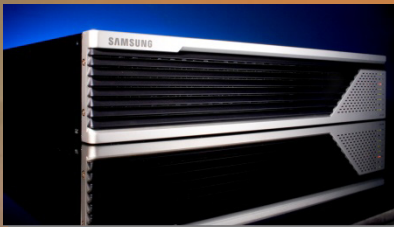


IPSec VPN Configuration



Contents

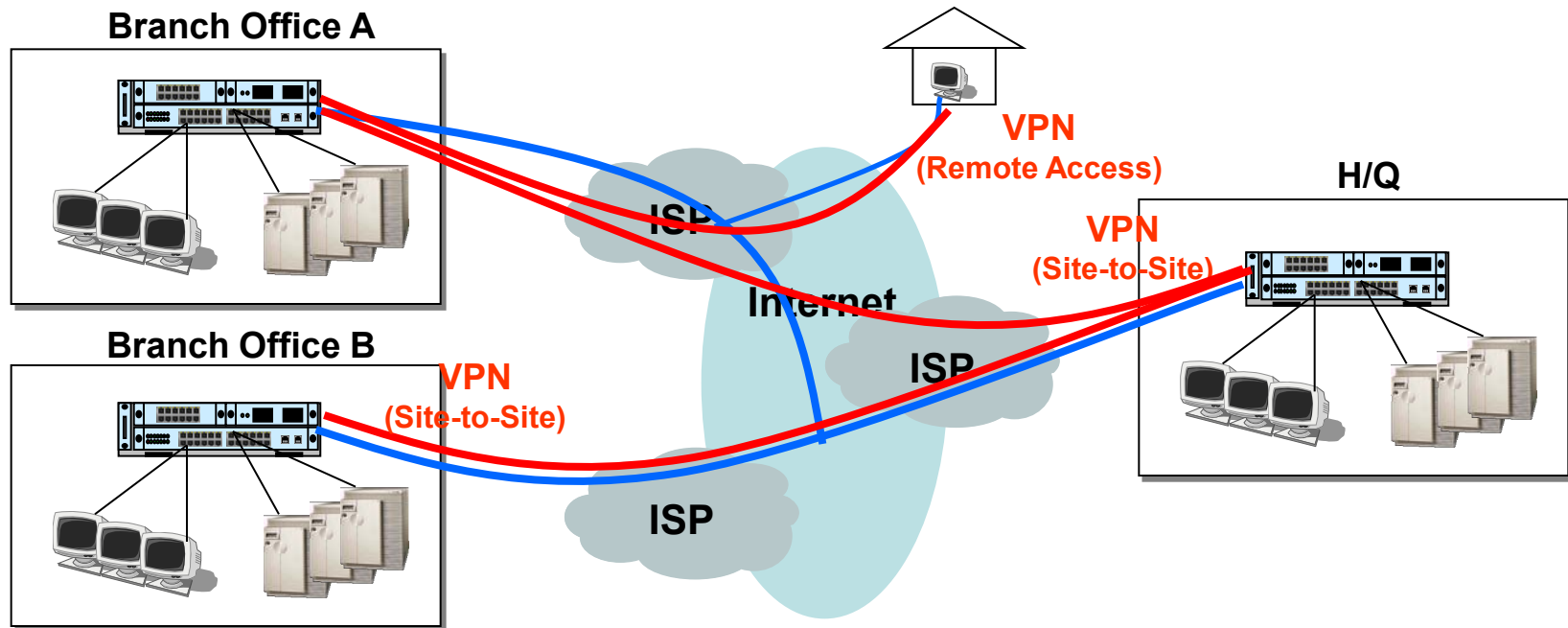
- Overview
- Basic Configuration

Overview



Virtual Private Network

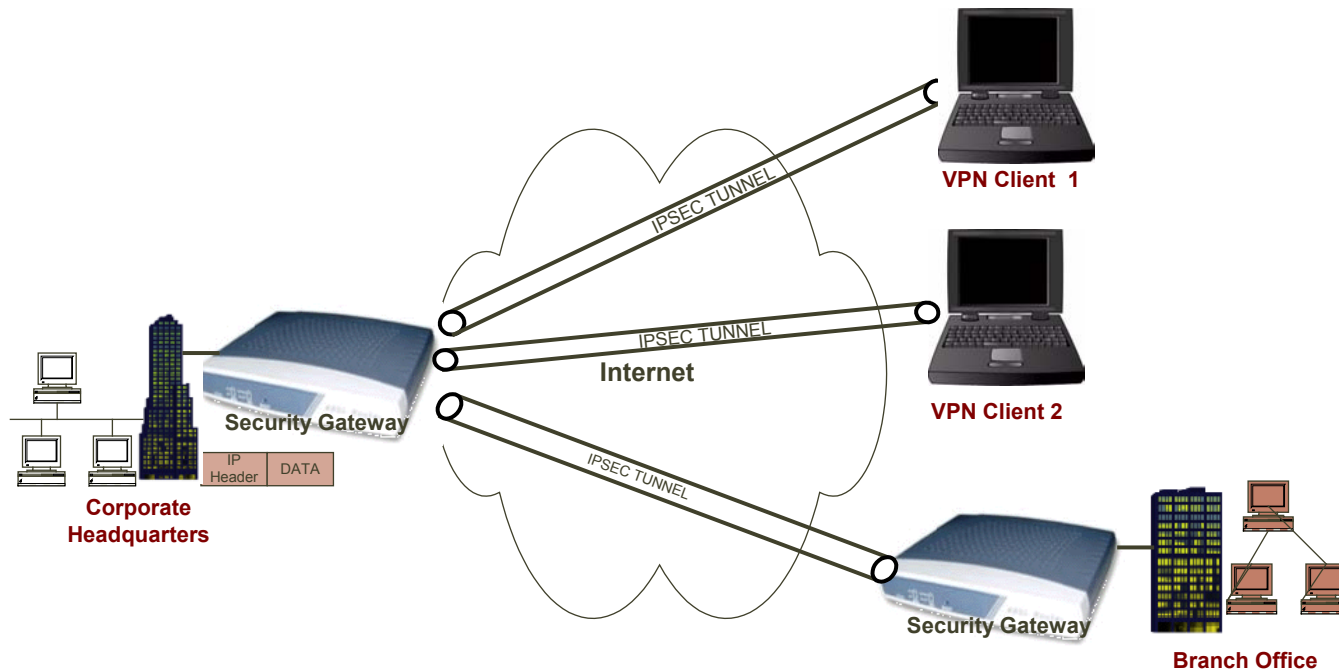
- VPN provides secure connectivity without seriously degrading performance.





Remote access VPN

- Remote Access VPN provide remote access to a corporate Intranet or extranet over a shared infrastructure with the same policies as a private network.
- Remote Access VPN enable users to access corporate resources whenever, wherever, and however they require.



