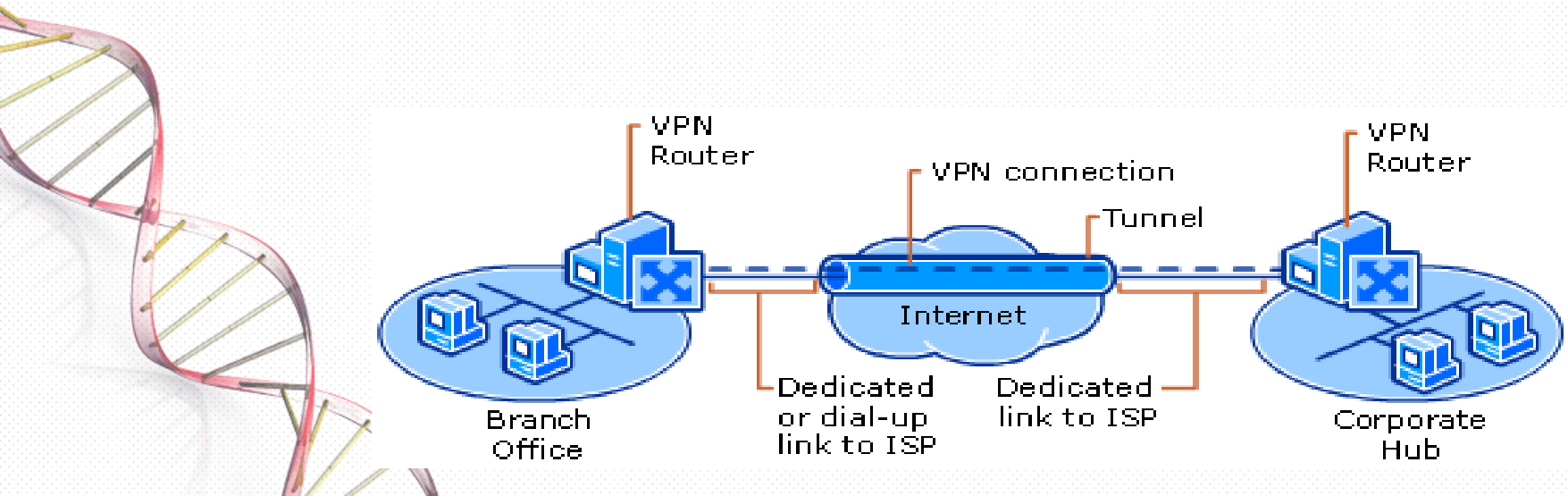
VPN Vendors

Discussion



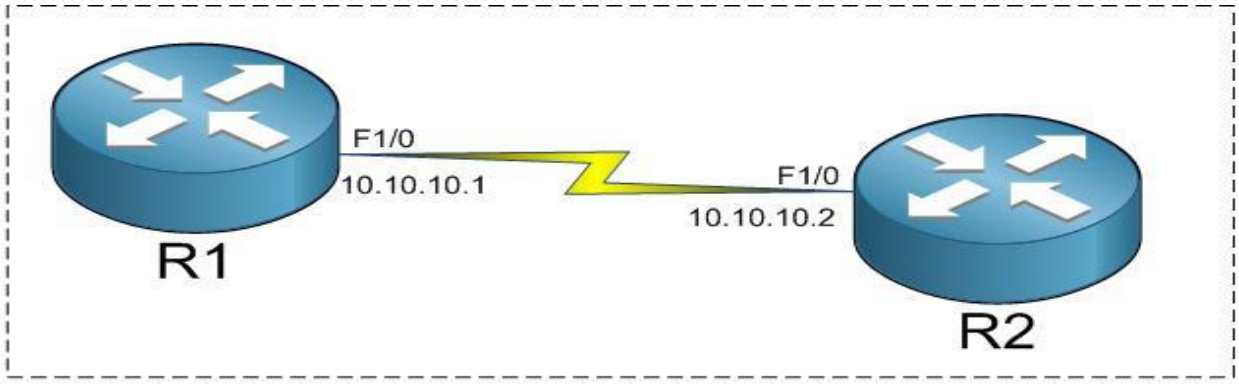
Site to Site VPN

- Site-to-site VPNs are a popular way to provide secure communication between sites
- Used instead of private WAN connections or to improve security of WAN connections
- There are a lot of configuration needed on both sites when creating VPN Site to Site such as (ISAKMP Policy, IPsec Policy, Crypto map, ACLs and interfaces)



Site to Site VPN

Configuration



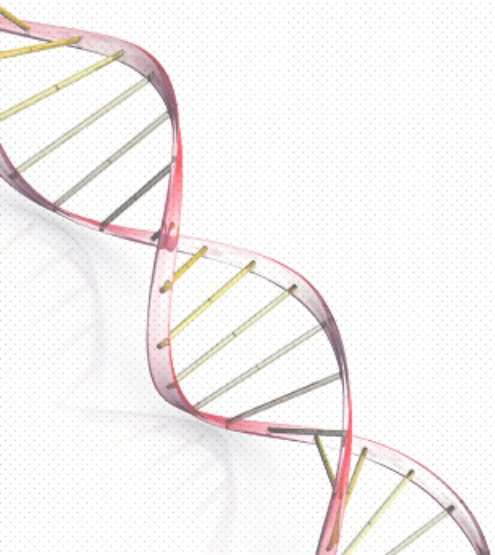
Site to Site VPN

```
crypto isakmp policy 1
authentication pre-share
hash md5
encryption des
group 1

crypto isakmp key 123 address 10.10.10.2

crypto ipsec transform-set MENOG esp-3des esp-sha

ip access-list extended 101
permit ip host 10.10.10.1 host 10.10.10.2

crypto map R1 10 ipsec-isakmp
set peer 10.10.10.2
match address 101
set transform-set MENOG

int F1/0
crypto map R1
```

```
crypto isakmp policy 1
authentication pre-share
hash md5
encryption des
group 1

crypto isakmp key 123 address 10.10.10.1

crypto ipsec transform-set MENOG esp-3des esp-sha

ip access-list extended 101
permit ip host 10.10.10.2 host 10.10.10.1

crypto map R1 10 ipsec-isakmp
set peer 10.10.10.1
match address 101
set transform-set MENOG

int F1/0
crypto map R1
```

