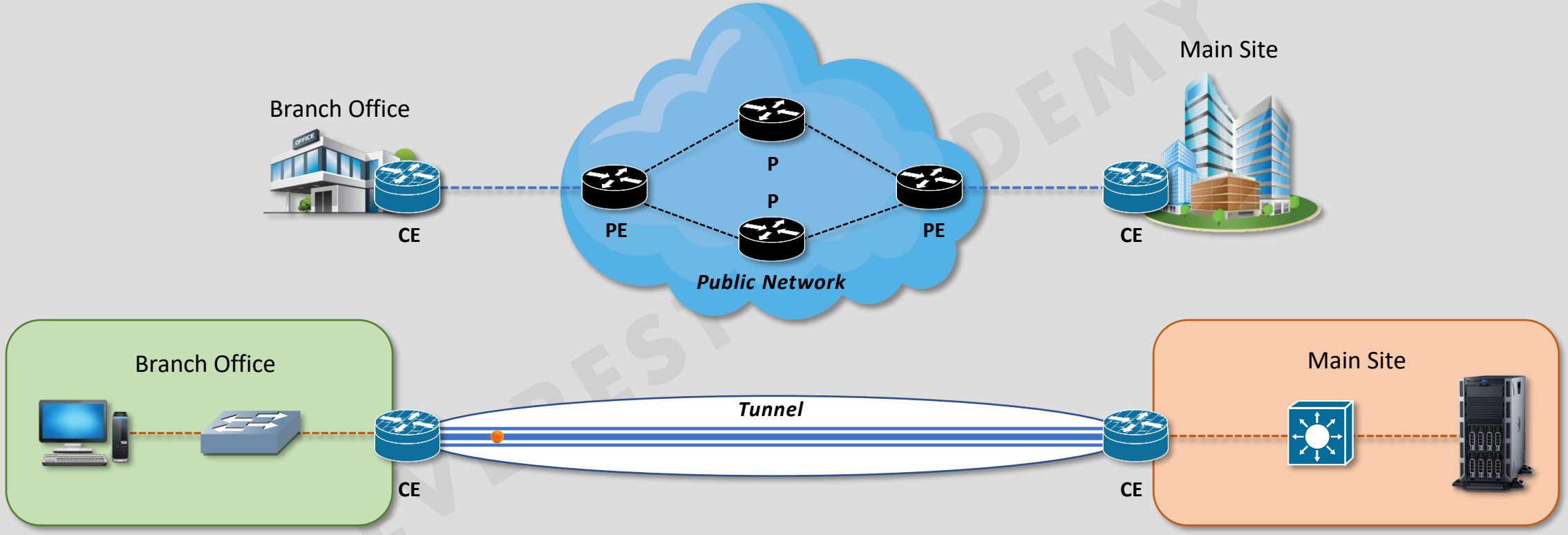
Virtual Private Networks (VPNs)

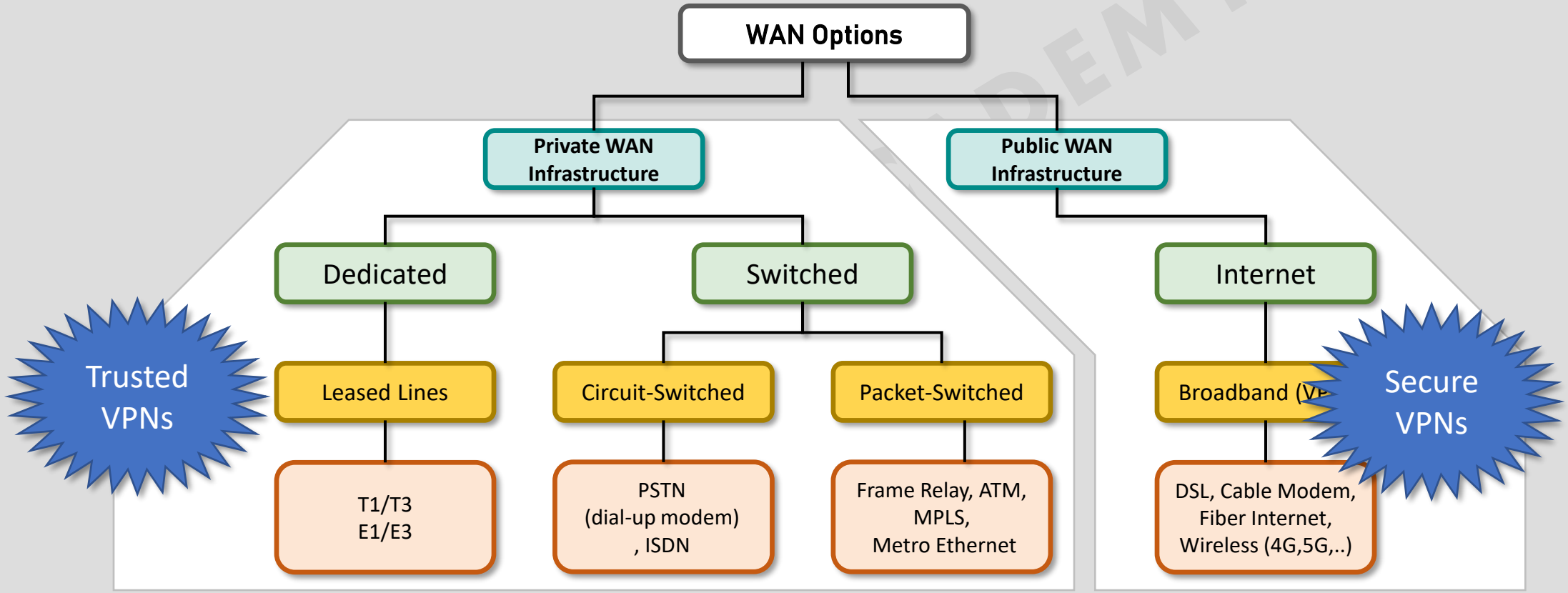
- **A virtual private network (VPN)** extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.



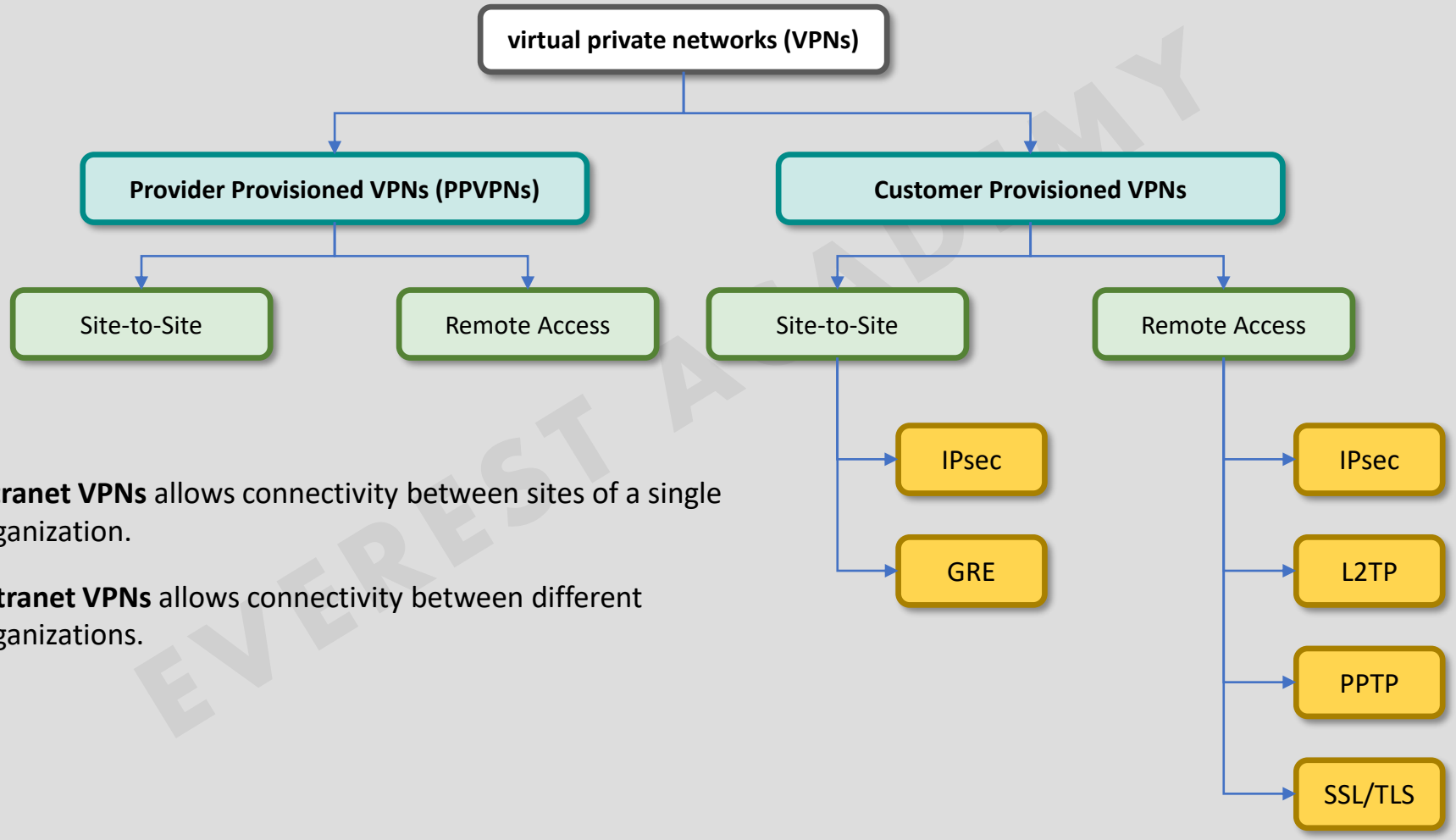
Virtual Private Network (VPN)