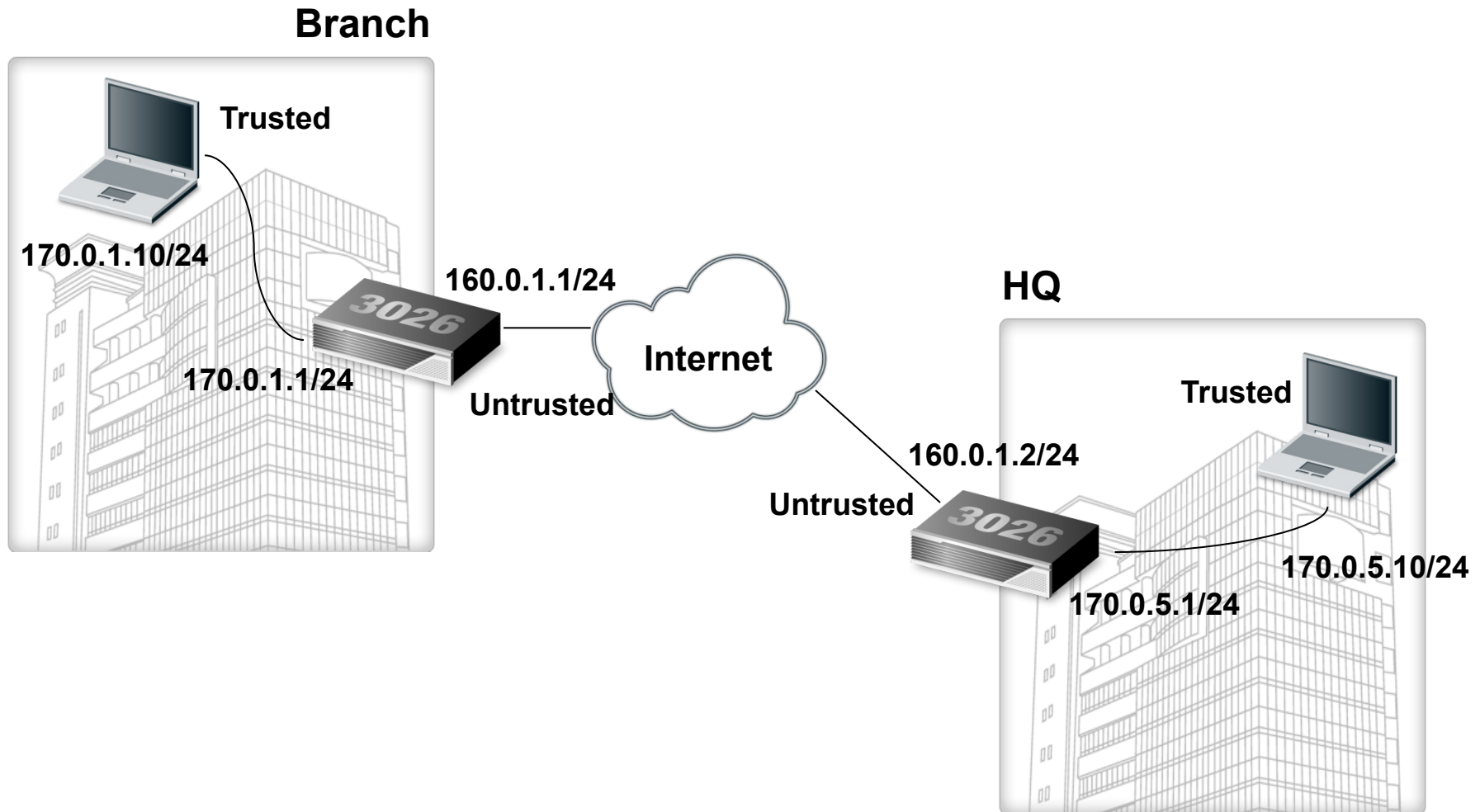
● Site to site VPN

- Site-to-Site VPN are an alternative WAN infrastructure that used to connect branch offices, home offices, or business partners' sites to all or portions of a company's network.
- VPN do not inherently change private WAN requirements, such as support for multiple protocols, high reliability, and extensive scalability, but instead meet these requirements more cost-effectively and with greater flexibility.
- Site to Site Tunneling supported in two ways
 - IPSec Tunneling
 - GRE + IPSec Tunneling

Basic Configuration

Network Configuration

● Site to Site IPSec VPN



Exercise) #1, Site to Site IPSec VPN (ibg01)



● Configuring a network type for interface. (trusted/untrusted)

```
Ibg01/configure# interface ethernet 0/2
Ibg01/configure/interface/ethernet (0/2)#
Ibg01/configure/interface/ethernet (0/2)# ip address 160.0.1.1/24
Ibg01/configure/interface/ethernet (0/2)# end

Ibg01/configure# interface ethernet 2/0
Ibg01/configure/interface/ethernet (2/0)#
Ibg01/configure/interface/ethernet (2/0)# ip address 170.0.1.1/24
Ibg01/configure/interface/ethernet (2/0)# end
```

● Enabling firewall policy

- VPN & firewall function is tightly coupled.

```
Ibg01/configure# firewall internet
Ibg01/configure/firewall internet# interface ethernet0/2
Ibg01/configure/firewall internet# policy 1022 in self
ibg01/configure/firewall internet/policy 100 in# exit 2
ibg01/configure/firewall internet#
ibg01/configure# firewall corp
ibg01/configure/firewall corp# interface ethernet2/0
ibg01/configure/firewall corp# policy 1021 in
ibg01/configure/firewall corp/policy 1021 in# exit 3
ibg01/configure/firewall corp#
```

Exercise) #1, Site to Site IPSec VPN (ibg01)



- Show a network type of the interface

```
ibg01# show firewall interface all
```

Interface	Map Name
-----	-----
ethernet0/2	internet
ethernet2/0	corp

```
ibg01#
```

Exercise) #1, Site to Site IPSec VPN (ibg02)



● Configuring a network type for interface. (trusted/untrusted)

```
Ibg01/configure# interface ethernet 0/2
Ibg01/configure/interface/ethernet (0/2)#
Ibg01/configure/interface/ethernet (0/2)# ip address 160.0.1.2/24
Ibg01/configure/interface/ethernet (0/2)# end

Ibg01/configure# interface ethernet 2/0
Ibg01/configure/interface/ethernet (2/0)#
Ibg01/configure/interface/ethernet (2/0)# ip address 170.0.5.1/24
Ibg01/configure/interface/ethernet (2/0)# end
```

● Enabling firewall policy

- VPN & firewall function is tightly coupled.

```
Ibg02/configure# firewall internet
Ibg02/configure/firewall internet# interface ethernet0/2
Ibg02/configure/firewall internet# policy 1022 in self
ibg02/configure/firewall internet/policy 100 in# exit 2
ibg02/configure/firewall internet#
ibg02/configure# firewall corp
ibg02/configure/firewall corp# interface ethernet2/0
ibg02/configure/firewall corp# policy 1021 in
ibg02/configure/firewall corp/policy 1021 in# exit 3
ibg02/configure/firewall corp#
```

Exercise) #1, Site to Site IPSec VPN (ibg02)



- Show a network type of the interface

```
ibg02# show firewall interface all
```

Interface	Map Name
-----	-----
ethernet0/2	internet
ethernet2/0	corp

```
ibg02#
```

Exercise) #2, IKE configuration (ibg01)



● Configure crypto ike policy

peer ip address

```
Ibg01/configure# crypto
Ibg01/configure/crypto# ike policy pol1 160.0.1.2
Ibg01/configure/crypto/ike/policy pol1 160.0.1.2# local-address 160.0.1.1
Default proposal created with priority1-des-sha1-pre_shared-g1
Key String has to be configured by the user
```

