DESIGN AND IMPLEMENTATION OF SECURE VPNs FOR REMOTE WORKPLACES

A Case Study

Submitted by

YAFFIN S [RA2211032010053]

MITUN M [RA2211032010090]

Under the Guidance of

Dr. K. KALAISELVI

Assistant Professor, Department of Networking and Communications

In partial fulfilment of the requirements for the degree of

BACHELOR OF TECHNOLOGY in

COMPUTER SCIENCE AND ENGINEERING

with a specialization in Internet of Things

DEPARTMENT OF NETWORKING AND COMMUNICATIONS

COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR – 603 203

NOVEMBER 2024

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR – 603 203

BONAFIDE CERTIFICATE

Certified that Computer Network A Case Study Report titled “**DESIGN AND IMPLEMENTATION OF SECURE VPNs FOR REMOTE WORKPLACES**” is the bonafide work of “**YAFFIN S” [RA2211032010053],** “**MITUN M” [RA221032010090],** who carried out the case study under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other work

SIGNATURE	**SIGNATURE**
Dr .K. KALAISELVI Associate Professor Department of Networking and Communications	Dr. M. LAKSHMI Head of the Department Department of Networking
Date: 09/11/2024	**Date: 09/11/2024**

ABSTRACT

The rapid adoption of remote work has heightened the need for secure and efficient communication channels, making Virtual Private Networks (VPNs) a critical component of modern enterprise infrastructure. This project focuses on the design and implementation of secure VPN solutions tailored specifically for remote workforces. Traditional VPNs often present challenges in terms of scalability, performance, and vulnerability to cyber threats, especially as remote access demands increase. To address these issues, this project explores an innovative VPN architecture that combines robust encryption, multi-factor authentication, and traffic segmentation to enhance security and usability for remote employees.

The proposed VPN solution integrates advanced cryptographic protocols and a zero-trust model to ensure secure access to organizational resources while minimizing risks from unauthorized access and data breaches. Additionally, the solution is optimized for bandwidth efficiency and low-latency communication to support high-performance applications. Implementation details include a comprehensive analysis of VPN protocols (such as OpenVPN, IPsec, and WireGuard), deployment in virtualized cloud environments, and real-time monitoring tools to maintain optimal security postures. This project aims to contribute to the field by offering a scalable, secure, and efficient VPN model that meets the demands of a dispersed workforce in today's digital landscape.

Table of Contents

TABLE OF FIGURES

1. Introduction :

With the increasing shift towards remote work, organizations are facing new challenges in securing their networks and ensuring reliable access to critical resources. Virtual Private Networks (VPNs) have become a fundamental solution to address these challenges, enabling secure and encrypted connections over public networks for remote employees. This project focuses on designing and implementing a secure VPN infrastructure to support a remote workforce, ensuring that employees can securely connect to organizational resources from any location.

The need for VPNs has grown significantly due to the following factors:

Data Security: As remote workforces access sensitive data, there’s a higher risk of interception and unauthorized access over public networks. A VPN ensures that all data transmitted between remote users and corporate servers is encrypted, reducing the risk of data breaches and unauthorized access.

Access Control: Organizations must control who can access which resources, even from remote locations. VPNs help enforce secure access policies by requiring user authentication and implementing role-based access controls.

Regulatory Compliance: Many industries, such as finance and healthcare, have strict compliance standards that require organizations to protect data confidentiality and integrity. Implementing a secure VPN helps organizations adhere to these regulations, mitigating legal and financial risks.

Network Performance: In addition to security, VPNs also contribute to network efficiency by optimizing routing and allowing bandwidth prioritization, which can improve the experience for remote users, particularly when accessing high-performance applications.