- **The benefits** of a VPN include increases in **functionality**, **security**, and **management** of the private network and it allows uses to **access** to resources inaccessible on the public.

Virtual Private Networks (VPNs)

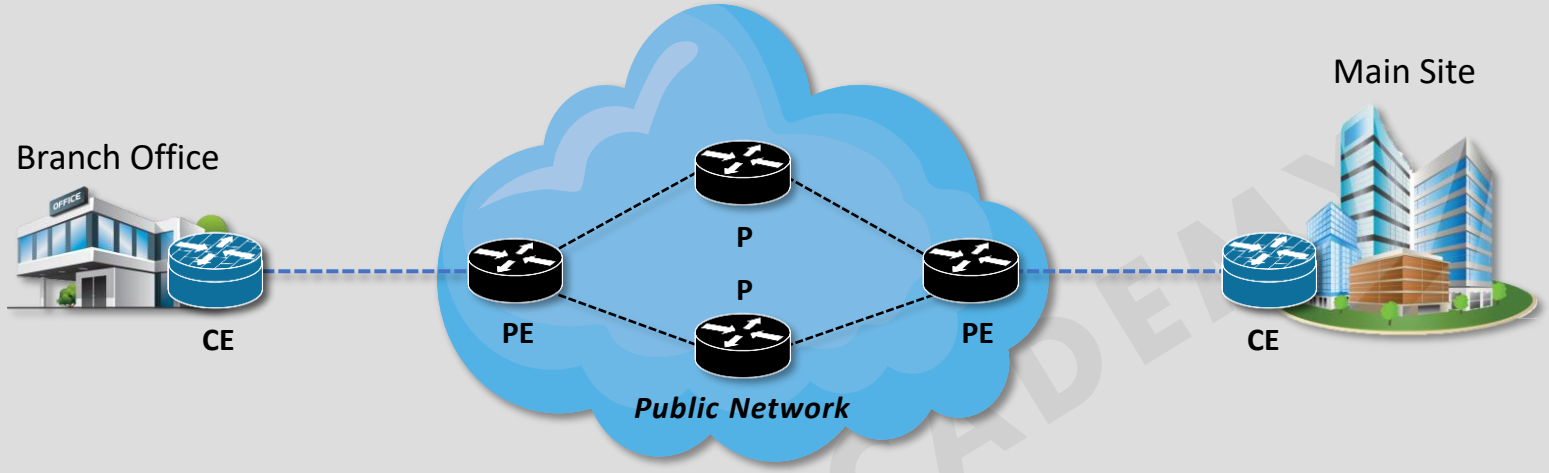


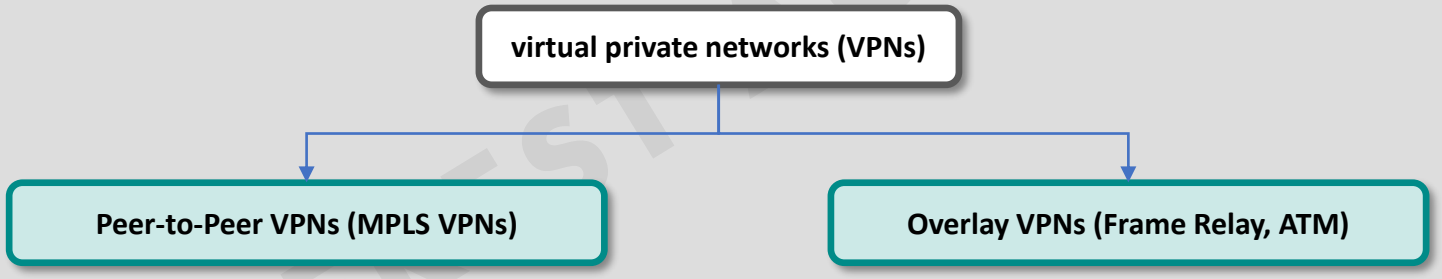
Virtual Private Networks (VPNs)



- **Intranet VPNs** allows connectivity between sites of a single organization.
- **Extranet VPNs** allows connectivity between different organizations.

Virtual Private Networks (VPNs)