● Configure crypto ike policy key

```
Ibg01/configure/crypto/ike/policy pol1 160.0.1.2# key samsung123
```


Exercise) #2, IKE configuration (ibg01)



● Show a ike information

```
ibg01/configure/crypto/ike/policy poll 160.0.1.2# show crypto ike policy
poll detail

Policy name poll, Local addr 160.0.1.1, Peer addr 160.0.1.2
Main mode, Initiator and Responder, PFS is not enabled, Shared Key is *****
Local ident 160.0.1.1 (ip-address), Remote Ident 160.0.1.2 (ip-address)
NGM attributes not configured
OCSP is not enabled

Proposal of priority 1
  Encryption algorithm: des
  Hash Algorithm: sha1
  Authentication Mode: pre-shared-key
  DH Group: group1
  Lifetime in seconds: 86400
  Lifetime in kilobytes: unlimited

ibg01/configure/crypto/ike/policy poll 160.0.1.2#
```

Exercise) #2, IKE configuration (ibg02)



● Configure crypto ike policy

peer ip address

```
ibg02/configure# crypto
ibg02/configure/crypto#
ibg02/configure/crypto# ike policy poll 160.0.1.1
ibg02/configure/crypto/ike/policy poll 160.0.1.1# local-address 160.0.1.2
Default proposal created with priority1-des-sha1-pre_shared-g1
Key String has to be configured by the user
```

● Configure crypto ike policy key

```
ibg02/configure/crypto/ike/policy poll 160.0.1.1# key samsung123
```

Exercise) #2, IKE configuration (ibg02)



● Show a ike information

```
ibg02/configure/crypto/ike/policy poll 160.0.1.1# show crypto ike policy
poll detail

Policy name poll, Local addr 160.0.1.2, Peer addr 160.0.1.1
Main mode, Initiator and Responder, PFS is not enabled, Shared Key is *****
Local ident 160.0.1.2 (ip-address), Remote Ident 160.0.1.1 (ip-address)
NGM attributes not configured
OCSP is not enabled

Proposal of priority 1
  Encryption algorithm: des
  Hash Algorithm: sha1
  Authentication Mode: pre-shared-key
  DH Group: group1
  Lifetime in seconds: 86400
  Lifetime in kilobytes: unlimited

ibg02/configure/crypto/ike/policy poll 160.0.1.1#
```

Exercise) #3, IPsec configuration (ibg01)



● Configure crypto ipsec policy

```
ibg01/configure# crypto
ibg01/configure/crypto# ipsec policy pol1 160.0.1.2
```

● Configure crypto ipsec policy match

```
ibg01/configure/crypto/ipsec/policy pol1 160.0.1.2# match address
170.0.1.0/24 170.0.5.0/24
Default proposal created with priority1-esp-3des-sha1-tunnel and activated.
```

● Configure crypto ipsec policy proposal

```
ibg01/configure/crypto/ipsec/policy pol1 160.0.1.2# proposal 1
```

Exercise) #3, IPsec configuration (ibg01)



● Show crypto ipsec policy

```
ibg01/configure/crypto/ipsec/policy poll 160.0.1.2# show crypto ipsec policy poll
```

Policy	Peer	Match	Proto	Transform
-----	----	-----	-----	-----
poll	160.0.1.2	S 170.0.1.0/24/any	Any	P1 esp-3des-sha1-tun1
		D 170.0.5.0/24/any		

Exercise) #3, IPsec configuration (ibg02)



● Configure crypto ipsec policy

```
ibg02/configure# crypto
ibg02/configure/crypto# ipsec policy pol1 160.0.1.1
```

● Configure crypto ipsec policy match

```
ibg02/configure/crypto/ipsec/policy pol1 160.0.1.1# match address
170.0.5.0/24 170.0.1.0/24
Default proposal created with priority1-esp-3des-sha1-tunnel and activated.
```

● Configure crypto ipsec policy proposal

```
ibg01/configure/crypto/ipsec/policy pol1 160.0.1.1# proposal 1
```

Exercise) #3, IPsec configuration (ibg02)



● Show crypto ipsec policy

```
ibg02/configure/crypto/ipsec/policy poll 160.0.1.1# show crypto ipsec policy poll
```

Policy	Peer	Match	Proto	Transform
-----	----	-----	-----	-----
poll	160.0.1.1	S 170.0.5.0/24/any	Any	P1 esp-3des-sha1-tun1
		D 170.0.1.0/24/any		

```
ibg02/configure/crypto/ipsec/policy poll 160.0.1.1#
```

Exercise) #4, Establish Session



- To establish an VPN session – Ping to the other match address

```
DUT-1# ping 170.0.5.1 sip 170.0.1.1
Pinging 170.0.5.1 (170.0.5.1); 64 bytes, timeout 5 seconds
.!!!!
Ping statistics for 170.0.5.1:
Packets: Transmitted 5, Received 4
Loss Rate 20%, approx. round-trip min/avg/max = 0/0/0 ms.
```

Exercise) #4, Establish Session



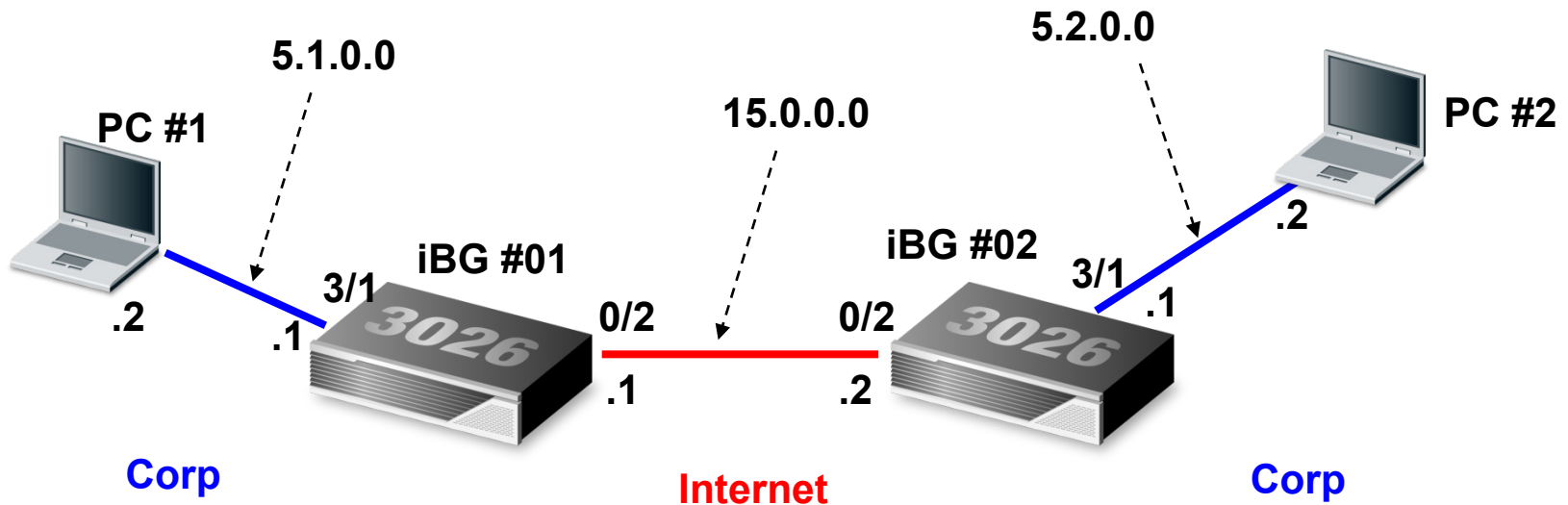
- After the VPN connection success, IPsec SA and IKE SA are created.

```
DUT-1# show crypto ipsec sa all
Policy      Dest IP      Spi          Packets      Transform
-----
INpol1      160.0.1.1    0xe47d8a2a   4            esp-aes-sha1-tunl
pol1        160.0.1.2    0xd8b99c50   4            esp-aes-sha1-tunl
DUT-1#
DUT-1# show crypto ike sa all
Policy      Peer          State         Bytes        Transform
-----
pol1        160.0.1.2     SA_MATURE     2040         pre-g1-des-sha1
DUT-1#
DUT-2#
DUT-2# show crypto ike sa all
Policy      Peer          State         Bytes        Transform
-----
pol1        160.0.1.1     SA_MATURE     2040         pre-g1-des-sha1
DUT-2#
DUT-2# show crypto ipsec sa all
Policy      Dest IP      Spi          Packets      Transform
-----
INpol1      160.0.1.2    0xd8b99c50   4            esp-aes-sha1-tunl
pol1        160.0.1.1    0xe47d8a2a   4            esp-aes-sha1-tunl
DUT-2#
```

