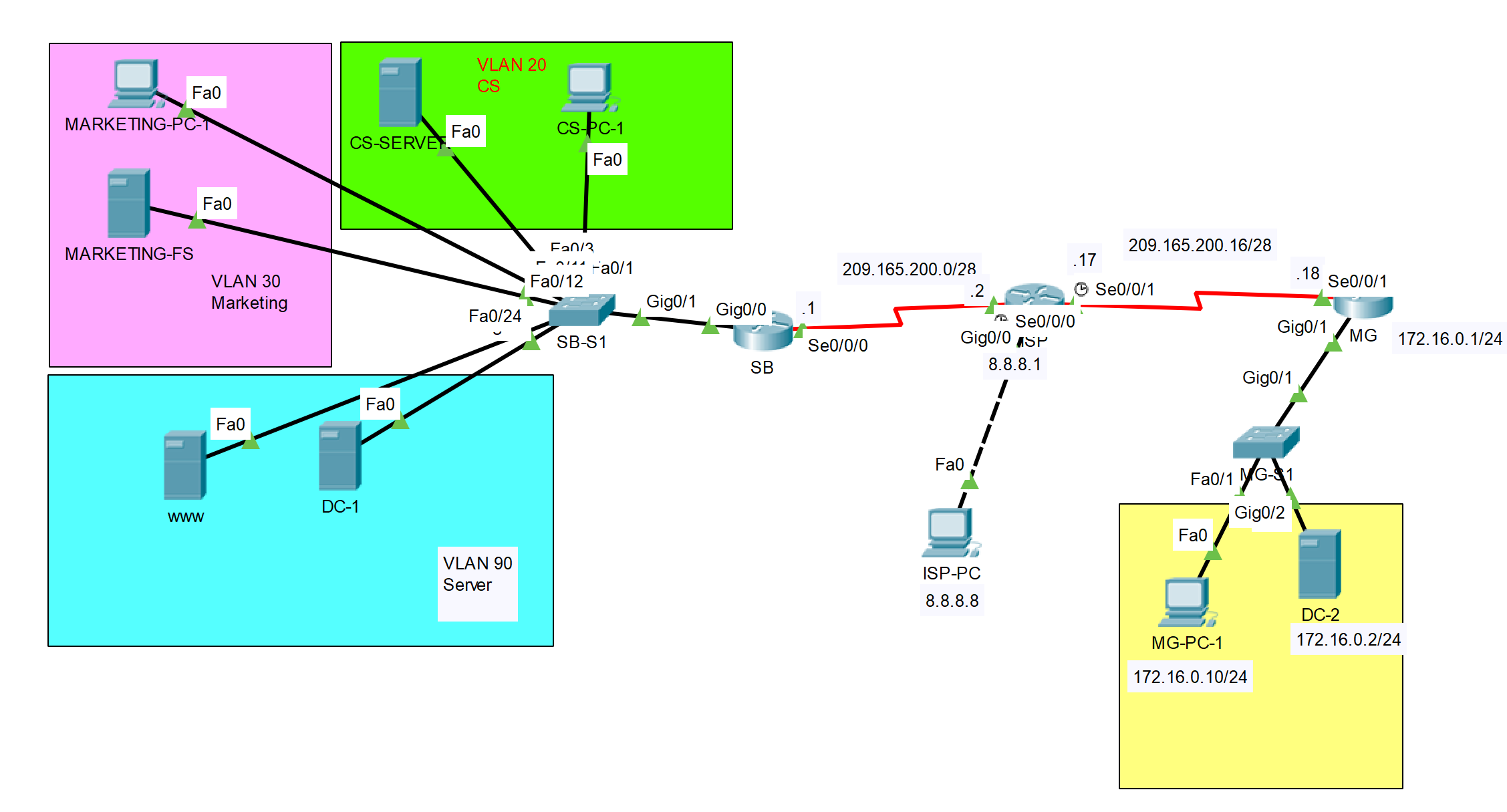
# Lab 5 VPN IPSec Over GRE Tunnel Instructions



|  |  |  |  |
| --- | --- | --- | --- |
| Device | Interface | IP Address/Prefix | Default Gateway |
| SB Router | S0/0/0 | 209.165.200.1/28 |  |
|  | Tunnel 0 | 172.16.12.1/30 |  |
| ISP | S0/0/0 | 209.165.200.2/28 |  |
|  | S0/0/1 | 209.165.200.17/28 |  |
|  | G0/0 | 8.8.8.1/8 |  |
| MG Router | S0/0/1 | 209.165.200.18/28 |  |
|  | Tunnel 0 | 172.16.12.1/30 |  |
|  | G0/1 | 172.16.0.1/24 |  |
| ISP-PC | Fastether port | 8.8.8.8/8 |  |
| MG-PC-1 | Fastether port | 172.16.0.10/24 | 172.16.0.1/24 |
| DC-2 | Fastether port | 172.16.0.2/24 | 172.16.0.1/24 |

In this lab, IPSec is going to be configured over the GRE tunnel on the router SB and MG. SB is symbolizing the head office of Mavis company in South Bank. MG is symbolizing the branch office of Mavis company in Mt Gravatt. When the lab is finished, any end devices from the SB Router’s LAN side should be able to ping any devices on the MG Router’s LAN side. Traffic flowing through the GRE tunnel should be encrypted by IPSec.