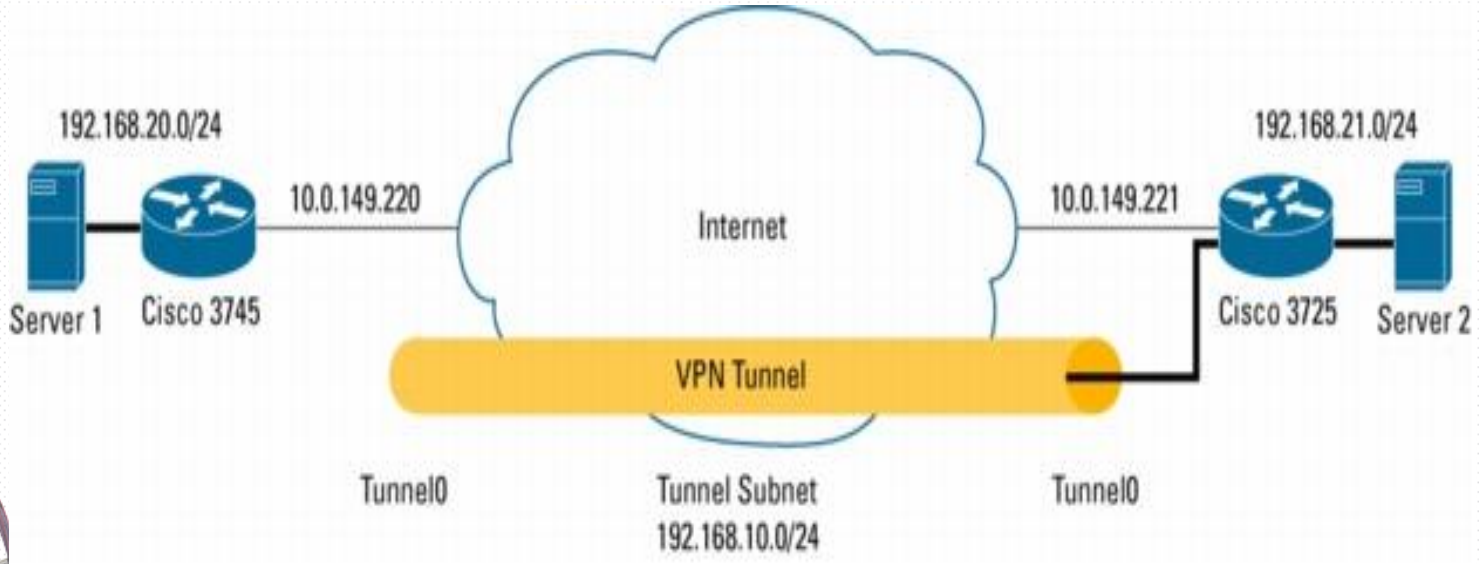
VTI Site to Site VPN

- IPsec VTIs make it much easier to provide protection between site-to-site VPN tunnel. Using a virtual tunnel interface .
- there is no longer a requirement to statically map an IPsec crypto map to a physical interface on the router/Firewall.



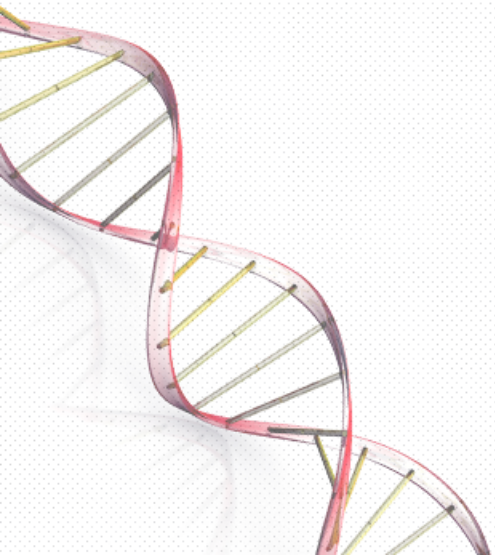
VTI Site to Site VPN

- IPsec VTIs have many benefits:
  - Simplify configuration Flexible interface
  - Support for multicast
  - Better scalability



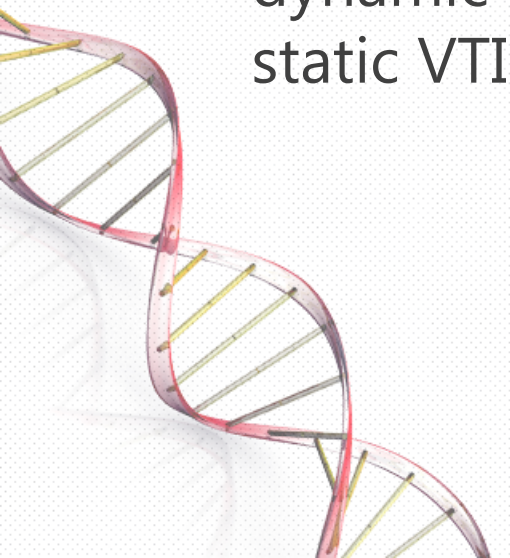
VTI Site to Site VPN Types

- Static Point-to-Point IPsec VTI Tunnels
- ➢ Static VTI VPN tunnels provide secure connectivity between two sites.
- ➢ Deploying static VTI tunnels involves configuring a tunnel interface on both VPN peers.
- ➢ Static VTI tunnels are permanently established immediately after being configured