Practice 1) Network Topology



● Configuration



Practice 1) Mission



● Site to Site VPN

1. Establish an VPN session

- Each of corp zone is match address.
- Internet zone is public network.

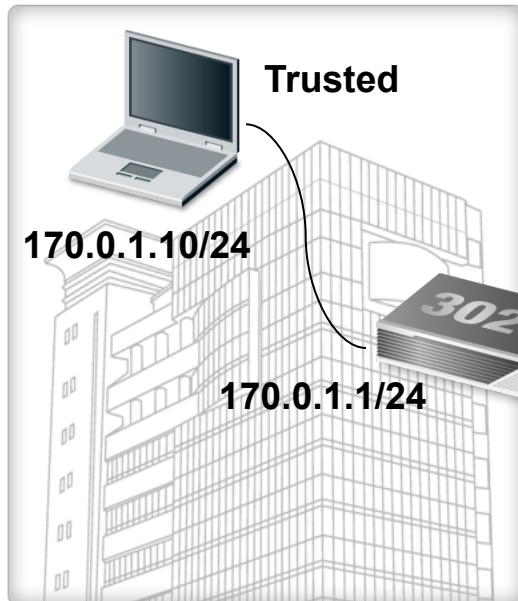


Advanced Configuration



● Site to site IPSec VPN

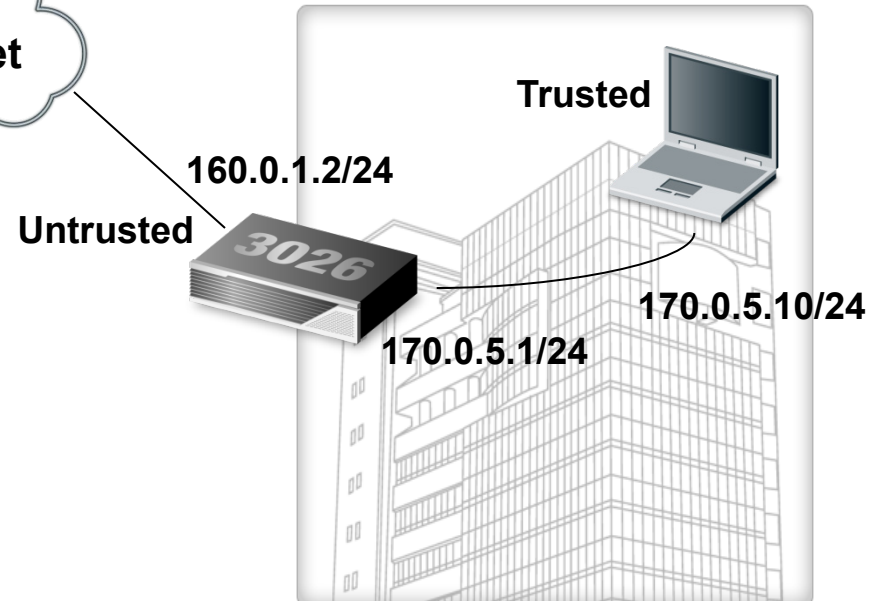
Branch



160.0.1.1/24

Internet

HQ



Exercise) #1, Site to Site IPSec VPN (ibg01)



● Configuring the IPSec manual policy and proposal

```
DUT-1/configure# crypto
DUT-1/configure/crypto# ipsec-manual policy pol1 160.0.1.2
DUT-1/configure/crypto/ipsec-manual/policy pol1 160.0.1.2# proposal
protocol esp
DUT-1/configure/crypto/ipsec-manual/policy pol1 160.0.1.2/proposal#
encryption-algorithm aes256-cbc out-cipher-key
0x0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef in-
cipher-key
0x0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef
DUT-1/configure/crypto/ipsec-manual/policy pol1 160.0.1.2/proposal# hash-
algorithm sha1-hmac out-authenticator-key
0x0123456789abcdef0123456789abcdef01234567 in-authenticator-key
0x0123456789abcdef0123456789abcdef01234567
DUT-1/configure/crypto/ipsec-manual/policy pol1 160.0.1.2/proposal# spi
10001 10002
DUT-1/configure/crypto/ipsec-manual/policy pol1 160.0.1.2/proposal# exit
DUT-1/configure/crypto/ipsec-manual/policy pol1 160.0.1.2# local-address
160.0.1.1
configure the proposals
DUT-1/configure/crypto/ipsec-manual/policy pol1 160.0.1.2# match address
170.0.1.0/24 170.0.5.0/24
proposal created and activated.
DUT-1/configure/crypto/ipsec-manual/policy pol1 160.0.1.2#
```

Exercise) #1, Site to Site IPSec VPN (ibg02)



● Configuring the IPSec manual policy and proposal

```
DUT-2/configure#
DUT-2/configure# crypto
DUT-2/configure/crypto# ipsec-manual policy pol1 160.0.1.1
DUT-2/configure/crypto/ipsec-manual/policy pol1 160.0.1.1# proposal
protocol esp
DUT-2/configure/crypto/ipsec-manual/policy pol1 160.0.1.1/proposal#
encryption-algorithm aes256-cbc out-cipher-key
0x0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef in-
cipher-key
0x0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef
DUT-2/configure/crypto/ipsec-manual/policy pol1 160.0.1.1/proposal# hash-
algorithm sha1-hmac out-authenticator-key
0x0123456789abcdef0123456789abcdef01234567 in-authenticator-key
0x0123456789abcdef0123456789abcdef01234567
DUT-2/configure/crypto/ipsec-manual/policy pol1 160.0.1.1/proposal# spi
10002 10001
DUT-2/configure/crypto/ipsec-manual/policy pol1 160.0.1.1/proposal# exit
DUT-2/configure/crypto/ipsec-manual/policy pol1 160.0.1.1# local-address
160.0.1.2
configure the proposals
DUT-2/configure/crypto/ipsec-manual/policy pol1 160.0.1.1# match address
170.0.5.0/24 170.0.1.0/24
proposal created and activated.
DUT-2/configure/crypto/ipsec-manual/policy pol1 160.0.1.1# end
```