1.1 Project Objectives

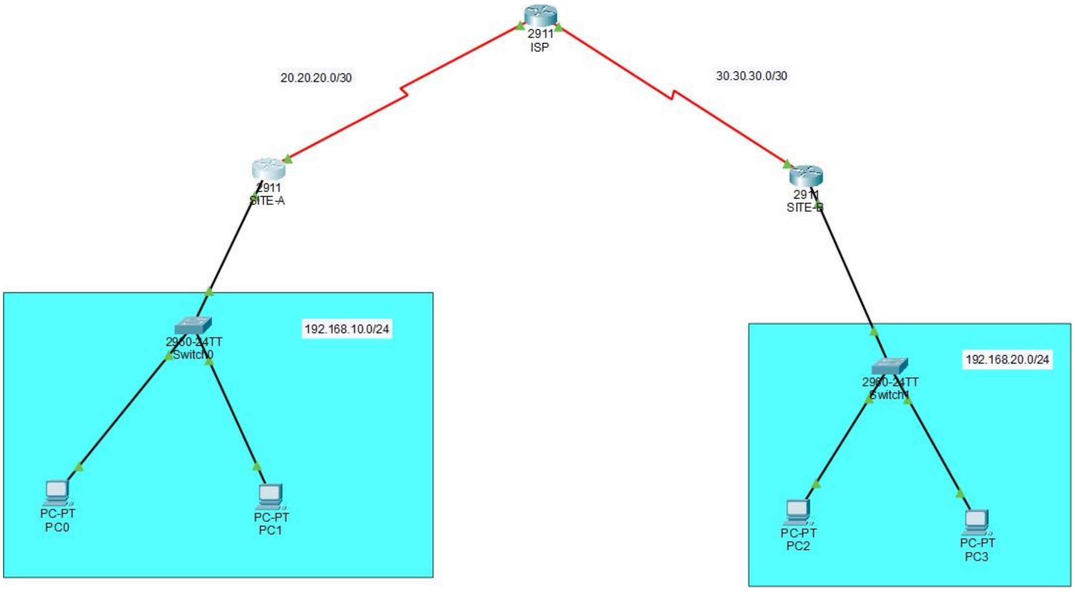
The primary objectives of this project are as follows:

To Design a Secure VPN Architecture: This project will create a VPN architecture that combines industry-standard security measures, including strong encryption protocols, multi-factor authentication, and secure key management.

To Implement and Test the VPN Solution: The VPN solution will be implemented using IPsec, an established protocol that supports secure communication by authenticating and encrypting each IP packet. Testing will include connectivity, security validation, and performance benchmarking.

To Optimize for Scalability and Performance: The VPN must support an expanding number of remote users without compromising speed or security. Therefore, the project will involve the design of a scalable infrastructure capable of handling increased network traffic.

2. Network Design :



The network design for implementing a secure VPN involves constructing a topology that supports encrypted communication across multiple locations, incorporating routers, switches, and endpoint devices. This section outlines the design and configuration steps necessary to set up the VPN infrastructure for a secure remote workforce, based on configurations specified in the provided document.

2.1 Constructing the Network Topology :

The network topology connects two primary sites, Site A and Site B, with a central Internet Service Provider (ISP) acting as the intermediary. This setup enables secure VPN communication between the sites, allowing remote users to access resources across both locations. Key components of the topology include:

Routers: Each site is equipped with a router (Router0 for Site A and Router1 for Site B) configured to enable IPsec VPN communication. A central ISP router (Router2) provides internet connectivity, acting as a bridge between the two sites.

PCs: Each site has PCs connected to the routers, configured to simulate end-user devices that access the network through the VPN.

VPN Configuration: IPsec VPN is established between the two routers to secure data in transit between Site A and Site B. This configuration includes both encryption and authentication protocols.

The topology design aims to maintain secure connectivity while allowing for future scalability as additional sites or devices may be integrated.

2.2 IP Address Configuration for Routers and PCs

Configuring the IP addresses for each network device is crucial to establishing communication across the network. Below are the specific IP configurations assigned to each device at Site A, Site B, and the ISP:

CONFIGURING IPSEC VPN WAN

1) Constuct the network topology
2) Configure the ip addresses to the routers interfaces and the PCs.
3) Configure OSPF and test connection
4) Configure IPSEC VPN.
   - enable security technology package.
   - Configure extened ACL permitting the target on each router
   - Configure the IKE phase 1 ISAKMP policy on each router
   - Configure the IKE phase 2 ISAKMP policy on each router
   - Configure the Crypto map on the outgoing interface.