## Part 1: Setup the network environment as in Lab 4

**Step 1**. Cable the network as the topology above.

**Note**: In each subnet, the PC and the Server can be running as VMs on a same physical host.

**Step 2**. Import the backup running-config files from Lab 4 to the network devices.

**Step 3**. Import the backup vlan.dat from Lab 4 into SB-S1.

**Step 4**. Configure the end devices IP address as in Lab 4.

**Step 5**. Verify the network connection.

* Trace route from CS-PC-1 to MG-PC-1 and notice the path is via the Tunnel Interface on the MG Router:

192.168.1.1 > 172.16.12.2 > 172.16.0.10

* Display the routing table by issuing the **show ip route** command on router SB and the router MG.
  + On router SB, the routes to the LANs on MG site should be via 172.16.12.2.
  + On router MG, the routes to the LANs on SB site should be via 172.16.12.1.

## Part 2: Configure a Site-To-Site IPSec VPN to protect GRE Tunnel Traffic

The diagram below shows the ISAKMP Policy and IPSec Policy are to be used in this lab.

**Step 1**. Configure ISAKMP policy on both SB and MG:

**Step 2**. Configure ISAKMP pre-shared key as “**cisco123**” and specify the peer on both SB and MG:

**Step 3**. Configure the IPSec transform set 50 on both SB and MG and make sure the transform-set mode is tunnel. Use esp-aes 256 as encryption and esp-sha-hmac as hash algorisim:

**Step 4**. Configure a crypto IPSec profile. Name it as CProfile and associate the transform set 50 to this profile on both router SB and MG:

**Step 5**. Apply the crypto IPSec profile to the tunnel interface on both router SB and MG:

**Note**: The IPSec profile’s name must be consistent with the name defined in step 4 (case sensitive).

**Note**: The **tunnel protection ipsec profile** command states that any traffic that traverses the tunnel should be encrypted with the IPSec profile called **CProfile**.

**Step 6**. Configure the tunnel protocol to be IPSec on the tunnel interface on both router SB and MG:

**Note**: After implementing the previous solution, every packet going through the tunnel has duplicate IP addresses in the header. One is encapsulated by the GRE protocol whereas the other is encapsulated by the IPSec protocol. You need to remove the extra GRE overhead by applying IPSec protocol on the GRE tunnel interface.

**Step 7**. Verify the configuration:

* From any end devices on router SB’s LAN, trace route to the MG-PC-1 or DC-2 should be successful via the Tunnel Interface IP on router MG 172.16.12.2;
* Use the command **show crypto isakmp sa** to verify the peers between 209.165.200.1 and 209.165.200.18.
* Use the command **show crypto ipsec sa** to verify the number of packets encrypted by IPSec when traversing through the GRE tunnel.
* Use the command **show interface tunnel 0** to verify the tunnel protocol is using IPSEC/IP instead of GRE.

## Part 3: Demonstration, Mark off, and Backup Network Configuration

1. Demonstrate the following to your instructor and ask for mark off:

* From any end devices on router SB’s LAN, trace route to the MG-PC-1 or DC-2 should be successful via the Tunnel Interface IP on router MG 172.16.12.2;
* Use the command **show crypto isakmp sa** to verify the peers between 209.165.200.1 and 209.165.200.18. Take a screenshot and pasted it to AT4 Part 2 template.
* Use the command **show crypto ipsec sa** to verify the number of packets encrypted by IPSec when traversing through the GRE tunnel. Take a screenshot and pasted it to AT4 Part 2 template.
* Use the command **show interface tunnel 0** to verify the tunnel protocol is using IPSEC/IP instead of GRE. . Take a screenshot and pasted it to AT4 Part 2 template.

1. Backup the running-config on the router SB.

* Backup the router SB’s running-config in plain text files for the future practical labs.
* Backup the ISP’s running-config in plain text files for the future practical labs.
* Backup the router MG’s running-config in plain text files for the future practical labs.
* Backup the SB-S1’s running-config and SB-S1’s VLAN.dat into plain text files for the future practical labs.