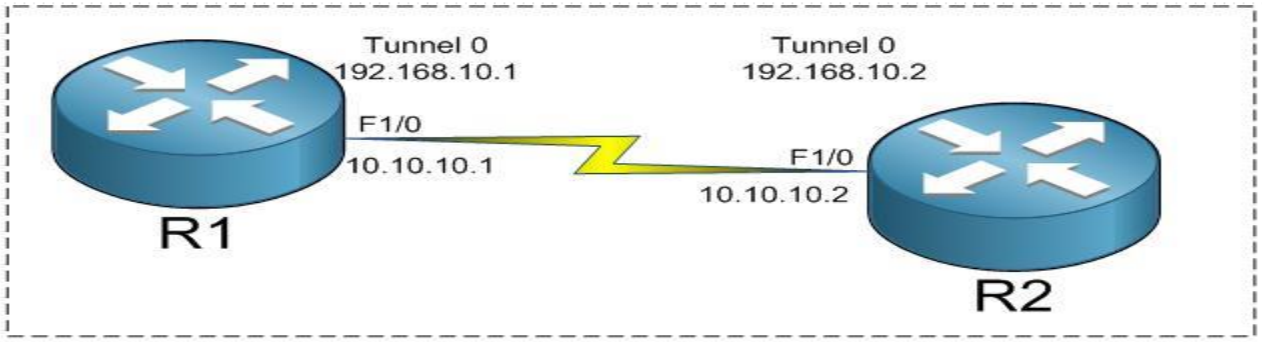
VTI Site to Site VPN Types

- Dynamic Point-to-Point VTI Tunnels
- ➢ It works with Hub-and-Spoke topology
- ➢ There is no requirement to statically map IPsec sessions to physical interfaces. Instead, VTIs on the hub are created dynamically as tunnels to the hub are established.
- ➢ When a spoke peer initiates a tunnel, the tunnel and dynamic VTI are created. On the spoke peer, use a static VTI to establish a tunnel with the hub peer.



Static VTI Site to Site VPN

Configuration



VTI Site to Site VPN

```
crypto isakmp policy 1
authentication pre-share
hash md5
encryption des
group 1

crypto isakmp key 123 address 10.10.10.2

crypto ipsec transform-set MENOG-TS esp-3des esp-sha

Crypto ipsec profile MENOG-PRO
set Transform-set MENOG-TS

interface tunnel0
ip address 192.168.10.1 255.255.255.0
tunnel source f0/0
tunnel destination 10.10.10.2
tunnel mode ipsec ipv4
tunnel protection ipsec profile MENOG-PRO

interface f0/0
ip address 10.10.10.1 255.255.255.0
no shut
```

```
crypto isakmp policy 1
authentication pre-share
hash md5
encryption des
group 1

crypto isakmp key 123 address 10.10.10.2

crypto ipsec transform-set MENOG-TS esp-3des esp-sha

Crypto ipsec profile MENOG-PRO
set Transform-set MENOG-TS

interface tunnel0
ip address 192.168.10.1 255.255.255.0
tunnel source f0/0
tunnel destination 10.10.10.2
tunnel mode ipsec ipv4
tunnel protection ipsec profile MENOG-PRO

interface f0/0
ip address 10.10.10.1 255.255.255.0
no shut
```

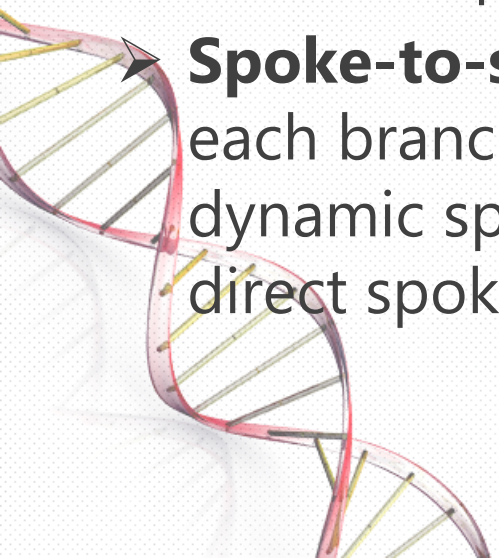
Dynamic Multipoint VPN - DMVPN

The DMVPN is the most scalable IPsec VPNs. It supports dynamically addressed spoke routers. You can add new spoke nodes without having extra configuration on the hub.

- DMVPNs have two models:

➢ **Hub-and-spoke:** A hub-and-spoke DMVPN requires that each branch (spoke) have a point-to-point GRE interface that is used to build a tunnel to the hub router. All traffic between spokes must flow through the hub router.

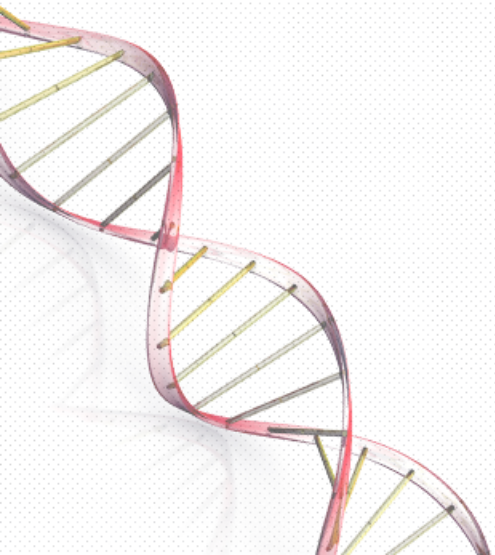
➢ **Spoke-to-spoke:** A spoke-to-spoke DMVPN requires that each branch (spoke) have an mGRE interface to create dynamic spoke-to-spoke tunnels . This model provides direct spoke-to- spoke communication.