Device	Interface	IP address	Subnet mask	Gateway
PC1	Fa0/0	192.168.10.10	255.255.255.0	192.168.10.1
PC2	Fa0/0	192.168.10.20	255.255.255.0	192.168.10.1
PC3	Fa0/0	192.168.20.10	255.255.255.0	192.168.20.1
PC4	Fa0/0	192.168.20.20	255.255.255.0	192.168.20.1
Router0(SITE A)	Gig0/0	192.168.10.1	255.255.255.0	-
Router1(SITE B)	Gig0/0	192.168.20.1	255.255.255.0	-
Router0(SITE A)	Se0/3/0	20.20.20.2	255.255.255.252	-
Router1(SITE B)	Se0/3/0	30.30.30.2	255.255.255.252	-
Router2(ISP)	Se0/3/0	20.20.20.1	255.255.255.252	-
Router2(ISP)	Se0/3/1	30.30.30.1	255.255.255.252	-

This configuration enables the following:

Local Communication: PCs at each site can communicate within their respective networks.

Remote Communication: Routers at each site use IPsec VPN to encrypt and route data across the internet via the ISP.

2.3 Configuring Routing Protocol (OSPF)

The Open Shortest Path First (OSPF) protocol is configured on each router to enable dynamic routing. OSPF ensures that each router has knowledge of the entire network topology, enabling efficient routing across the VPN connection. Configuration steps include:

Enable OSPF: OSPF is enabled on both Site A and Site B routers to facilitate communication between devices at both locations.

Assign Network Statements: Each router is configured to recognize the networks it directly connects to and exchanges this information with other routers.

Verify Connectivity: After configuring OSPF, ping tests are conducted to ensure proper connectivity between sites.

2.4 Configuring IPsec VPN

The IPsec VPN configuration process establishes a secure, encrypted tunnel between Site A and Site B. Key configuration steps include:

Enable Security Technology Package: The security technology package must be activated to support IPsec functionality on the routers. This step ensures that advanced encryption and authentication protocols are available.

SHELL:

```
Router(config)#license boot module c2900 technology-package securityk9
```

Extended Access Control Lists (ACLs): Extended ACLs are configured to define the permitted traffic between Site A and Site B. These ACLs specify which IP addresses and protocols are allowed to communicate across the VPN.

```
access-list 130 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
```

ISAKMP Policies: Internet Security Association and Key Management Protocol (ISAKMP) policies are set up to establish the IPsec VPN connection in two phases:

IKE Phase 1: Configures encryption, authentication, and Diffie-Hellman group for initial negotiation.

IKE Phase 2: Sets up the secure channel for encrypted data transmission.

SHELL:

```
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config)#crypto isakmp key tech61 address 20.20.20.2
```

Crypto Map Configuration: A crypto map is applied to the outgoing interfaces on both routers. This crypto map links the ACLs and ISAKMP policies, enforcing VPN encryption on specified traffic.

```
Router(config-if)#crypto map VPN-MAP
```

2.5 Testing the Network Design

After configuring the IP addresses, OSPF routing, and IPsec VPN, the network is tested to confirm successful configuration. Testing involves:

Ping Tests: To verify connectivity between devices at both sites through the VPN.

OSPF Verification: Running commands such as show ip ospf neighbor to confirm that OSPF has established neighbor relationships and the network is stable.

VPN Status Checks: Using commands like show crypto ipsec sa to monitor active IPsec sessions and verify the encryption and decryption of data.

3. Routing Configuration

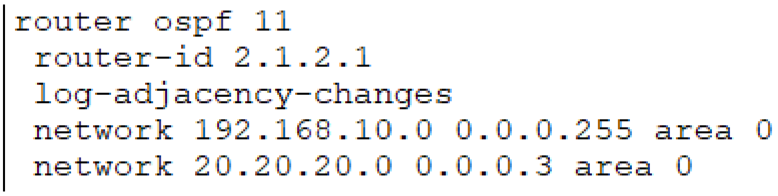
3.1 Router Configuration

In this section, we will detail the routing configuration steps necessary to enable efficient, secure data transmission across the VPN network for remote access. This project uses the Open Shortest Path First (OSPF) routing protocol to dynamically route traffic between Site A and Site B through an IPsec VPN. OSPF is selected for its scalability and efficiency in quickly adapting to network changes, which is critical for a dynamic environment with remote workforce demands.