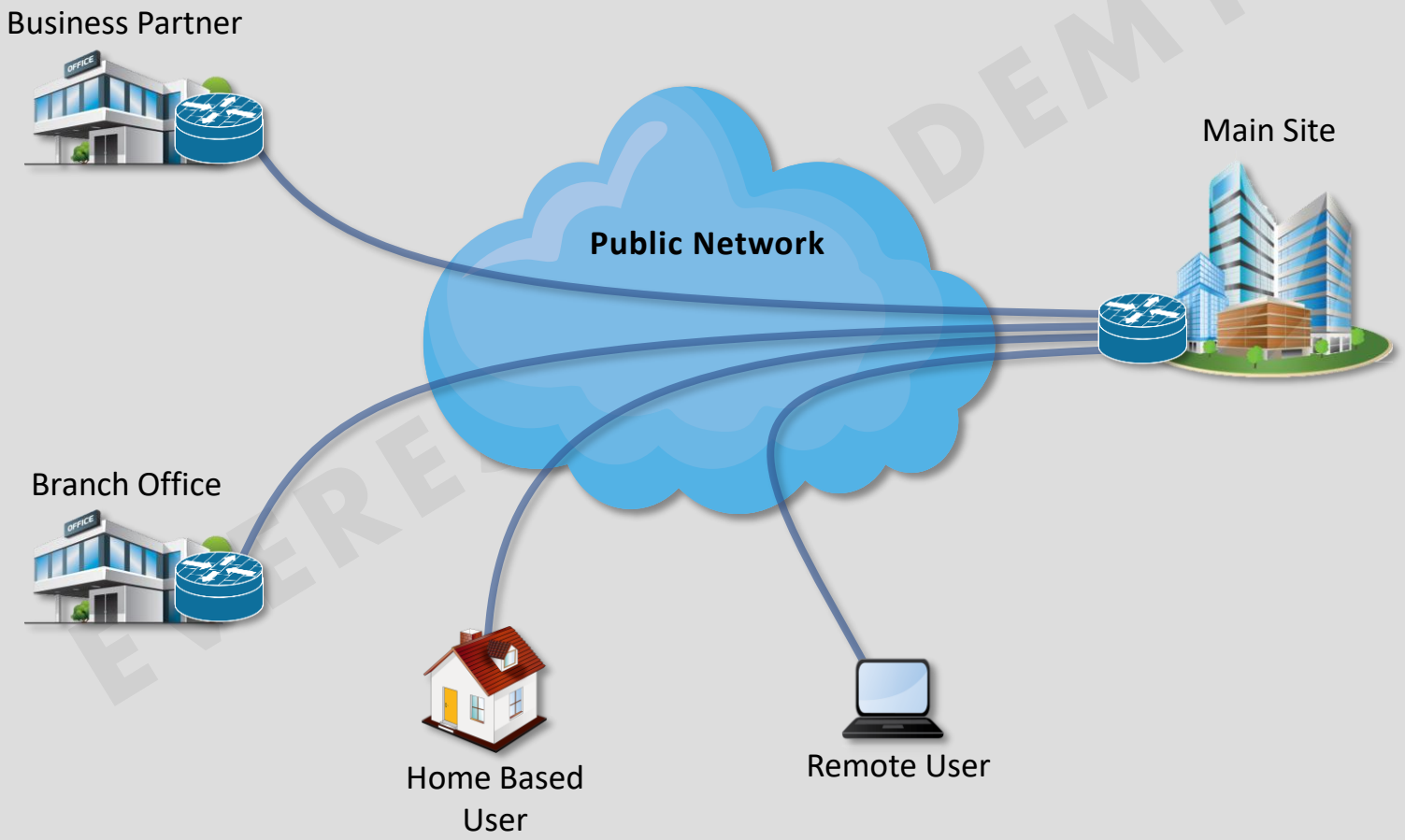




- **Peer-to-Peer VPNs** : the service provider routers carry the customer data across the network, but they also **participate in the customer routing**. In other words, the service provider routers peer directly with the customer routers at Layer 3. The result is that one routing protocol neighborship or adjacency exists between the customer and the service provider router.

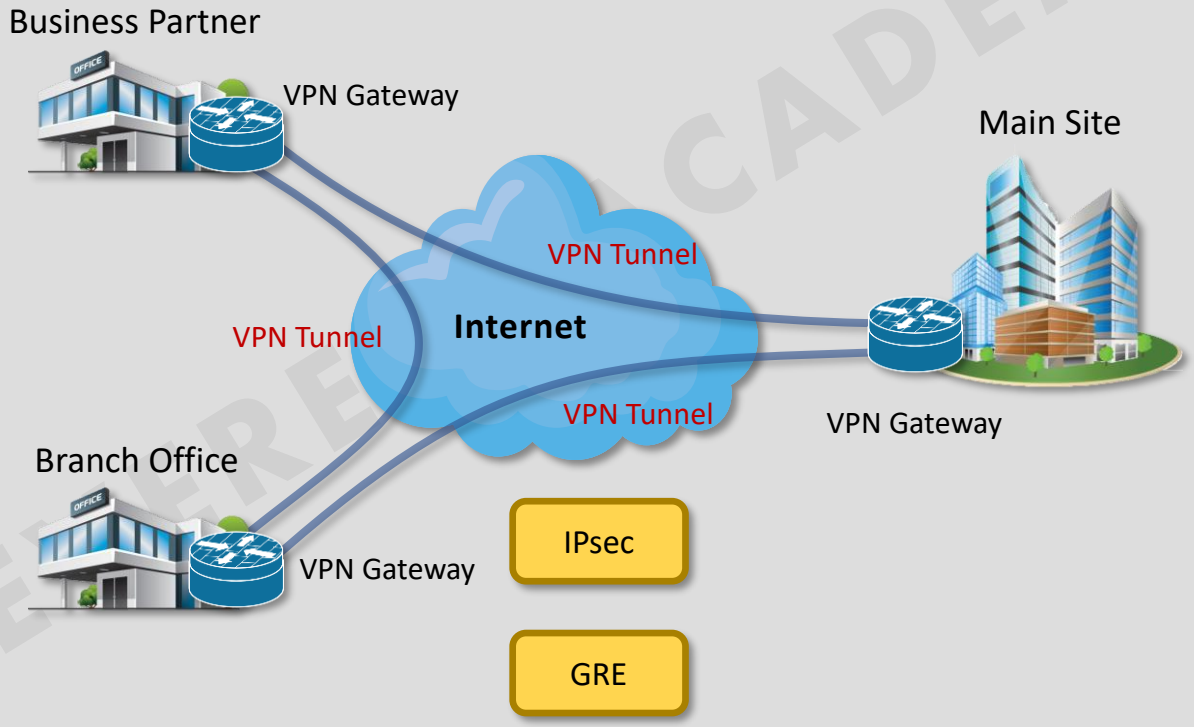
- **Overlay VPNs :** the service provider supplies a service of **point-to-point links** or **virtual circuits** across his network between the routers of the customer. The customer routers form routing peering between them directly across the links or virtual circuits from the service provider. The routers or switches from the service provider carry the customer data across the service provider network, but **no routing peering** occurs between a customer and a service provider router.

Virtual Private Networks (VPNs)