DMVPN

- DMVPNs components are:

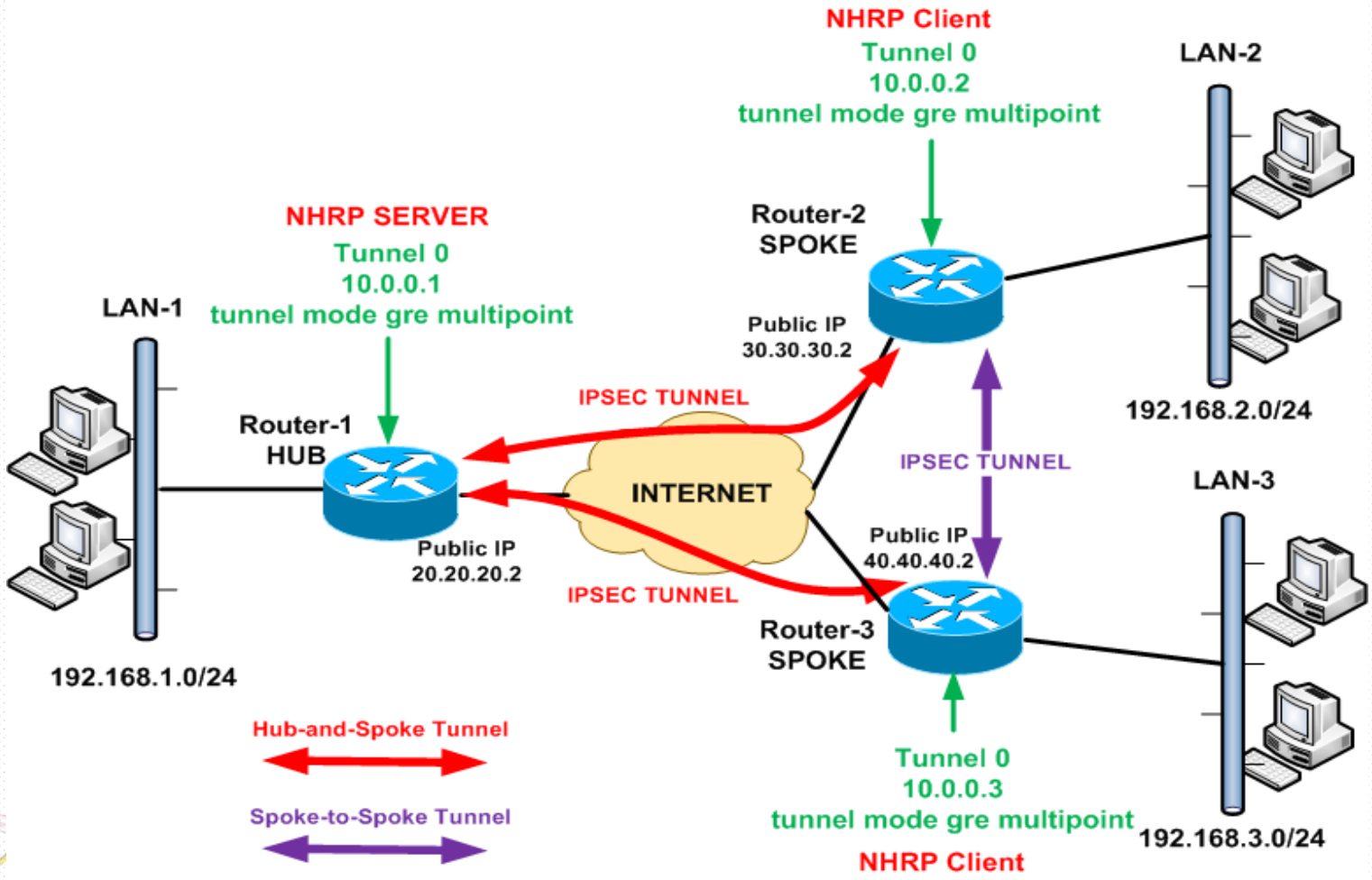
- **mGRE:** mGRE allows a single Generic Routing Encapsulation (GRE) interface to support multiple GRE tunnels and makes the configuration much easier. Using GRE tunnels provides support for IP multicast. Which enables the use of dynamic routing protocols such as EIGRP or OSPF to update routing tables and create redundant VPN paths if needed.



DMVPN

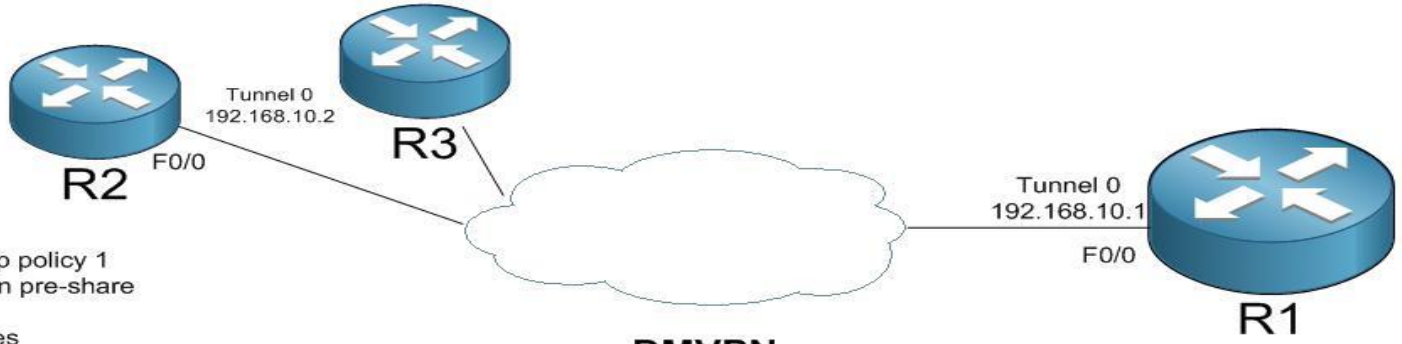
- **NHRP:** Next Hop Resolution Protocol (NHRP) is a client and server protocol where the hub acts as the NHRP server and the spokes are the NHRP clients. The NHRP database maintains mappings between the router (physical interface) and the tunnel (tunnel interface) IP addresses of each spoke. Each spoke registers its physical and internal tunnel addresses to the NHRP database.
- **IPsec:** IPsec provides transmission protection for GRE tunnels.