3.1 Introduction to OSPF

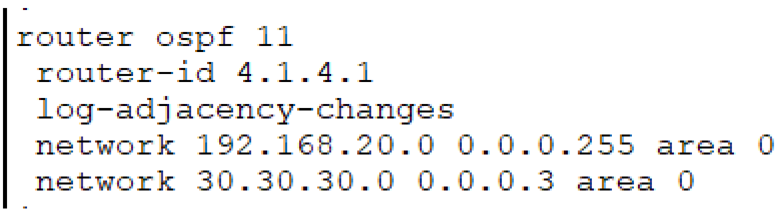
Open Shortest Path First (OSPF) is a link-state routing protocol used for efficiently sharing routing information between routers within the same Autonomous System (AS). OSPF maintains a routing table by constructing a link-state database based on each router's view of the network topology. This allows for automatic rerouting in case of network failures, providing robust connectivity for the VPN infrastructure.

On site A:



```
router ospf 11
 router-id 2.1.2.1
 log-adjacency-changes
 network 192.168.10.0 0.0.0.255 area 0
 network 20.20.20.0 0.0.0.3 area 0
```

On site B:



```
router ospf 11
 router-id 4.1.4.1
 log-adjacency-changes
 network 192.168.20.0 0.0.0.255 area 0
 network 30.30.30.0 0.0.0.3 area 0
```

3.2 Configuring OSPF on Routers

The configuration of OSPF is performed on both routers at Site A and Site B to enable them to exchange routing information and support efficient packet transmission over the VPN.

Steps for Configuring OSPF

Enabling OSPF on Each Router

Begin by enabling OSPF on each router in the network. We assign an OSPF process ID (a locally significant identifier for the OSPF process) and define the specific networks that each router will advertise to its neighbors.

Example configuration for Router0 (Site A):

Shell:

```
Router(config)#router ospf 1
```

Assigning Network Statements

Network statements identify which interfaces will participate in OSPF and specify the area to which each network belongs. In this configuration, Area 0 (the OSPF backbone area) is used, which is standard practice to maintain routing efficiency and stability.

Router0 (Site A):

Shell:

```
Router(config-router)#network 192.168.10.0 0.0.0.255 area 0

Router(config-router)#network 20.20.20.0 0.0.0.3 area 0
```

Router1 (Site B):

Shell:

```
Router(config-router)#network 192.168.20.0 0.0.0.255 area 0

Router(config-router)#network 30.30.30.0 0.0.0.3 area 0
```

Each network statement identifies a specific range of IP addresses (indicated by the wildcard mask, which is an inverse subnet mask) and associates these addresses with OSPF Area 0. This ensures that all interfaces within these IP ranges participate in OSPF and share routing information with other routers in the area.

Setting Router IDs

Setting a unique Router ID for each OSPF router helps in uniquely identifying routers within the network. Although optional, this step can improve network management and troubleshooting by making each router's OSPF identifier explicit.

Router0 (Site A):

Shell :

```
Router(config-router)#router-id 1.1.1.1
```

Router1 (Site B):

Shell :

```
Router(config-router)#router-id 2.2.2.2
```

3.3 Verifying OSPF Neighbor Relationships

After configuring OSPF on both routers, it is essential to verify that they have established a neighbor relationship. The OSPF neighbor adjacency process ensures that routers within the same area recognize each other and can exchange route information.Using the show ip ospf neighbor Command This command allows administrators to confirm that each router has discovered and established an adjacency with its OSPF neighbors.

Example output on Router0 (Site A):

Shell :

```
Router#show ip ospf neighbor

Neighbor ID     Pri   State          Dead Time   Address         Interface

2.2.2.2           1    FULL/DR        00:00:38    20.20.20.1      Serial0/3/0
```

In this output:

Neighbor ID: The Router ID of the adjacent router (Router1 in this case).

State: Indicates that the OSPF relationship is in the "FULL" state, meaning a complete adjacency has been established.

Dead Time: The remaining time before OSPF considers the neighbor down if no hello packets are received.

Address: The IP address of the neighboring router.

Interface: The interface through which the adjacency was established.

OSPF Database Verification

To further verify the OSPF configuration, we can use the show ip ospf database command. This command provides a comprehensive view of the OSPF link-state database, confirming that each router has an accurate topology view of the network.

3.4 Adjusting OSPF Timers (Optional)

OSPF hello and dead timers dictate how frequently routers communicate to maintain adjacencies. The default timers are often sufficient, but they may be adjusted in high-performance networks to ensure faster reconvergence times in case of a failure.

Example of adjusting timers on an interface:

shell

```
Router(config-if)#ip ospf hello-interval 10Router(config-if)#ip ospf dead-interval 40
```

In this configuration:

Hello Interval: Sets the frequency (in seconds) that the router sends hello packets to neighbors.