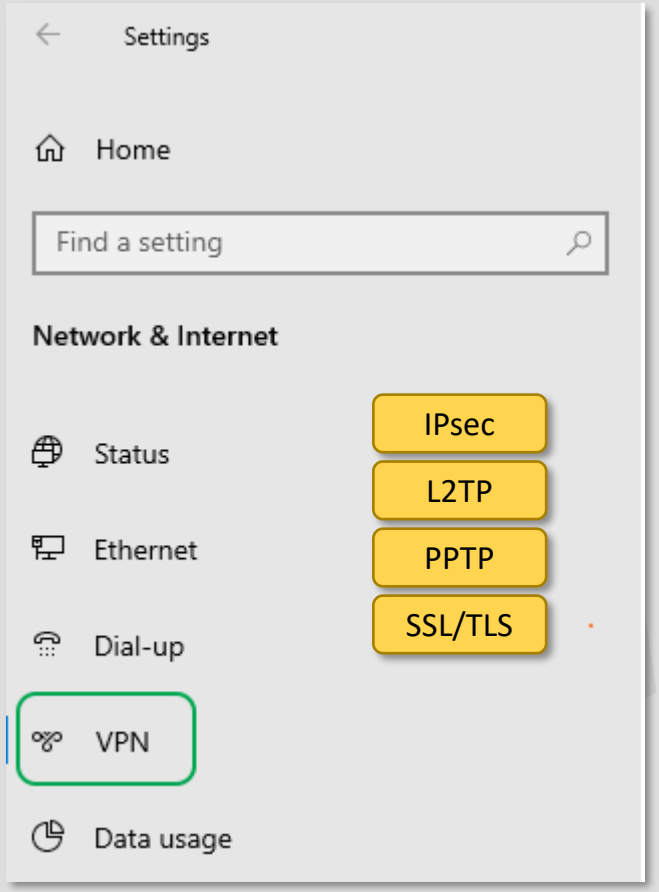
Site-to-Site VPNs

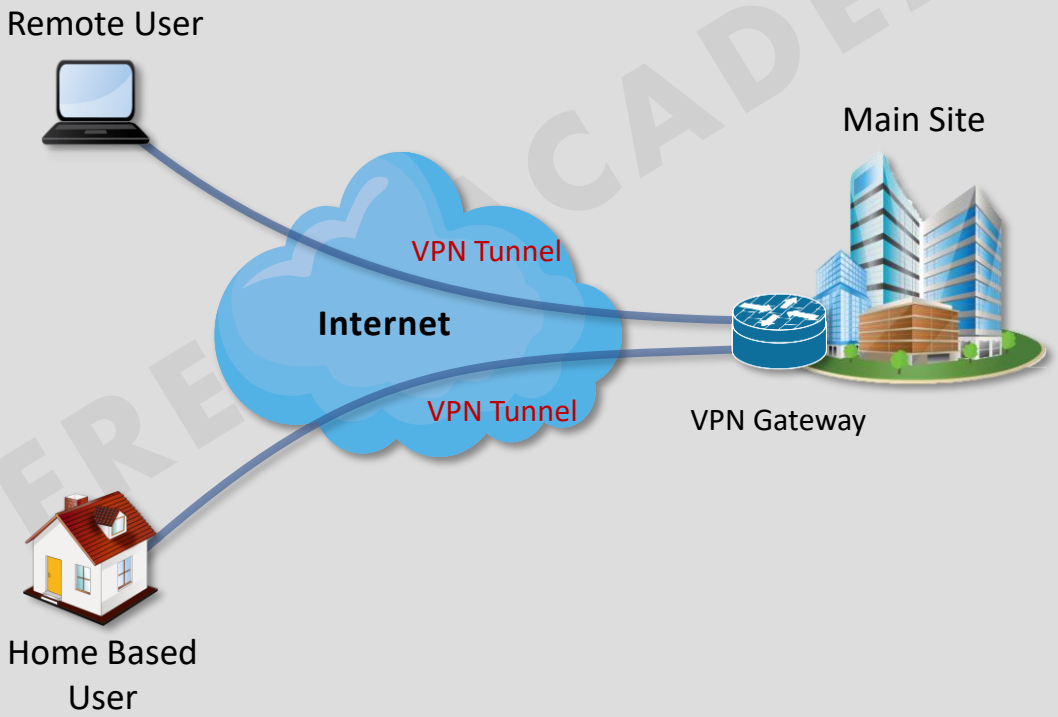
- **Site-to-site VPNs** are deployed for interconnecting corporate sites. the network of one location (site) is connected to the network of another location (site) via a VPN.



Remote Access VPNs

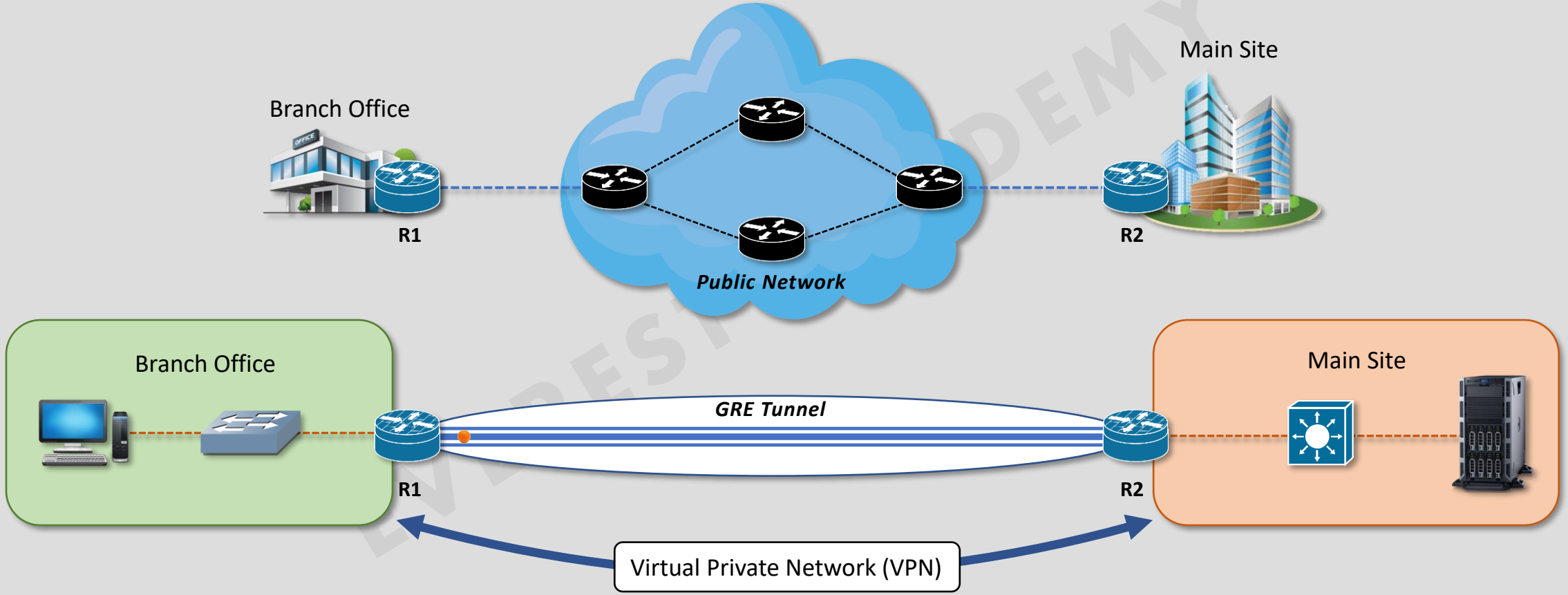
- **Remote access VPNs** allow mobile or home-based users to access an organization's recourses remotely. It provide a secure connection (tunnel) back to the organization.





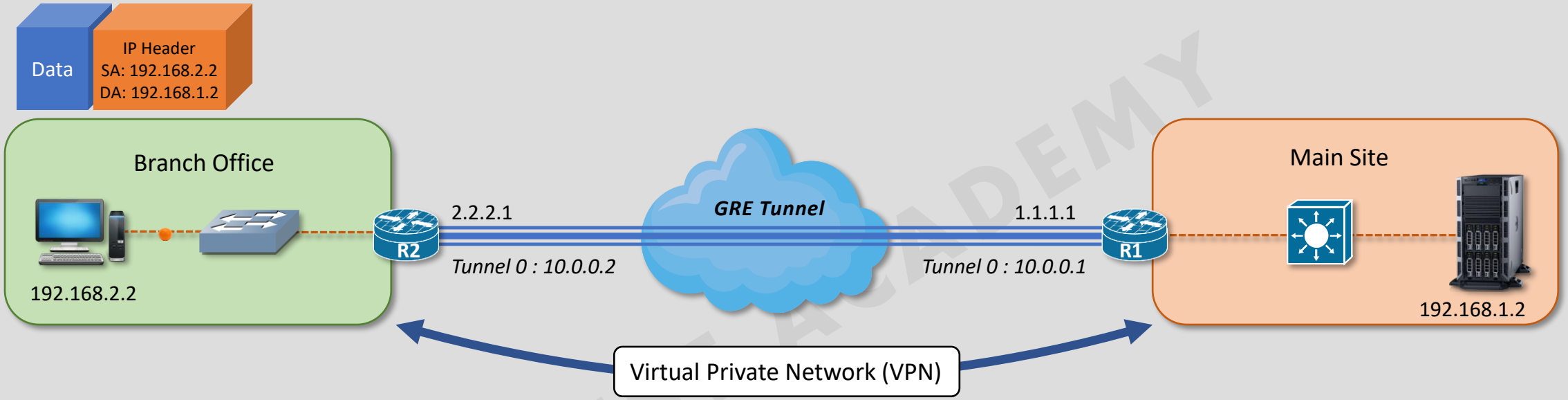
Generic Routing Encapsulation (GRE)

- **Generic Routing Encapsulation (GRE)** is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links or point-to-multipoint links over an Internet Protocol network.



- **GRE** can be used with IPsec VPNs to allow passing of routing information between connected networks.