DMVPN


NHRP Client
Tunnel 0
10.0.0.2
tunnel mode gre multipoint
LAN-2
NHRP SERVER
Tunnel 0
10.0.0.1
tunnel mode gre multipoint
Router-2
SPOKE
LAN-1
Public IP
30.30.30.2
IPSEC TUNNEL
Router-1
HUB
INTERNET
IPSEC TUNNEL
192.168.2.0/24
LAN-3
Public IP
20.20.20.2
Public IP
40.40.40.2
IPSEC TUNNEL
Router-3
SPOKE
192.168.1.0/24
Hub-and-Spoke Tunnel
Tunnel 0
10.0.0.3
tunnel mode gre multipoint
Spoke-to-Spoke Tunnel
NHRP Client
192.168.3.0/24

DMVPN

Configuration




```
crypto isakmp policy 1
authentication pre-share
hash md5
encryption des
group 1

crypto isakmp key 6 123 address 10.10.10.1

crypto ipsec transform-set MENOG-TS esp-3des esp-sha

crypto ipsec profile MENOG-PRO
set Transform-set MENOG-TS

interface tunnel0
ip address 192.168.10.2 255.255.255.0
ip nhrp authentication 123
ip nhrp map multicast dynamic
ip nhrp map 192.168.10.1 10.10.10.1
ip nhrp map multicast 10.10.10.1
ip nhrp network-id 1
ip nhrp nhs 192.168.10.1
tunnel source f0/0
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile MENOG-PRO

interface f0/0
ip address 10.10.10.2 255.255.255.0
no shut
```

```
crypto isakmp policy 1
authentication pre-share
hash md5
encryption des
group 1

crypto isakmp key 6 123 address 0.0.0.0 0.0.0.0

crypto ipsec transform-set MENOG-TS esp-3des esp-sha


Crypto ipsec profile MENOG-PRO
set Transform-set MENOG-TS

interface tunnel0
ip address 192.168.10.1 255.255.255.0

ip nhrp authentication 123
ip nhrp map multicast dynamic
ip nhrp network-id 1
tunnel source 10.10.10.1
tunnel mode gre multipoint
tunnel protection ipsec profile MENOG-PRO


interface f0/0
ip address 10.10.10.1 255.255.255.0
no shut
```

GET VPN

- GET VPNs provide large-scale, connectionless, tunnel-free transmission protection that takes advantage of an existing routing infrastructure . So, it can be used with MPLS, IP, Frame Relay, and ATM networks.
- GET VPNs remove the need to establish point-to-point tunnels, Therefore it can be used to transmit voice and video with high quality, and managed the quality of service (QoS), routing, and multicast. GET VPNs uses the concept of “trusted” group members.
- It is only work with Cisco devices

GET VPN

The two components in GET VPN architecture:

1. **Key Server**

Authenticates all group members, performs admission control to the GET VPN domain, And creates and supplies group authentication key as security associations (SA) to group Members.

2. **Group Members**

Group members provide transmission protection to sensitive site-to-site (member-to-member) traffic.

Key servers distribute keys and policies to all registered and authenticated group member routers .

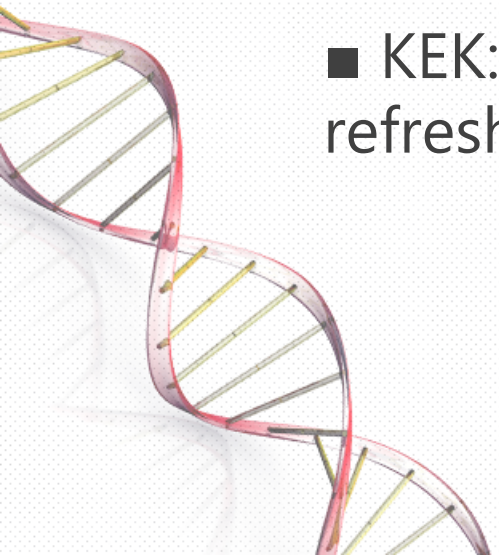
GET VPN

All communication between a key server and group members is encrypted and secured using the Internet Key Exchange (IKE) Group Domain of Interpretation (GDOI) protocol.

IKE GDOI supports the use of two keys: Traffic Encrypting Key (TEK) and Key Encrypting

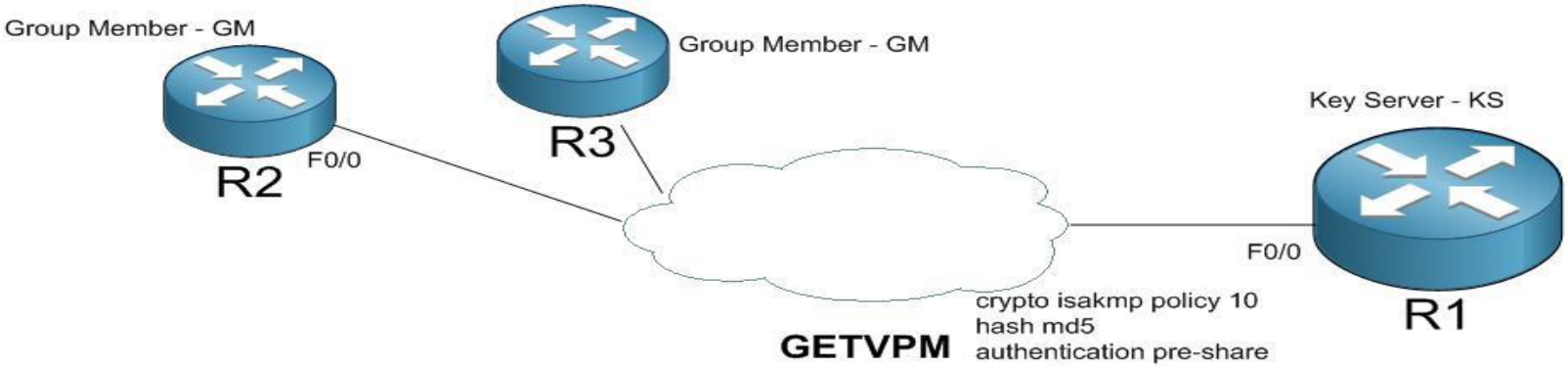
Key (KEK):

- TEK: A key that is used to protect traffic between group members
- KEK: A key this is used to protect rekeys (during a key refresh) between key servers and group members