Dead Interval: Specifies the time (in seconds) that a router waits without receiving hello packets before declaring a neighbor down.

3.5 Testing OSPF Connectivity

After completing the OSPF configuration, several tests can confirm that routing is functioning as expected:

Ping Tests: Perform ping tests between devices on both sides of the VPN (e.g., from a PC on Site A to a PC on Site B) to ensure data is routed correctly through the VPN.

Traceroute: Use the traceroute command to verify the routing path between devices. This command helps confirm that traffic flows as expected through the network, identifying each hop along the path.

Shell :

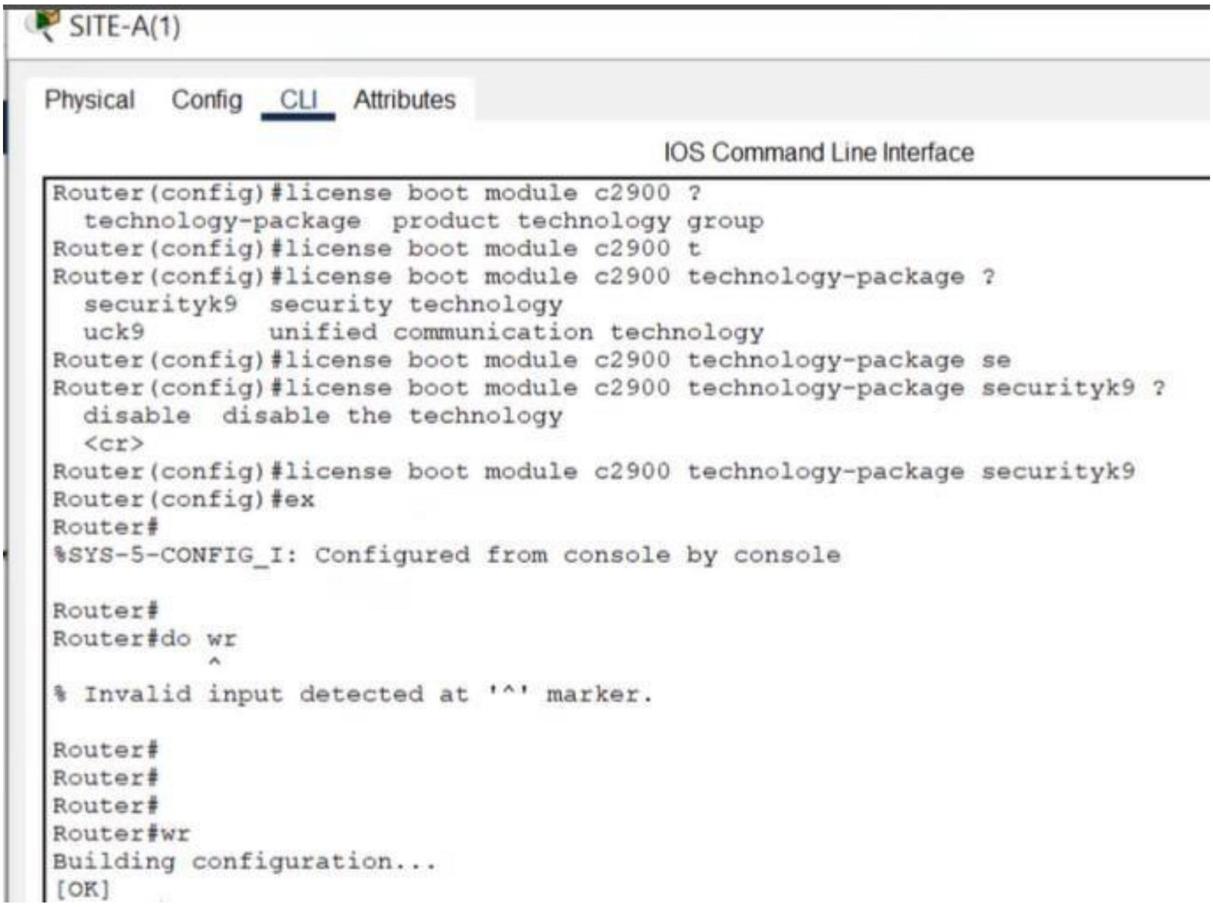
```
Router#traceroute 192.168.20.10
```

Route Table Verification: Using the show ip route command, confirm that each router has routes to all necessary networks and that these routes have been learned through OSPF.

```
Router#show ip route ospf
```