Generic Routing Encapsulation (GRE)

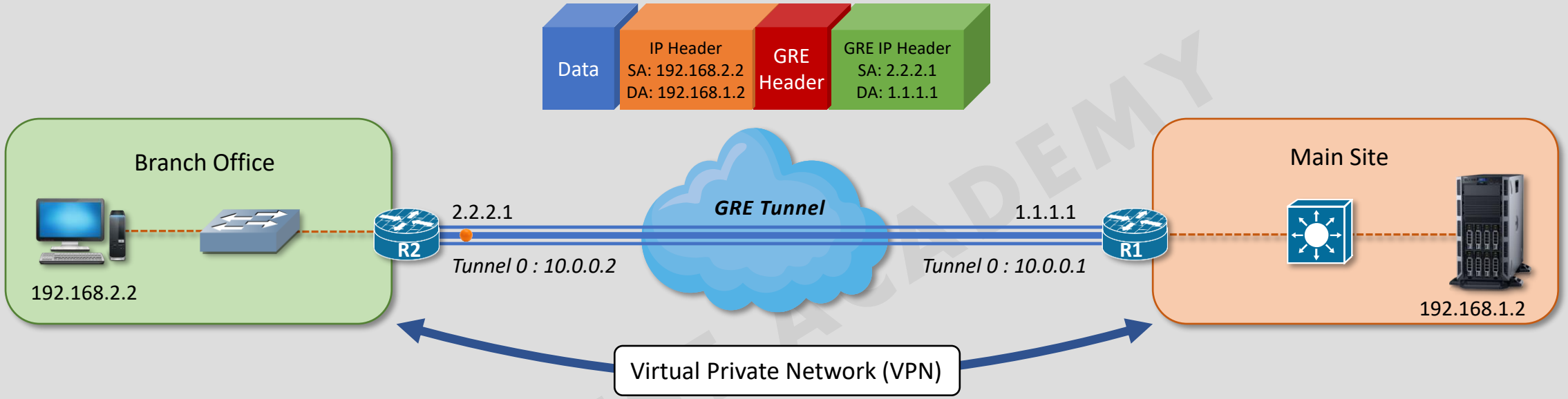


icmp

Source	Destination	Protocol
192.168.2.2	192.168.1.2	ICMP

```
> Frame 14: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
> Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: c0:01:04:04:00:00 (c0:01:04:04:00:00)
> Internet Protocol Version 4, Src: 192.168.2.2 (192.168.2.2), Dst: 192.168.1.2 (192.168.1.2)
> Internet Control Message Protocol
```

Generic Routing Encapsulation (GRE)

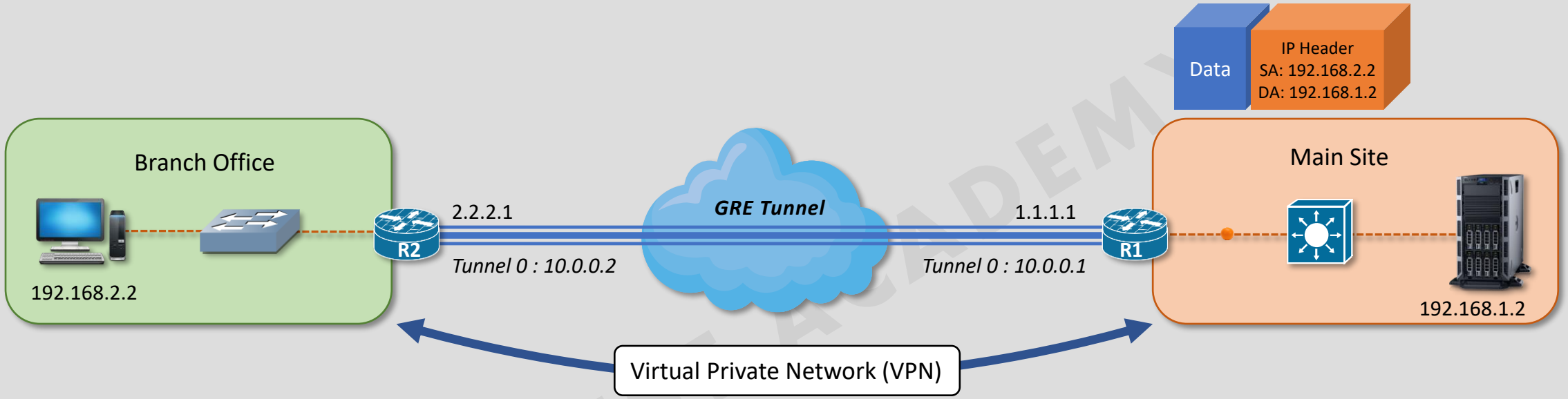


icmp

Source	Destination	Protocol
192.168.2.2	192.168.1.2	ICMP

```
> Frame 5: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface -, id 0
> Ethernet II, Src: c0:01:04:04:00:01 (c0:01:04:04:00:01), Dst: c0:03:04:24:00:01 (c0:03:04:24:00:01)
> Internet Protocol Version 4, Src: 2.2.2.1 (2.2.2.1), Dst: 1.1.1.1 (1.1.1.1)
> Generic Routing Encapsulation (IP)
> Internet Protocol Version 4, Src: 192.168.2.2 (192.168.2.2), Dst: 192.168.1.2 (192.168.1.2)
> Internet Control Message Protocol
```

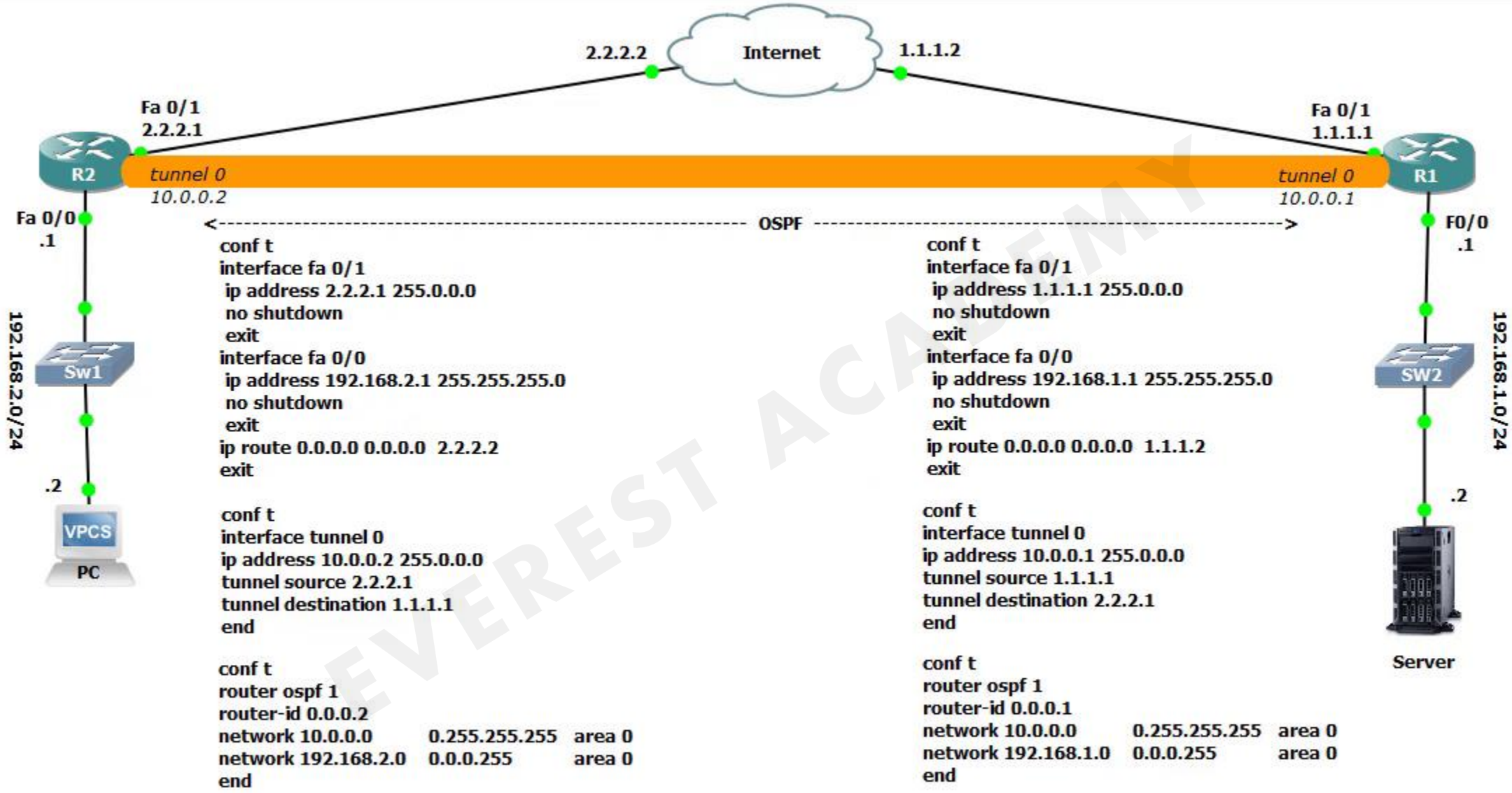
Generic Routing Encapsulation (GRE)