GET VPN

Configuration

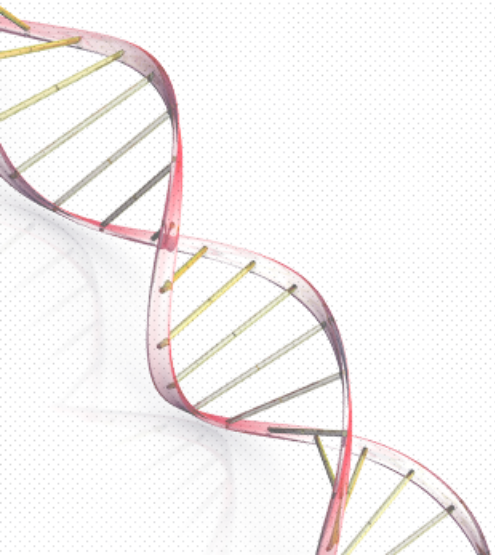



```
crypto isakmp policy 10
hash md5
authentication pre-share
group 1
encryption des

crypto isakmp key 6 123 address 10.10.10.1

crypto gdoi group GDOI-GRP
identity number 555
server address ipv4 10.10.10.1

crypto map GETVPN-MAP 100 gdoi
set group GDOI-GRP

interface FastEthernet0/0
ip address 10.10.10.2 255.255.255.0
crypto map GETVPN-MAP
```

```
crypto isakmp policy 10
hash md5
authentication pre-share
group 1
encryption des

crypto isakmp key 6 123 address 0.0.0.0
crypto key generate rsa label VPNKEY mod 1024 exportable
crypto ipsec transform-set MENOG-TS esp-3des esp-sha-hmac

crypto ipsec profile MENOG-PRO
set transform-set MENOG-TS

crypto gdoi group GDOI-GRP
identity number 555
server local
rekey algorithm aes 256
rekey lifetime seconds 900
rekey retransmit 40 number 3
rekey authentication mypubkey rsa VPNKEY
rekey transport unicast
sa ipsec 10
match address ipv4 GET-ACL
replay counter window-size 64
address ipv4 10.10.10.1

interface FastEthernet0/0
ip address 10.10.10.1 255.255.255.0

ip access-list extended GET-ACL
permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
```

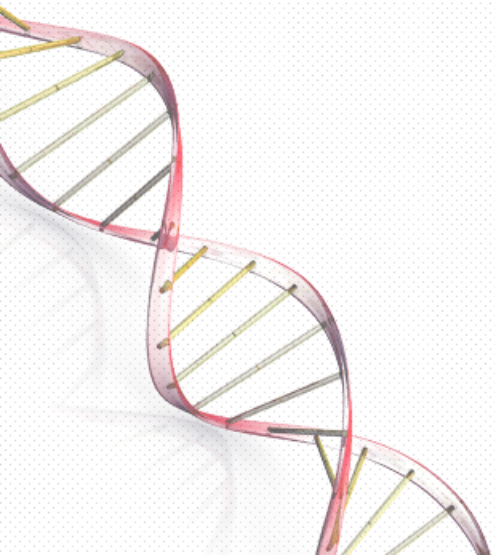
Flex VPN

FlexVPN is Cisco's implementation of the IKEv2 standard that combines site to site, remote access, hub and spoke topologies and partial meshes (spoke to spoke direct). FlexVPN offers a simple but modular framework that extensively uses the tunnel interface model while remaining compatible with legacy VPN implementations using crypto maps.



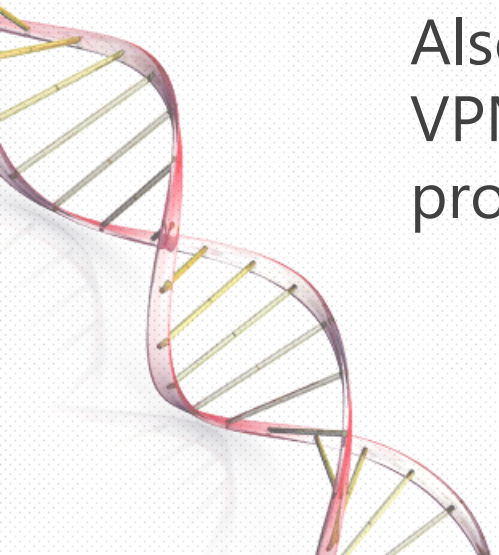
Remote Access VPN

Remote access VPNs connect remote users to a set of resources on internal network. Remote access VPNs typically need very strong client authentication, which requires users to prove their identity and encryption to protect transmissions across an untrusted network, typically the Internet.



SSL and TLS

- Transport Layer Security (TLS) and Secure Socket Layer (SSL), are cryptographic protocols that provide security for transmissions of public transports such as the Internet.
- The SSL protocol was developed by Netscape in 1994 to protect web transactions.
- Most web browsers have implemented SSL. Also, Many other applications, such as SSL VPN clients, also use SSL/TLS for transmission protection.



SSL and TLS

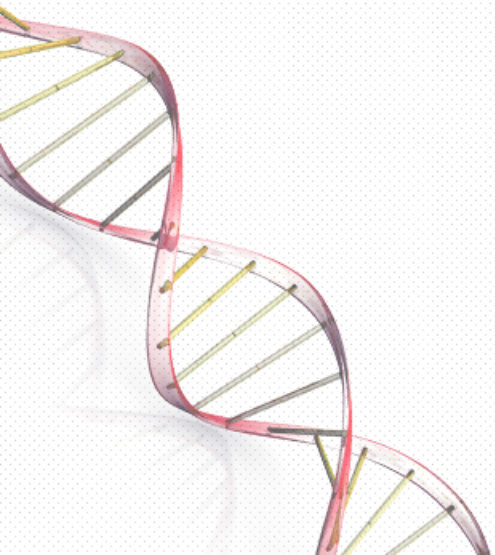
- SSL/TLS provides endpoint authentication for the client and the server, data encryption to ensure confidentiality, and data integrity and authentication . Both the SSL and TLS protocols work in two phases:

➢ **Session establishment phase:** When the negotiation of parameters and peer authentication takes place.

➢ **Data transfer phase:** User data is exchanged securely between encapsulating endpoints.

