Project Report
Topic 4: Hybrid Cloud & Remote Management (WAN & Ops)

Group 4: Srun Nai Eang, Noch Munny Ratanak, Nut Sophaphirum

1. Project Objective

1.1. The Problem

Modern enterprises require secure communication between a Branch office and a Data Center. Transmitting sensitive data over the public internet without encryption exposes the company to “Man-in-the-Middle” attacks and data breaches. Additionally, administrators at the Data Center need a real-time alert into the health of remote hardware to minimize downtime.

1.2. The Solution

We implemented a **Site-to-Site IPsec VPN** using Cisco ISR 2911 routers. This solution provides:

- **Confidentiality:** AES Encryption ensures data are encrypted and cannot be read by outsiders.
- **Integrity:** SHA Hashing ensures data is not tampered with in transit.
- **Centralized Monitoring:** SNMP and Syslog protocols allow the Data Center Server to track router status and receive instant alerts.
- **Split Tunneling:** Optimizes bandwidth by only encrypting traffic destined for the corporate network.

2. IP Addressing SchemeSecurity Implementation

Device	Interface	IP Address	Subnet Mask	Default Gate way
Office PC	NIC	192.168.10.10	255.255.255.0	192.168.10.1
Office Router	Gig0/0 (LAN)	192.168.10.1	255.255.255.0	N/A
Officer Router	Gig0/1 (WAN)	203.0.113.1	255.255.255.252	203.0.113.2
Internet Router	Gig0/0	203.0.113.2	255.255.255.252	N/A
Internet Router	Gig0/1	198.51.100.1	255.255.255.252	N/A
DC Router	Gig0/0 (WAN)	198.51.100.2	255.255.255.252	198.51.100.1
DC Router	Gig0/1 (LAN)	10.10.10.1	255.255.255.0	N/A
DC Server	NIC	10.10.10.10	255.255.255.0	10.10.10.1

3. Configuration Snippets (Key Highlights)

3.1. IPsec VPN Phase 1 (ISAKMP)

This establishes the secure handshake between the two sites.

```
crypto isakmp policy 10
 encryption aes
 hash sha
 authentication pre-share
 group 2
crypto isakmp key vpn123 address 198.51.100.2
```

3.2. IPsec VPN Phase 2 & Crypto Map

This defines the actual encryption and applies it to the outgoing WAN interface.

```
crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
!
crypto map MYMAP 10 ipsec-isakmp
 set peer 198.51.100.2
 set transform-set MYSET
 match address 100
!
interface GigabitEthernet0/1
 crypto map MYMAP
```

3.3. Management & Monitoring (SNMP & Syslog)

Enabling the router to talk to the Data Center Management Server.

```
snmp-server community public RO
logging 10.10.10.10
logging source-interface g0/0
```

4. Verification & Testing

4.1. VPN Tunnel Verification

The command show crypto isakmp was used to verify the tunnel status. The output showed QM_IDLE, confirming the tunnel is active and encrypted.

```
Office-Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
198.51.100.2    203.0.113.1     QM_IDLE           1061    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

4.2. Split Tunneling Test

- **Result:** A ping from Office PC to 10.10.10.10 increased the #pkts encaps counter on the router.
- **Result:** A ping to the public 203.0.113.2 did not increase the counter, proving that non-corporate traffic bypasses the VPN.

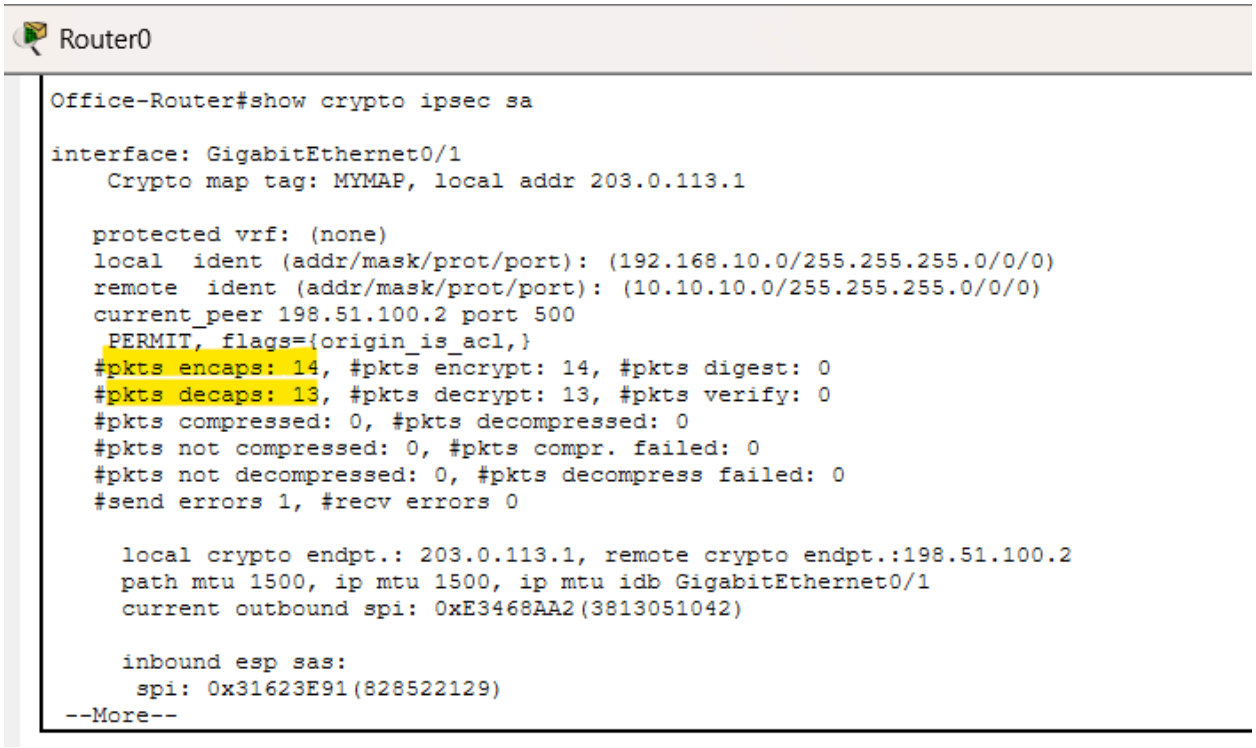
4.3. Syslog Failure Test

When the Office Router's LAN interface was manually shut down, the Data Center Server immediately logged the event:
%LINK-5-CHANGED: Interface GigabitEthernt0/0, changed state to administratively down
This confirms that the management system is functioning correctly over the secure tunnel.

5. Simulation File (.pkt) Setup

Note to instructor:

- All router and switch passwords have been set to cisco.
- The enable secret password is set to class.
- To trigger the VPN, please initiate a ping from the **Office PC** to the **Data Center Server (10.10.10.10).**



```
 PERMIT, flags={origin_is_acl,}
#pkts encaps: 18, #pkts encrypt: 18, #pkts digest: 0
#pkts decaps: 17, #pkts decrypt: 17, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
```