Exercise) #2, IPsec configuration (ibg01)



- show the configured IPsec manual policy

```
DUT-1# show crypto ipsec-manual policy all
Policy      Peer      Match      Proto Transform
-----
pol1        160.0.1.2  S 170.0.1.0/28/any  Any  P1 esp-aes-sha1-tunl
              D 170.0.5.0/24/any
INpol1      160.0.1.1  S 170.0.5.0/24/any  Any  P1 esp-aes-sha1-tunl
              D 170.0.1.0/28/any
DUT-1#
```

Exercise) #2, IPsec configuration (ibg02)



● Show the configured IPsec manual policy

```
DUT-2# show crypto ipsec-manual policy all
```

Policy	Peer	Match	Proto	Transform
-----	----	-----	-----	-----
pol1	160.0.1.1	S 170.0.1.0/28/any D 170.0.5.0/24/any	Any	P1 esp-aes-sha1-tunl
INpol1	160.0.1.2	S 170.0.5.0/24/any D 170.0.1.0/28/any	Any	P1 esp-aes-sha1-tunl

Exercise) #3, Establish Session

- After the VPN connection success, IPSec SA and IKE SA are created.

```
DUT-1# show crypto ipsec sa all
```

Policy	Dest IP	Spi	Packets	Transform
-----	-----	---	-----	-----
INpol1	160.0.1.1	0x2712	4	esp-aes-sha1-tun1
pol1	160.0.1.2	0x2711	4	esp-aes-sha1-tun1

```
DUT-1#
```

```
DUT-2#
```

```
DUT-2# show crypto ipsec sa all
```

Policy	Dest IP	Spi	Packets	Transform
-----	-----	---	-----	-----
INpol1	160.0.1.2	0x2711	9	esp-aes-sha1-tun1
pol1	160.0.1.1	0x2712	9	esp-aes-sha1-tun1

```
DUT-2#
```

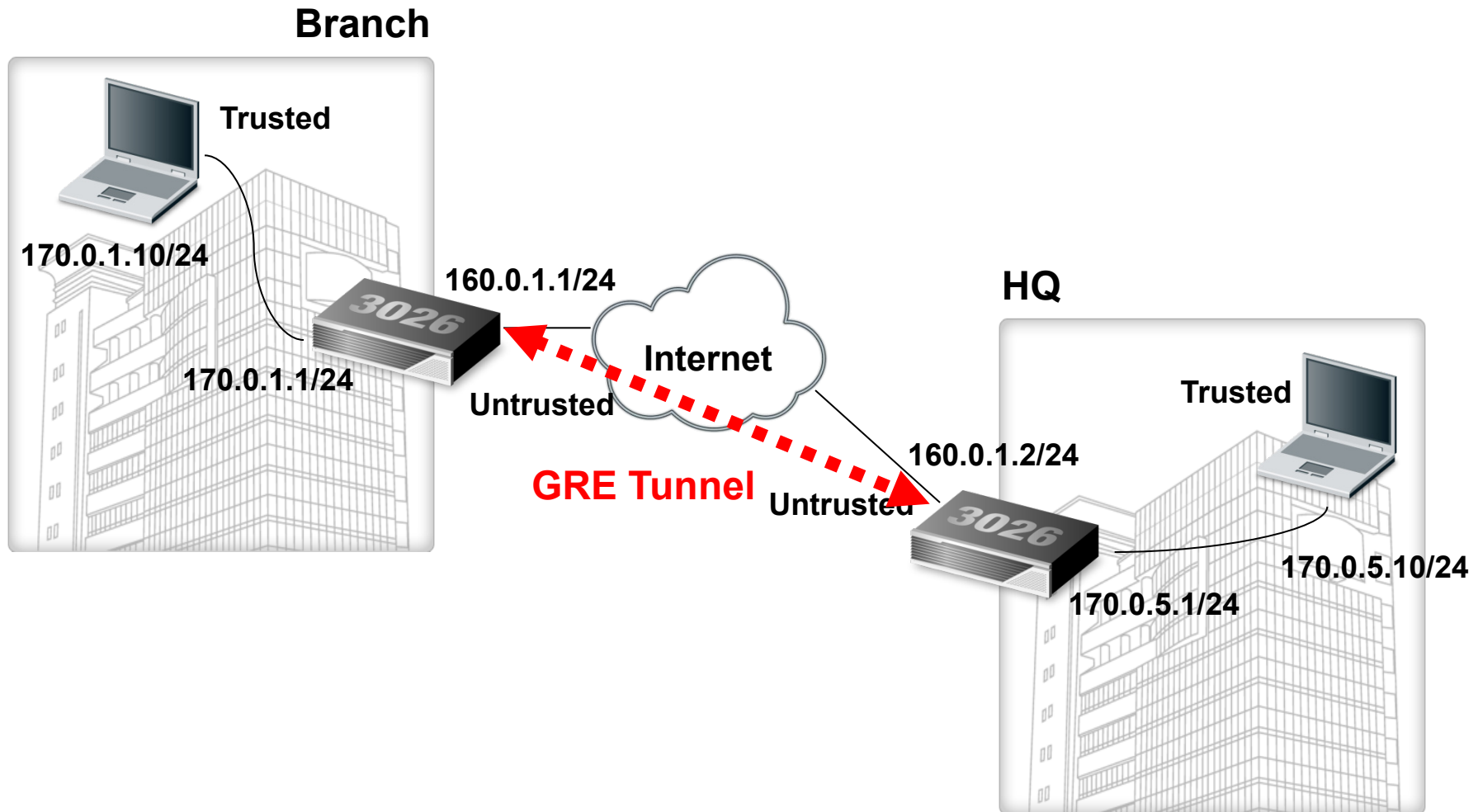


Advanced Configuration 2

IPSec Protection for GRE



● Site to site IPSec VPN



Exercise) #1, Site to Site IPSec VPN (ibg01)



● Configuring a network type for interface. (trusted/untrusted)

```
Ibg01/configure# interface ethernet 0/2
Ibg01/configure/interface/ethernet (0/2)#
Ibg01/configure/interface/ethernet (0/2)# ip address 160.0.1.1/24
Ibg01/configure/interface/ethernet (0/2)# end

Ibg01/configure# interface ethernet 2/0
Ibg01/configure/interface/ethernet (2/0)#
Ibg01/configure/interface/ethernet (2/0)# ip address 170.0.1.1/24
Ibg01/configure/interface/ethernet (2/0)# end
```