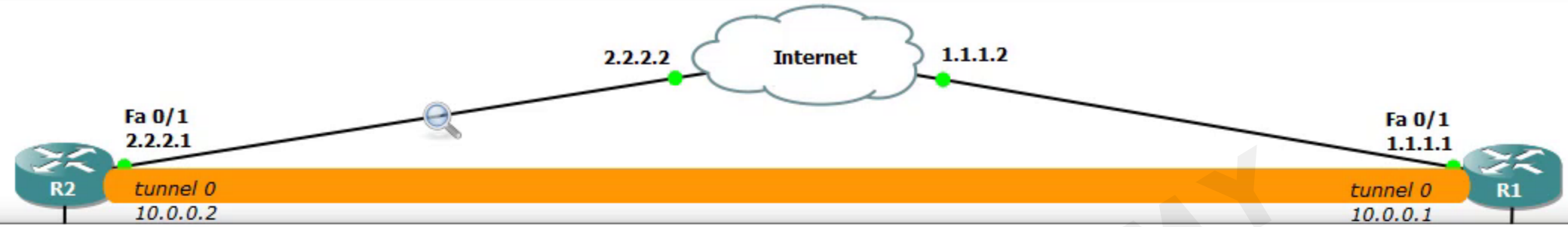


icmp

Source	Destination	Protocol
192.168.2.2	192.168.1.2	ICMP

```
> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
> Ethernet II, Src: c0:02:04:14:00:00 (c0:02:04:14:00:00), Dst: Private_66:68:01 (00:50:79:66:68:01)
> Internet Protocol Version 4, Src: 192.168.2.2 (192.168.2.2), Dst: 192.168.1.2 (192.168.1.2)
> Internet Control Message Protocol
```





*- [R2 FastEthernet0/1 to Internet FastEthernet0/1]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

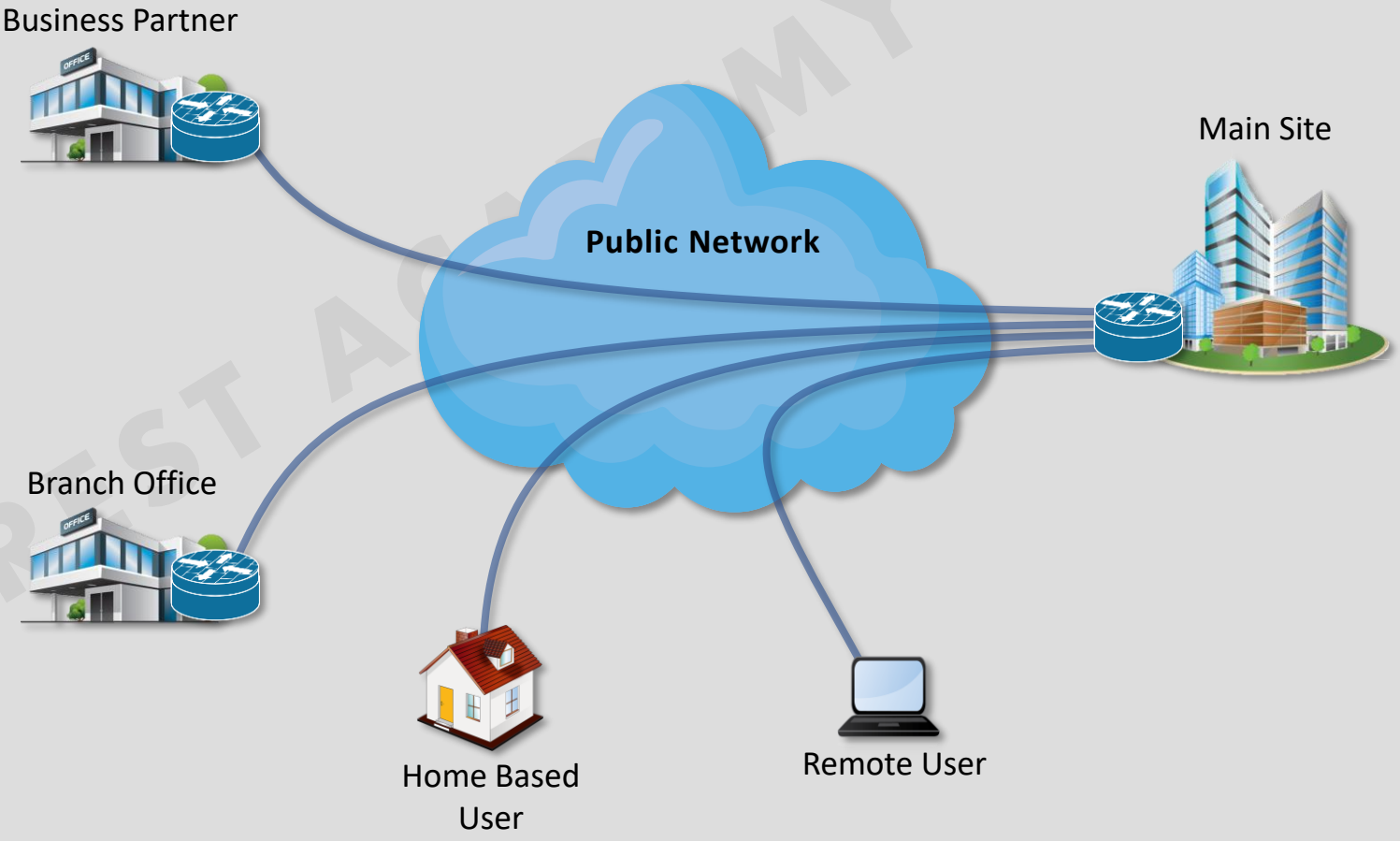
Source	Destination	Protocol	data
192.168.2.2	192.168.1.2	ICMP	

```
> Frame 20: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface -, id 0
> Ethernet II, Src: c0:01:04:04:00:01 (c0:01:04:04:00:01), Dst: c0:03:04:24:00:01 (c0:03:04:24:00:01)
> Internet Protocol Version 4, Src: 2.2.2.1 (2.2.2.1), Dst: 1.1.1.1 (1.1.1.1)
> Generic Routing Encapsulation (IP)
> Internet Protocol Version 4, Src: 192.168.2.2 (192.168.2.2), Dst: 192.168.1.2 (192.168.1.2)
> Internet Control Message Protocol
```

Internet Protocol Security (IPsec)

- **Internet Protocol Security (IPsec)** is a secure network protocol suite that *authenticates* and *encrypts* the packets of data to provide secure encrypted communication between two devices over an Internet Protocol network.