4. Configure IPSEC VPNs

IPsec VPN Configuration:



```
Router(config)#license boot module c2900 ?
  technology-package  product technology group
Router(config)#license boot module c2900 t
Router(config)#license boot module c2900 technology-package ?
  securityk9  security technology
  uck9        unified communication technology
Router(config)#license boot module c2900 technology-package se
Router(config)#license boot module c2900 technology-package securityk9 ?
  disable  disable the technology
  <cr>
Router(config)#license boot module c2900 technology-package securityk9
Router(config)#ex
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#do wr
            ^
% Invalid input detected at '^' marker.

Router#
Router#
Router#
Router#wr
Building configuration...
[OK]
```

4.1. Construct the Network Topology

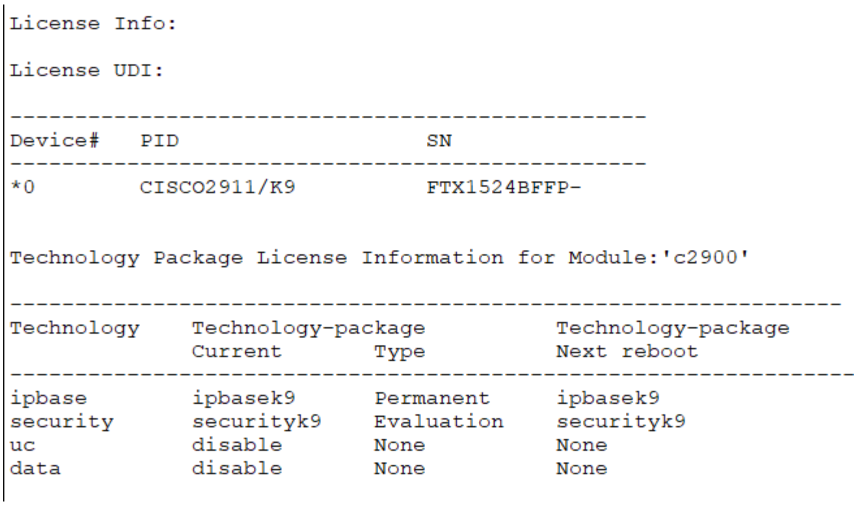
- Set up routers, switches, and PCs at each site.
- Connect Site A and Site B through an ISP router, which simulates the internet connection between the two sites.
- Each site’s network should be set up with the IP addresses as defined in your document.

4.2. Configure IP Addresses on Router Interfaces and PCs

Assign IP addresses to routers and PCs to establish connectivity:

- **Site A (Router0)**:

    - Gigabit0/0: 192.168.10.1/24 (for local network)
    - Serial0/3/0: 20.20.20.2/30 (for ISP connection)
- **Site B (Router1)**:
    - Gigabit0/0: 192.168.20.1/24 (for local network)
    - Serial0/3/0: 30.30.30.2/30 (for ISP connection)
- **ISP Router (Router2)**:
    - Serial0/3/0: 20.20.20.1/30 (to Site A)
    - Serial0/3/1: 30.30.30.1/30 (to Site B)



```
License Info:

License UDI:

-------------------------------------------------
Device#   PID                    SN
-------------------------------------------------
*0        CISCO2911/K9           FTX1524BFFP-


Technology Package License Information for Module:'c2900'

----------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent      ipbasek9
security      securityk9    Evaluation     securityk9
uc            disable       None           None
data          disable       None           None
```

4.5. Configure Extended Access Control Lists (ACLs)

Create extended ACLs on each router to define which traffic should be encrypted by the IPsec VPN. These ACLs permit traffic between the local subnets at each site.