● Enabling firewall policy

- VPN & firewall function is tightly coupled.

```
Ibg01/configure# firewall internet
Ibg01/configure/firewall internet# interface ethernet0/2
Ibg01/configure/firewall internet# policy 1022 in self
ibg01/configure/firewall internet/policy 100 in# exit 2
ibg01/configure/firewall internet#
ibg01/configure# firewall corp
ibg01/configure/firewall corp# interface ethernet2/0
ibg01/configure/firewall corp# policy 1021 in
ibg01/configure/firewall corp/policy 1021 in# exit 3
ibg01/configure/firewall corp#
```

Exercise) #1, Site to Site IPSec VPN (ibg01)



- Show a network type of the interface

```
ibg01# show firewall interface all
```

Interface	Map Name
-----	-----
ethernet0/2	internet
ethernet2/0	corp

```
ibg01#
```


Exercise) #1, Site to Site IPSec VPN (ibg01)



- Configuring the GRE tunnel interface with IPSec protection enabled.

```
DUT-1/configure# interface tunnel tun1
configuring new tunnel interface
tun1=====>
DUT-1/configure/interface/tunnel tun1# ip address 24.24.24.1/24
DUT-1/configure/interface/tunnel tun1# tunnel source 150.0.1.1
DUT-1/configure/interface/tunnel tun1# tunnel destination 150.0.1.2
DUT-1/configure/interface/tunnel tun1# tunnel protection poll samsung123
DUT-1/configure/interface/tunnel tun1# tunnel mode gre
DUT-1/configure/interface/tunnel tun1# exit 2
```

Exercise) #1, Site to Site IPSec VPN (ibg01)



- show the configured GRE tunnel interface & IPSec policy derived from it.

```
DUT-1/configure# show interface tunnel tun1
Tunnel: tun1                                Status: up
Internet Address: 24.24.24.1                Internet Netmask: 255.255.255.0
Source Address: 150.0.1.1                  Destination Address: 150.0.1.2
MTU: 1476 bytes                            Protocol: GRE
ICMP unreachable: will be sent              ICMP redirect: will be sent
Crypto type: not set                       IPSEC/IKE: policy poll key ****
TTL: 30                                    Keepalive: disabled
TOS: not set                               Path MTU discovery: disabled
Key Value: not set                         Checksum: disabled
Sequence Datagrams: disabled

Tunnel Statistics:
  Bytes Rx      0      Bytes Tx      0
  Packets Rx    0      Packets Tx    0
  Err Packets Rx 0      Output Errs  0
```

Exercise) #1, Site to Site IPSec VPN (ibg02)



● Configuring a network type for interface. (trusted/untrusted)

```
Ibg01/configure# interface ethernet 0/2
Ibg01/configure/interface/ethernet (0/2)#
Ibg01/configure/interface/ethernet (0/2)# ip address 160.0.1.2/24
Ibg01/configure/interface/ethernet (0/2)# end

Ibg01/configure# interface ethernet 2/0
Ibg01/configure/interface/ethernet (2/0)#
Ibg01/configure/interface/ethernet (2/0)# ip address 170.0.5.1/24
Ibg01/configure/interface/ethernet (2/0)# end
```

● Enabling firewall policy

- VPN & firewall function is tightly coupled.

```
Ibg02/configure# firewall internet
Ibg02/configure/firewall internet# interface ethernet0/2
Ibg02/configure/firewall internet# policy 1022 in self
ibg02/configure/firewall internet/policy 100 in# exit 2
ibg02/configure/firewall internet#
ibg02/configure# firewall corp
ibg02/configure/firewall corp# interface ethernet2/0
ibg02/configure/firewall corp# policy 1021 in
ibg02/configure/firewall corp/policy 1021 in# exit 3
ibg02/configure/firewall corp#
```

Exercise) #1, Site to Site IPSec VPN (ibg02)



- Show a network type of the interface

```
ibg02# show firewall interface all
```

Interface	Map Name
-----	-----
ethernet0/2	internet
ethernet2/0	corp

```
ibg02#
```

Exercise) #1, Site to Site IPSec VPN (ibg02)



- Configuring the GRE tunnel interface with IPSec protection enabled.

```
DUT-2/configure# interface tunnel tun2
configuring new tunnel interface
tun2=====>
DUT-2/configure/interface/tunnel tun2# ip address 24.24.24.2/24
DUT-2/configure/interface/tunnel tun2# tunnel source 150.0.1.2
DUT-2/configure/interface/tunnel tun2# tunnel destination 150.0.1.1
DUT-2/configure/interface/tunnel tun2# tunnel protection poll samsung123
DUT-2/configure/interface/tunnel tun1# tunnel mode gre
DUT-2/configure/interface/tunnel tun2# exit
DUT-2/configure#
```

Exercise) #1, Site to Site IPSec VPN (ibg02)



- show the configured GRE tunnel interface & IPSec policy derived from it.

```
DUT-2/configure# show interface tunnel tun2
Tunnel: tun2                                Status: up
Internet Address: 24.24.24.2                Internet Netmask: 255.255.255.0
Source Address: 150.0.1.2                   Destination Address: 150.0.1.1
MTU: 1476 bytes                             Protocol: GRE
ICMP unreachable: will be sent              ICMP redirect: will be sent
Crypto type: not set                        IPSEC/IKE: policy poll key ****
TTL: 30                                     Keepalive: disabled
TOS: not set                               Path MTU discovery: disabled
Key Value: not set                         Checksum: disabled
Sequence Datagrams: disabled
Tunnel Statistics:
    Bytes Rx          0      Bytes Tx          0
    Packets Rx        0      Packets Tx          0
    Err Packets Rx    0      Output Errs      0
DUT-2/configure#
```

Exercise) #2, IKE configuration (ibg01)



● Configure crypto ike policy

peer ip address

```
Ibg01/configure# crypto
Ibg01/configure/crypto# ike policy pol1 160.0.1.2
Ibg01/configure/crypto/ike/policy pol1 160.0.1.2# local-address 160.0.1.1
Default proposal created with priority1-des-sha1-pre_shared-g1
Key String has to be configured by the user
```

● Configure crypto ike policy key

```
Ibg01/configure/crypto/ike/policy pol1 160.0.1.2# key samsung123
```

Exercise) #2, IKE configuration (ibg01)



● Show a ike information

```
ibg01/configure/crypto/ike/policy poll 160.0.1.2# show crypto ike policy
poll detail

Policy name poll, Local addr 160.0.1.1, Peer addr 160.0.1.2
Main mode, Initiator and Responder, PFS is not enabled, Shared Key is *****
Local ident 160.0.1.1 (ip-address), Remote Ident 160.0.1.2 (ip-address)
NGM attributes not configured
OCSP is not enabled

Proposal of priority 1
  Encryption algorithm: des
  Hash Algorithm: sha1
  Authentication Mode: pre-shared-key
  DH Group: group1
  Lifetime in seconds: 86400
  Lifetime in kilobytes: unlimited

ibg01/configure/crypto/ike/policy poll 160.0.1.2#
```


Exercise) #2, IKE configuration (ibg02)



● Configure crypto ike policy

peer ip address

```
ibg02/configure# crypto
ibg02/configure/crypto#
ibg02/configure/crypto# ike policy poll 160.0.1.1
ibg02/configure/crypto/ike/policy poll 160.0.1.1# local-address 160.0.1.2
Default proposal created with priority1-des-sha1-pre_shared-g1
Key String has to be configured by the user
```

