-Site 2 site Drawbacks
-- Intresting traffic is define by ACL

1
2
3
4
5
.
.
100
latency

Does not Support BUM
Broadcast
Unknown unicast
Multicast
Class D 224.0.0.0/24
224.0.0.10
224.0.0.9
224.0.0.5
224.0.0.6

GRE (Generic routing encapsulation)
--Developed by cisco system
--RFC 2874
--Tunneling protocol
--Protocol no 47
-Can Encapsulate ip,non ip
-Point to point
-Point to Multipoint
-Supports BUM
-Supports Dynamic routing/Static

-Clear/plain tunnel
-Does not offer Security

R1
conf t
int e0/0
Desc conn to internet
ip add 1.1.1.1 255.255.255.0
no shut
int e0/1
Desc conn to LAN
ip add 10.1.1.1 255.255.255.0
no shut
exit

ip route 0.0.0.0 0.0.0.0 1.1.1.2

R2: internet
conf t

```
int e0/0
ip add 1.1.1.2 255.255.255.0
no sh
int e0/1
ip add 3.3.3.2 255.255.255.0
no sh
exit

R3
conf t
int e0/0
Desc conn to internet
ip add 3.3.3.3 255.255.255.0
no shut
int e0/1
Desc conn to LAN
ip add  192.168.3.254  255.255.255.0
no shut
exit

ip route 0.0.0.0 0.0.0.0  3.3.3.2

=======================================================
GRE config
R1
interface Tunnel1
 bandwidth 4000
 ip address 192.168.1.1 255.255.255.0
 ip mtu 1400
 keepalive 10 3
 tunnel source Ethernet0/0
 tunnel destination 3.3.3.3
 tunnel key 123
exit


R3:
interface Tunnel1
 bandwidth 4000
 ip address 192.168.1.2 255.255.255.0
 ip mtu 1400
 keepalive 10 3
 tunnel source 3.3.3.3
 tunnel destination 1.1.1.1
 tunnel key 123
exit


interface Tunnel1
 ip address 192.168.1.2 255.255.255.0
 tunnel source 3.3.3.3
 tunnel destination 1.1.1.1
exit

=============================================
```

Static routing

R1
ip route 192.168.3.0 255.255.255.0 tun1 192.168.1.2

R3
ip route 10.1.1.0 255.255.255.0 tun1 192.168.1.1

==========
Dynamic Routing

Tunnel ip
LAN
RIPV2:

R1:
Router Rip
ver 2
no auto
net 192.168.1.0
net 10.0.0.0
exit

R3:
Router rip
ver 2
no auto
net 192.168.1.0
net 192.168.3.0
exit

OSPF
R1
Int range tun1,e0/1
ip ospf 1 area 0
exit

R3
Router ospf 1
net 192.168.1.2 0.0.0.0 area 0
net 192.168.3.254 0.0.0.0 area 0
exit

Eigrp:

R1
Router Eigrp 1
net 192.168.1.1 0.0.0.0
net 10.1.1.1 0.0.0.0
exit

R3
Router Eigrp 1
net 192.168.1.2 0.0.0.0
net 192.168.3.0
exit
==========
Site2Site
1.Create isakmp policy
2.pre shared key
3. Define Intresting with ACL
4.Transform-set ESP/AH
5.Crypto MAP (Physical interfaces)
6.Apply cmap on WAN interface

crypto map cmap 10 ipsec-isakmp
 set peer 3.3.3.3
 set transform-set tset
 match address 101
exit

int e0/0
Cry map cmap
exit

GRE over ipsec
1.Create the isakmp policy
2.pre share key
3.ACL not required (Dynamic Routing)
4.Transform-set ESP/AH
5.Cry ipsec profile

Cry ipsec prof PROF
set transform-set tset
exit

6. Tunnel protection with ipsec prof
  int tun 1
tunnel protection ipsec profile PROF
exit

R1
Phase 1:

Crypto isakmp policy 1
hash md5
auth pre-share
group 5
enc aes
exit

cry isakmp key cisco123 address 3.3.3.3

Phase 2:

cry ipsec transform-set tset esp-aes esp-sha-hmac
exit

crypto ipsec profile PROF
set transform-set tset
exit

in tun 1
tunnel protection ipsec profile PROF
exit

R3:
Crypto isakmp policy 1
hash md5
auth pre-share
group 5
enc aes
exit

cry isakmp key cisco123 address 3.3.3.3

Phase2:
---
cry ipsec transform-set tset esp-aes esp-sha-hmac
exit

crypto ipsec profile PROF
set transform-set tset
exit

in tun 1
tunnel protection ipsec profile PROF
exit

==========
Changing Transform set mode from tunnel to Transport

R1/R3
int tun 1
shut
exit

clear cry sess
clear cry sa

cry ipsec transform-set tset esp-aes esp-sha-hmac
mode transport
exit