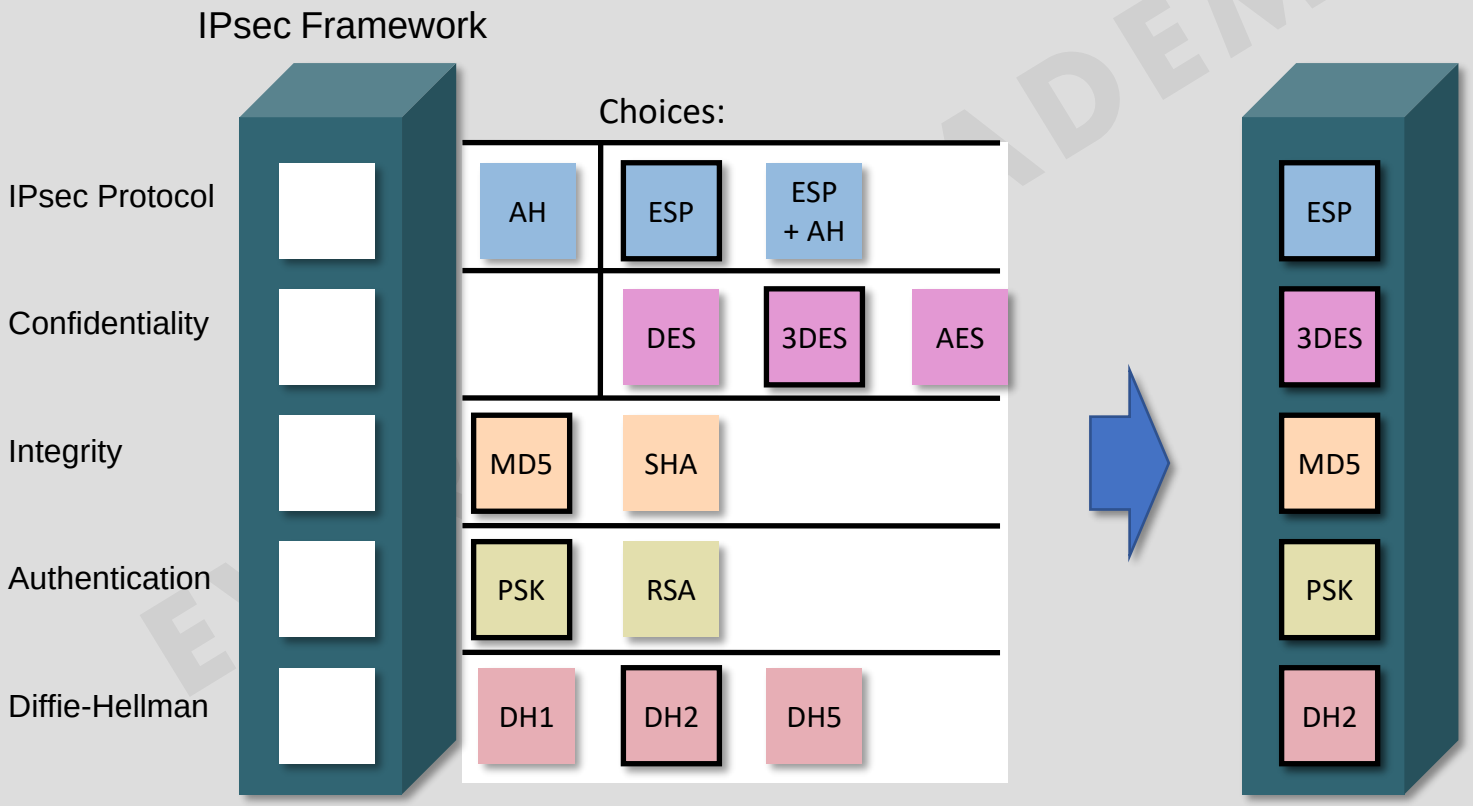
- Confidentiality
- Integrity
- Authentication
- Anti-replay



- Routers.
- Firewalls.
- Hosts.
- Servers.

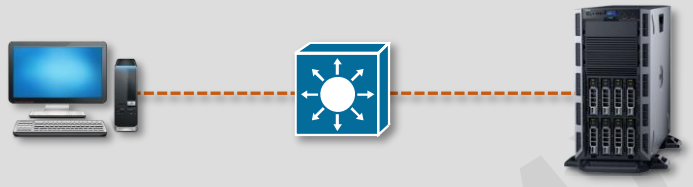
Internet Protocol Security (IPsec)

- **IPsec Authentication Header (AH).**
- **Encapsulating Security Payload (ESP).**

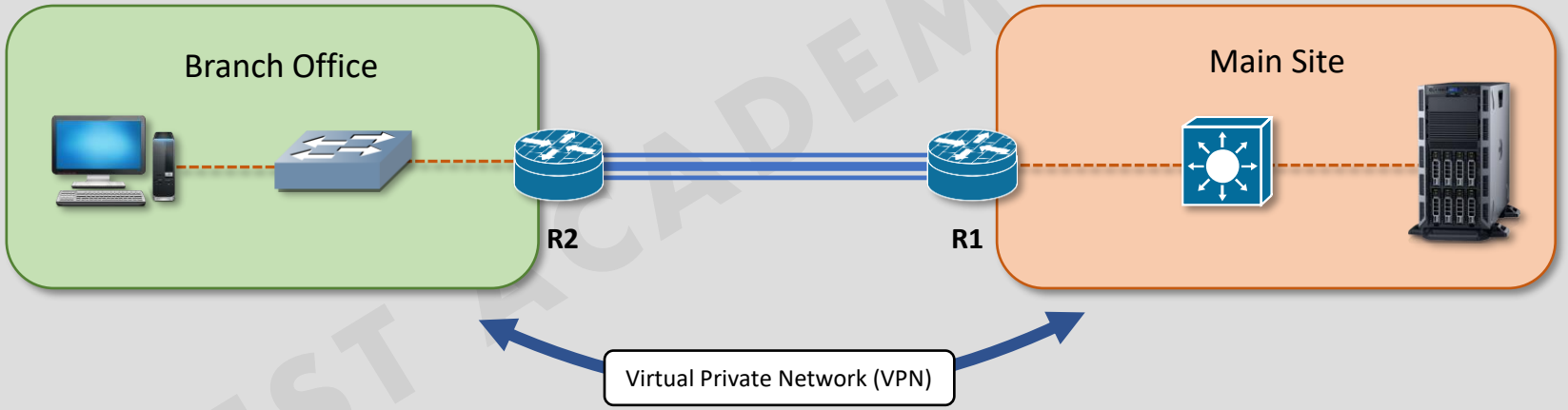


IPsec Encapsulation modes

- **Transport mode.**

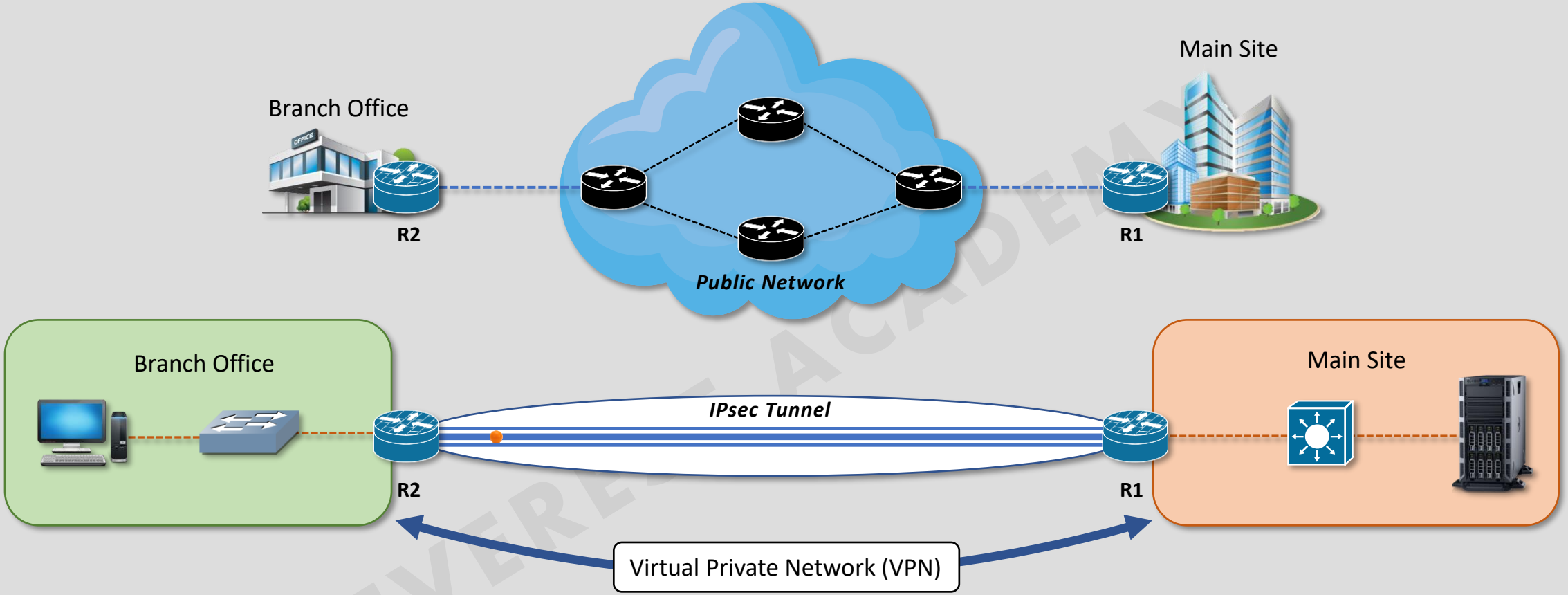


- **Tunnel mode.**



Protocol	Transport Mode	Tunnel Mode
AH	IP AH Data	IP AH IP Data
ESP	IP ESP Data ESP-T	IP ESP IP Data ESP-T
ESP+AH	IP AH ESP Data ESP-T	IP AH ESP IP Data ESP-T