● Configure crypto ike policy key

```
ibg02/configure/crypto/ike/policy poll 160.0.1.1# key samsung123
```

Exercise) #2, IKE configuration (ibg02)



● Show a ike information

```
ibg02/configure/crypto/ike/policy poll 160.0.1.1# show crypto ike policy
poll detail

Policy name poll, Local addr 160.0.1.2, Peer addr 160.0.1.1
Main mode, Initiator and Responder, PFS is not enabled, Shared Key is *****
Local ident 160.0.1.2 (ip-address), Remote Ident 160.0.1.1 (ip-address)
NGM attributes not configured
OCSP is not enabled

Proposal of priority 1
  Encryption algorithm: des
  Hash Algorithm: sha1
  Authentication Mode: pre-shared-key
  DH Group: group1
  Lifetime in seconds: 86400
  Lifetime in kilobytes: unlimited

ibg02/configure/crypto/ike/policy poll 160.0.1.1#
```

Exercise) #3, IPsec configuration (ibg01)



● Configure crypto ipsec policy

```
ibg01/configure# crypto
ibg01/configure/crypto# ipsec policy pol1 160.0.1.2
```

● Configure crypto ipsec policy match

```
ibg01/configure/crypto/ipsec/policy pol1 160.0.1.2# match address
170.0.1.0/24 170.0.5.0/24
Default proposal created with priority1-esp-3des-sha1-tunnel and activated.
```

● Configure crypto ipsec policy proposal

```
ibg01/configure/crypto/ipsec/policy pol1 160.0.1.2# proposal 1
```

Exercise) #3, IPsec configuration (ibg01)



● Show crypto ipsec policy

```
ibg01/configure/crypto/ipsec/policy poll 160.0.1.2# show crypto ipsec policy poll
```

Policy	Peer	Match	Proto	Transform
-----	----	-----	-----	-----
poll	160.0.1.2	S 170.0.1.0/24/any	Any	P1 esp-3des-sha1-tun1
		D 170.0.5.0/24/any		

Exercise) #3, IPsec configuration (ibg02)



● Configure crypto ipsec policy

```
ibg02/configure# crypto
ibg02/configure/crypto# ipsec policy pol1 160.0.1.1
```

● Configure crypto ipsec policy match

```
ibg02/configure/crypto/ipsec/policy pol1 160.0.1.1# match address
170.0.5.0/24 170.0.1.0/24
Default proposal created with priority1-esp-3des-sha1-tunnel and activated.
```

● Configure crypto ipsec policy proposal

```
ibg01/configure/crypto/ipsec/policy pol1 160.0.1.1# proposal 1
```

Exercise) #3, IPsec configuration (ibg02)



● Show crypto ipsec policy

```
ibg02/configure/crypto/ipsec/policy poll 160.0.1.1# show crypto ipsec policy poll
```

Policy	Peer	Match	Proto	Transform
-----	----	-----	-----	-----
poll	160.0.1.1	S 170.0.5.0/24/any	Any	P1 esp-3des-sha1-tun1
		D 170.0.1.0/24/any		

```
ibg02/configure/crypto/ipsec/policy poll 160.0.1.1#
```

Exercise) #4, Establish Session

- To establish an VPN session – Ping to the other match address

```
DUT-1# ping 170.0.5.1 sip 170.0.1.1
Pinging 170.0.5.1 (170.0.5.1); 64 bytes, timeout 5 seconds
.!!!!
Ping statistics for 170.0.5.1:
Packets: Transmitted 5, Received 4
Loss Rate 20%, approx. round-trip min/avg/max = 0/0/0 ms.
```

Exercise) #4, Establish Session

- After the VPN connection success, IPsec SA and IKE SA are created.

```
DUT-1# show crypto ipsec sa all
Policy      Dest IP      Spi      Packets      Transform
-----      -
INpol1      160.0.1.1    0xe47d8a2a  4            esp-aes-sha1-tunl
pol1        160.0.1.2    0xd8b99c50  4            esp-aes-sha1-tunl
DUT-1#
DUT-1# show crypto ike sa all
Policy      Peer      State      Bytes      Transform
-----      -
pol1        160.0.1.2  SA_MATURE  2040       pre-g1-des-sha1
DUT-1#
DUT-2#
DUT-2# show crypto ike sa all
Policy      Peer      State      Bytes      Transform
-----      -
pol1        160.0.1.1  SA_MATURE  2040       pre-g1-des-sha1
DUT-2#
DUT-2# show crypto ipsec sa all
Policy      Dest IP      Spi      Packets      Transform
-----      -
INpol1      160.0.1.2    0xd8b99c50  4            esp-aes-sha1-tunl
pol1        160.0.1.1    0xe47d8a2a  4            esp-aes-sha1-tunl
DUT-2#
```


Exercise) #5, Route via GRE tunnel



- Configure the route for the source to reach destination via GRE

```
DUT-1/configure# ip route 170.0.5.0/24 tun1
DUT-1/configure#
DUT-1/configure# show ip route 170.0.5.0
Routing entry for 170.0.5.0/24
  Known via "static", distance 1, metric 0, best
    * directly connected, tun1

DUT-2/configure# ip route 170.0.1.0/24 tun2
DUT-2/configure# end
DUT-2# show ip route 170.0.1.0
Routing entry for 170.0.1.0/24
  Known via "static", distance 1, metric 0, best
    * directly connected, tun2
```

Exercise) #5, Route via GRE tunnel



● Make the VPN connection

```
DUT-1# ping 170.0.5.1 sip 170.0.1.1
Pinging 170.0.5.1 (170.0.5.1); 64 bytes, timeout 5 seconds
!!!!
Ping statistics for 170.0.5.1:
Packets: Transmitted 5, Received 5
Loss Rate 0%, approx. round-trip min/avg/max = 0/0/0 ms.
DUT-1#
DUT-1#
DUT-1#
DUT-1# show crypto ipsec sa all
```

Policy	Dest IP	Spi	Packets	Transform
-----	-----	---	-----	-----
INpol1	150.0.1.1	0xde9fad2	14	esp-3des-sha1-tran
pol1	150.0.1.2	0x90fc1067	14	esp-3des-sha1-tran

```
DUT-1#
DUT-1#
```