Full Tunneling Remote Access SSL VPN

In the full tunneling VPN, remote users should install VPN client to establish a Secure Socket Layer/Transport Layer Security (SSL/TLS) tunnel with the VPN Gateway. After successful authentication, VPN Gateway will apply a set of authorization and accounting rules to the user's session.

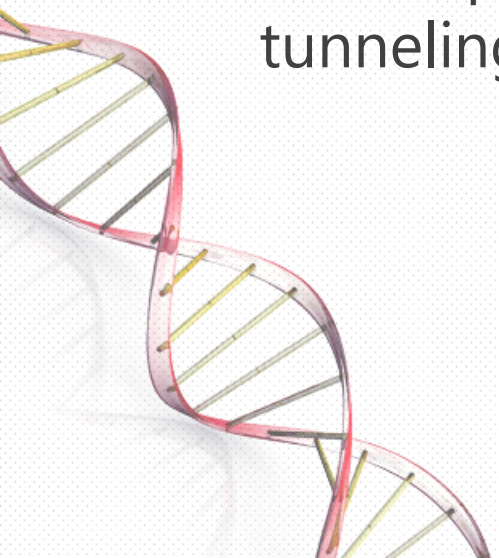


Clientless Remote Access SSL VPN

In the clientless remote access VPN architecture, remote users use their web browser to

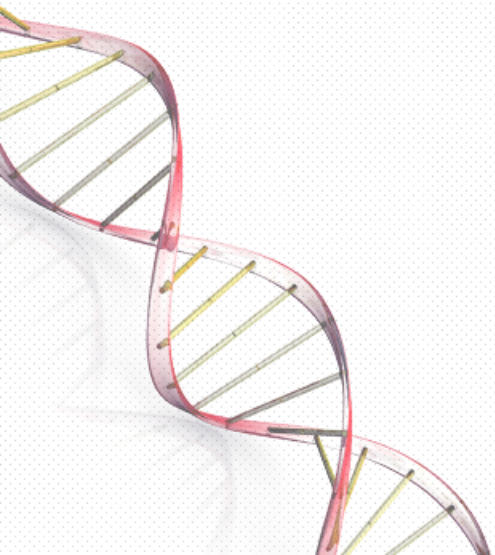
establish an SSL/TLS session with the VPN Gateway. After successful authentication,

VPN Gateway will apply a set of authorization and accounting rules to the user's session and the user is presented with a web portal. Clientless SSL VPNs do not provide full network access like the full tunneling VPNs.



Remote Access IPsec VPN

This architecture provides full tunneling client-based IPsec VPN . With this option, remote users use the VPN client to build an IPsec tunnel with VPN Gateway. Just as with the full tunneling remote access SSL VPN, after mutual authentication has taken place, VPN Gateway will apply a set of authorization and accounting rules to the user's session.



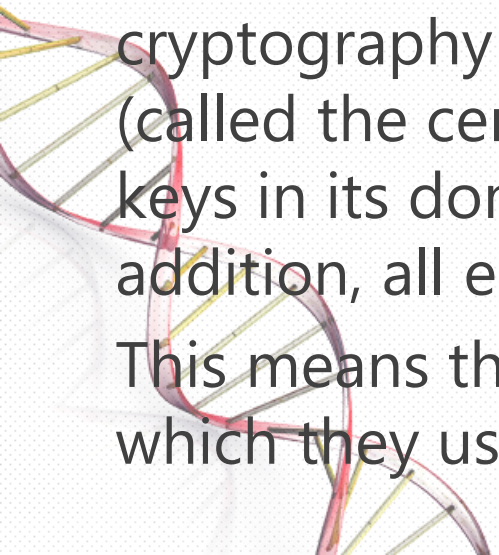
Public Key Infrastructure

IPsec VPNs can use public key infrastructure to provide a scalable solution for peer authentication.

Public key cryptography, which uses the (RSA) algorithm, uses pairs of keys called the public and private key for its encryption and digital signature processes. Both of these activities call for an exchange of public keys between the two sites that want to communicate.

The use of a trusted third-party protocol with public key cryptography is based on one central trusted introducer (called the certificate authority [CA]) that signs all the public keys in its domain (servers, users, routers, and so on). In addition, all entities in this domain trust the CA.

This means that all entities have the public key of the CA, which they use to verify messages from the CA.

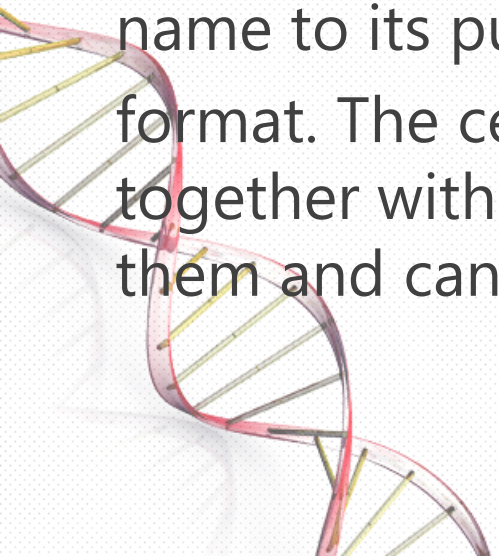


Public Key Infrastructure

To participate in the PKI system, all end users must enroll with the CA, which involves a process in which they submit their public key and their name to the CA. After a user submits his public key and name to the CA, the CA verifies the identity and public key of the enrolling user. The CA then digitally signs the submitted information with its private key.

This creates a *certificate* for the submitter. An identity certificate is a piece of information that binds a PKI member's name to its public key and puts it into a standard

format. The certificates are returned to the users bound together with the signature of the CA. The users then install them and can use them.