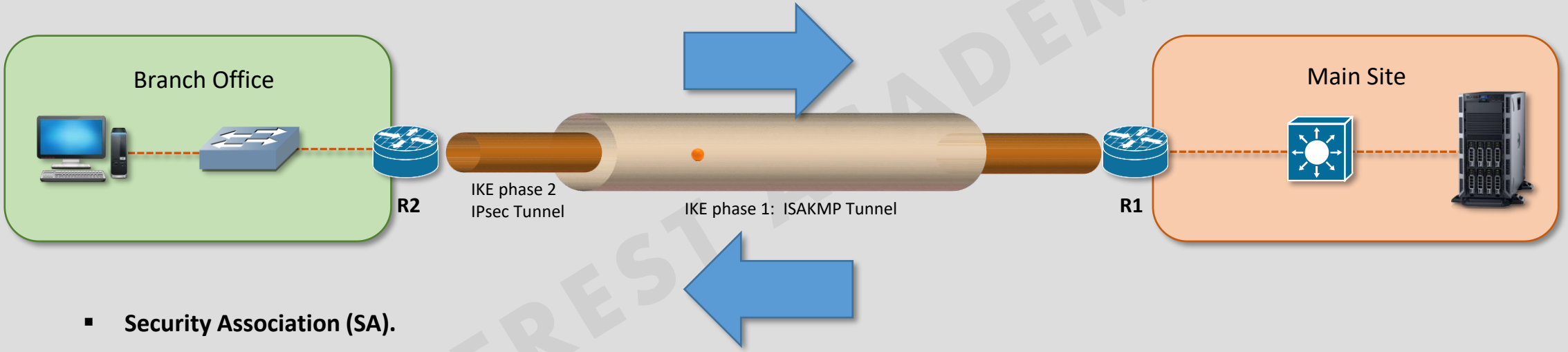
IPsec tunnel



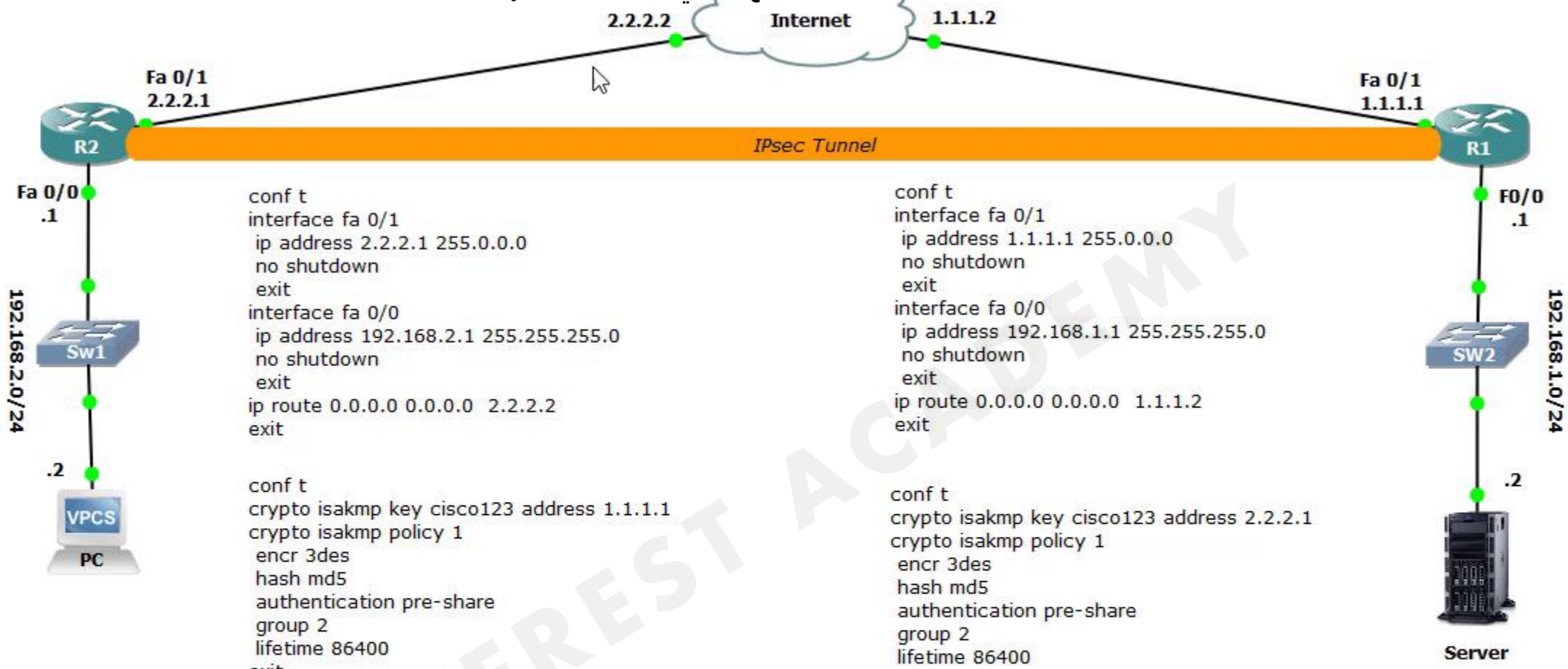
- **Internet Key Exchange (IKE) Protocol.**

1. IKE phase 1.
2. IKE phase 2.

IKE Phase 1 and IKE Phase 2



- **Security Association (SA).**
- **Internet Security Association and Key Management Protocol (ISAKMP).**




```
conf t
interface fa 0/1
 ip address 2.2.2.1 255.0.0.0
 no shutdown
 exit
interface fa 0/0
 ip address 192.168.2.1 255.255.255.0
 no shutdown
 exit
ip route 0.0.0.0 0.0.0.0  2.2.2.2
exit
```

```
conf t
crypto isakmp key cisco123 address 1.1.1.1
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 86400
exit
ip access-list extended VPN_TRAFFIC
 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
exit
crypto ipsec transform-set TS esp-3des esp-md5-hmac
exit
crypto map BranchA 10 ipsec-isakmp
 set peer 1.1.1.1
 set transform-set TS
 match address VPN_TRAFFIC
exit
 interface FastEthernet0/1
 crypto map BranchA
end
```

```
conf t
interface fa 0/1
 ip address 1.1.1.1 255.0.0.0
 no shutdown
 exit
interface fa 0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown
 exit
ip route 0.0.0.0 0.0.0.0  1.1.1.2
exit
```

```
conf t
crypto isakmp key cisco123 address 2.2.2.1
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 86400
exit
ip access-list extended VPN_TRAFFIC
 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
exit
crypto ipsec transform-set TS esp-3des esp-md5-hmac
exit
crypto map Main_Site 10 ipsec-isakmp
 set peer 2.2.2.1
 set transform-set TS
 match address VPN_TRAFFIC
exit
 interface FastEthernet0/1
 crypto map Main_Site
end
```