Exercise) #5, Route via GRE tunnel



● Make the VPN connection

```
DUT-2#
DUT-2# ping 170.0.1.1 sip 170.0.5.1
Pinging 170.0.1.1 (170.0.1.1); 64 bytes, timeout 5 seconds
!!!!
Ping statistics for 170.0.1.1:
Packets: Transmitted 5, Received 5
Loss Rate 0%, approx. round-trip min/avg/max = 0/0/0 ms.
DUT-2#

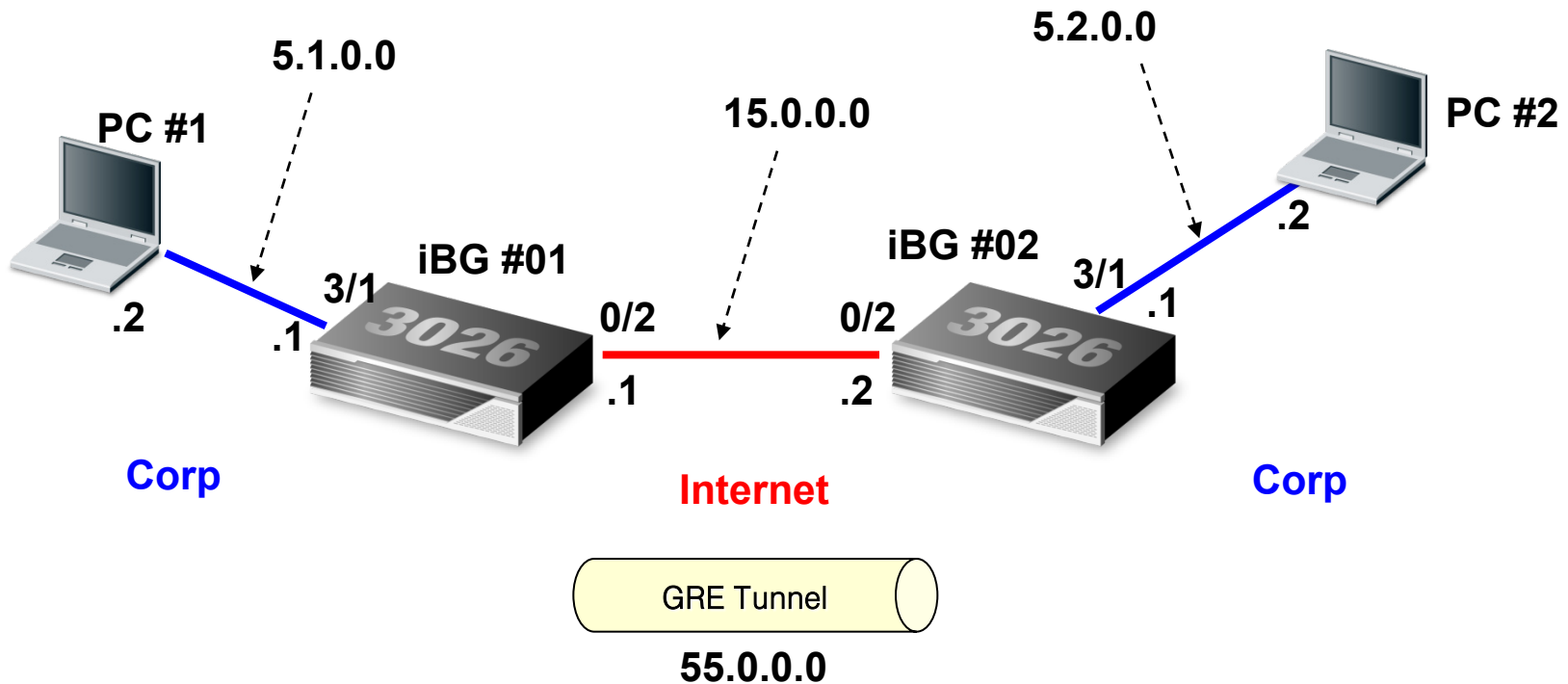
DUT-2# show crypto ipsec sa all
Policy      Dest IP      Spi          Packets      Transform
-----
INpol1      150.0.1.2    0x90fc1067   19           esp-3des-sha1-tran
pol1        150.0.1.1    0xdea9fad2   19           esp-3des-sha1-tran
DUT-2#

DUT-1# show crypto ipsec sa all
Policy      Dest IP      Spi          Packets      Transform
-----
INpol1      150.0.1.1    0xdea9fad2   19           esp-3des-sha1-tran
pol1        150.0.1.2    0x90fc1067   19           esp-3des-sha1-tran
DUT-1#
```

Practice 2) Network Topology



● Configuration



Practice 2) Mission



● GRE over Site to Site VPN

1. Establish an GRE over VPN session

- Each of corp zone is match address.
- Internet zone is public network.



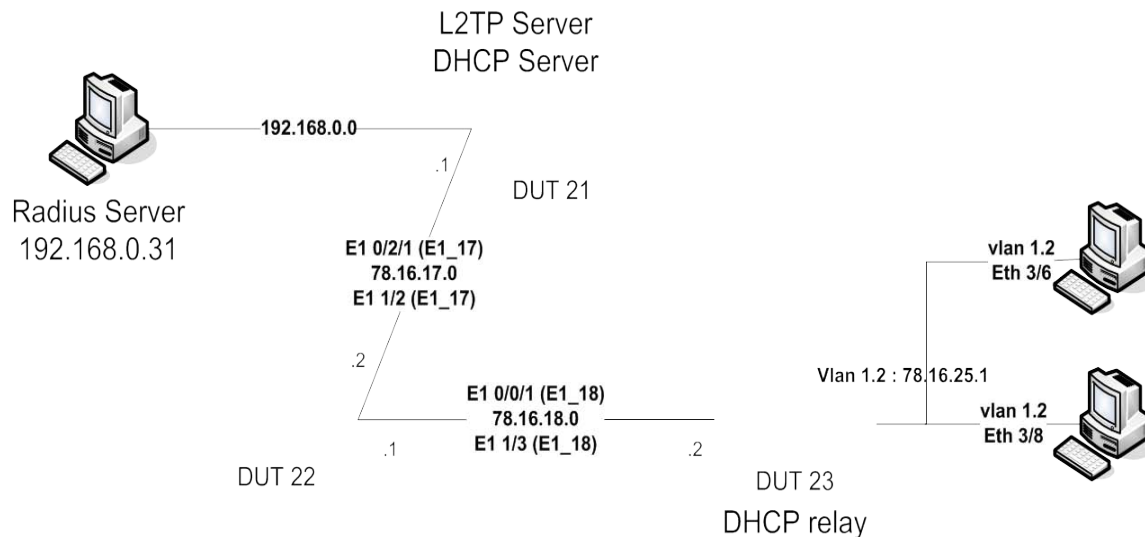
Advanced Configuration 3



● L2TP IPsec VPN

Objective

Verify the functionality of L2TP/IPsec session establishment with Local user MS-CHAP authentication method and Local IP-Pool on PPP wan bundle on the DUT



Exercise) #1, L2TP Server Configuration



● L2TP Server Configuration

```
DUT/configure# interface l2tp-server l2tp1
DUT/configure/interface/l2tp-server l2tp1# ip address 10.1.1.1
DUT/configure/interface/l2tp-server l2tp1# remote-user username1 password1
DUT/configure/interface/l2tp-server l2tp1# remote-user username2 password2
DUT/configure/interface/l2tp-server l2tp1# remote-config samsung.com
DUT/configure/interface/l2tp-server l2tp1/remote-config# address-pool
10.1.1.2 10.1.1.3
DUT/configure/interface/l2tp-server l2tp1/remote-config# dns 40.10.10.20
DUT/configure/interface/l2tp-server l2tp1/remote-config# nbns 40.10.10.20
DUT/configure/interface/l2tp-server l2tp1/remote-config# exit
DUT/configure/interface/l2tp-server l2tp1# ipsec-protection ltpipsec
78.16.17.1 key samsung123456
DUT/configure/interface/l2tp-server l2tp1# exit
```

- Establish L2TP session from LAC1 Windows XP Client to DUT with username1@samsung.com and password1 and with MS-CHAP authentication method.

Thank you!