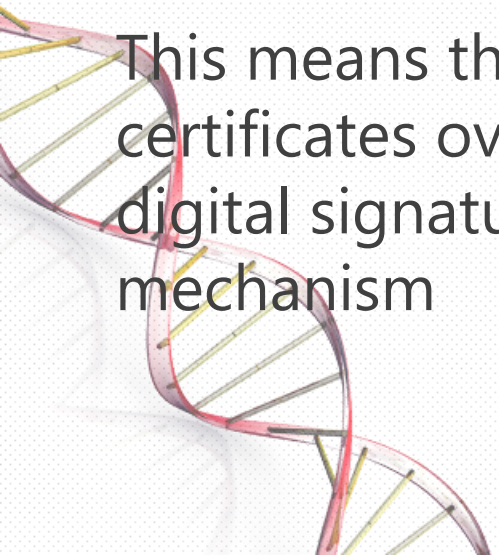
Public Key Infrastructure

Each entity has the public key of the certificate authority along with its own identity certificate, which has been signed by the certificate authority, the identity can

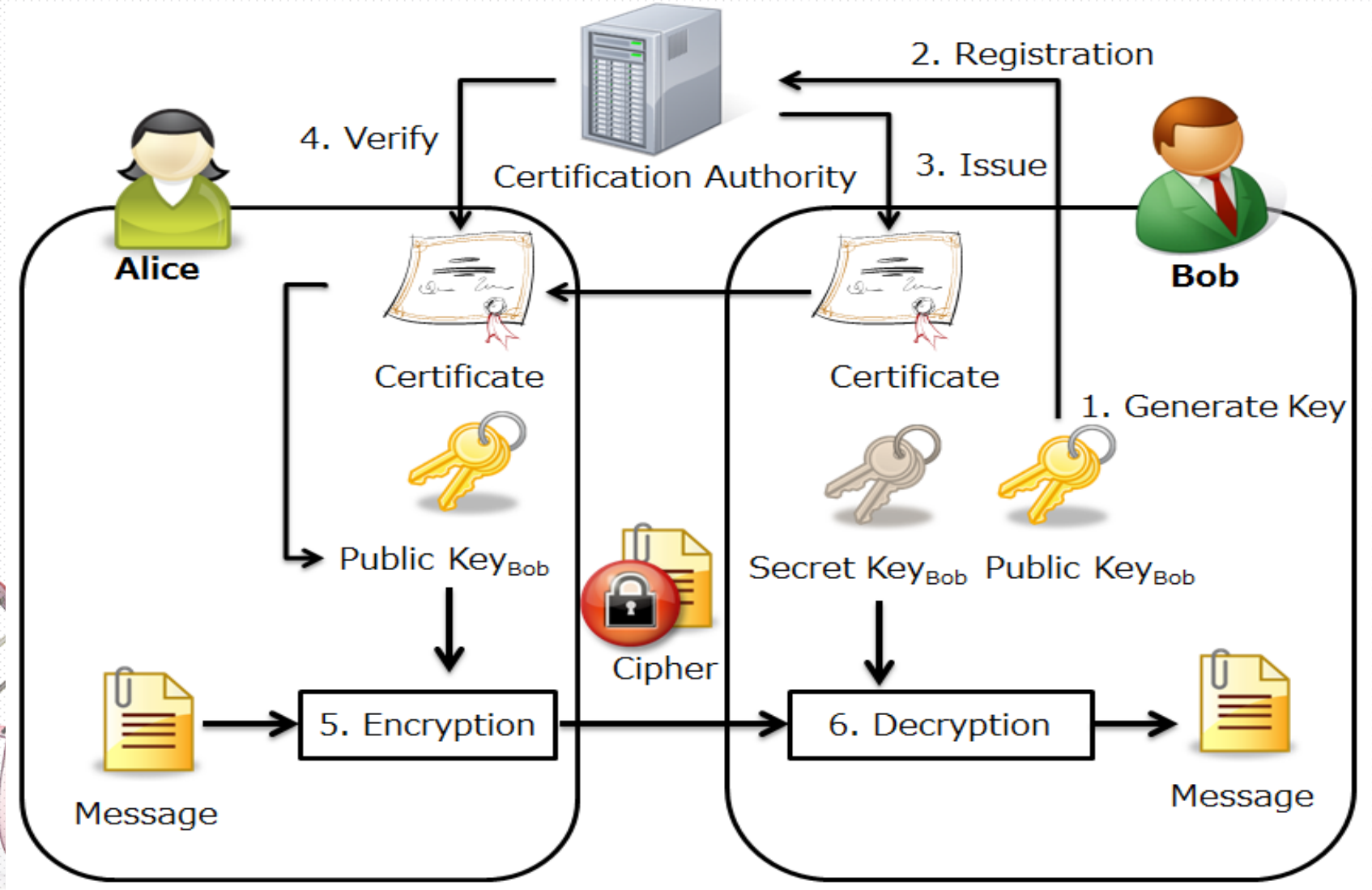
verify any data that is signed by the CA.

The entities can now act independently of the CA and establish point-to-point communications with each other by exchanging information about themselves by using this certificate.

This means that end users can now mutually exchange certificates over untrusted public networks and use the digital signature of the certificate authority as the trust mechanism

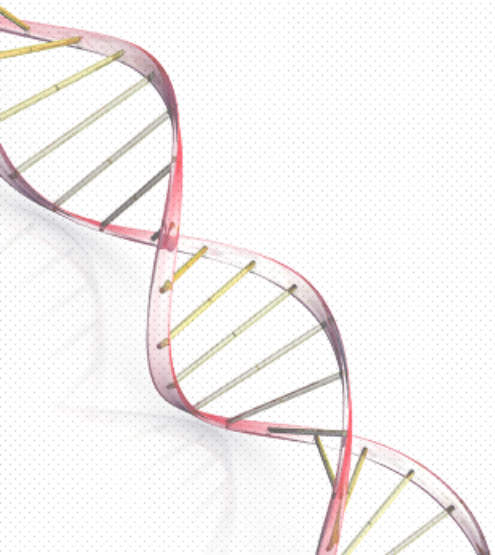


Public Key Infrastructure



Refrences

- CCNP Security SECURE by Sean Wilkins, Franklin H. Smith – ciscopress
- Concepts and Examples, ScreenOS Refrence Guide (Virtual Private Network) – Juniper Networks
- FortiOS Handbook, IPsec VPN for FortiOS 5.0 – FortiNet



Ziad Zubidah
National Info. Tech. Center – Jordan
+962799074805
Ziad.zubidah@gmail.com
SKYPE:zubidah.ziad

Thank You