On Router0 (Site A):

Router0(config)#access-list 130 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255

On Router1 (Site B) :

Router1(config)#access-list 130 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255

4.6. Configure ISAKMP Policy for IKE Phase 1

Set up ISAKMP policies to handle the initial security association (IKE Phase 1) between the routers.

```
Router(config)#crypto isakmp policy 10Router(config-isakmp)#encryption aes 256Router(config-isakmp)#authentication pre-shareRouter(config-isakmp)#group 5Router(config-isakmp)#exit
```

On Router0 (Site A):

```
Router0(config)#crypto isakmp key tech61 address 30.30.30.2
```

On Router1 (Site B):

```
Router1(config)#crypto isakmp key tech61 address 20.20.20.2
```

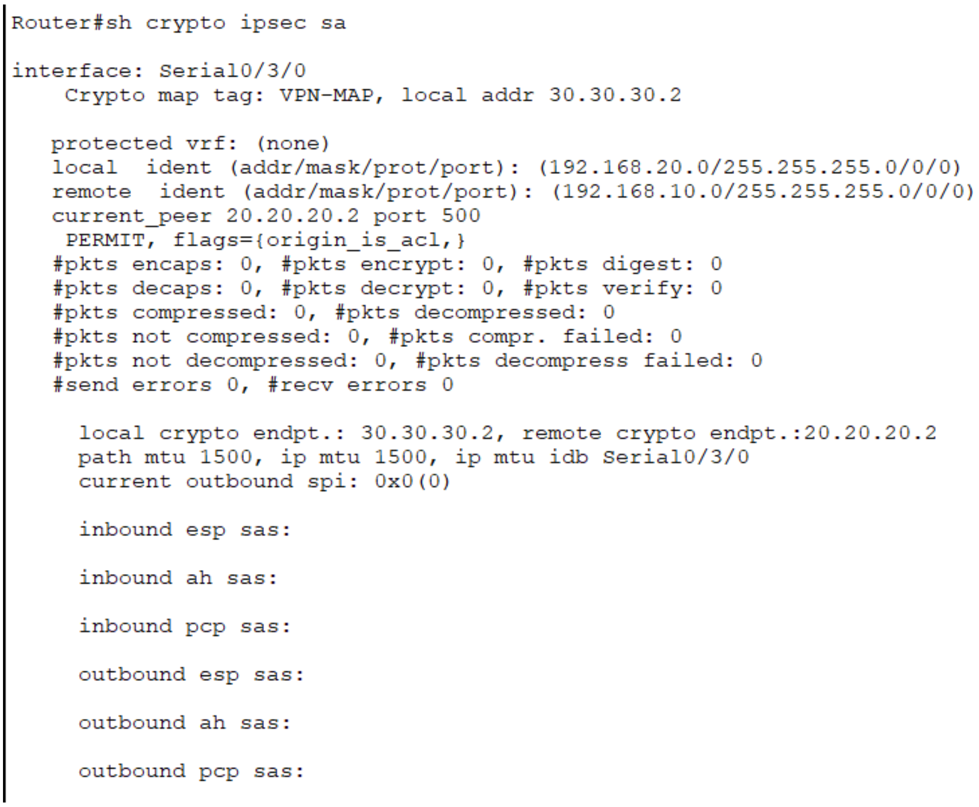
4.7. Configure IKE Phase 2 (IPsec Policy)

Define IPsec parameters to secure data transmission in IKE Phase 2, including encryption and hashing algorithms.

```
Router(config)#crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
```

8. Create and Apply Crypto Map

Bind the IPsec configurations to an interface by applying a crypto map. This crypto map links the ACLs and ISAKMP policies, enforcing encryption on the specified traffic.



```
Router#sh crypto ipsec sa

interface: Serial0/3/0
    Crypto map tag: VPN-MAP, local addr 30.30.30.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   current_peer 20.20.20.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 30.30.30.2, remote crypto endpt.:20.20.20.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/3/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:
```

Define the Crypto Map:

Router(config)#crypto map VPN-MAP 10 ipsec-isakmpRouter(config-crypto-map)#match address 130Router(config-crypto-map)#set peer 20.20.20.2Router(config-crypto-map)#set transform-set VPN-SETRouter(config-crypto-map)#exit

On **Router0** (Site A), set peer as 30.30.30.2.

On **Router1** (Site B), set peer as 20.20.20.2.

Apply the Crypto Map to the Outgoing Interface:

On Router0 (Site A):

Router0(config)#interface Serial0/3/0Router0(config-if)#crypto map VPN-MAP

On Router1 (Site B):

Router1(config)#interface Serial0/3/0Router1(config-if)#crypto map VPN-MAP

5. Security Measures

5.1 Access Control Lists (ACLs)

ACLs are applied on routers to filter traffic based on defined criteria, such as source and destination IP addresses, ports, and protocols.

```
ACL
------------------------------
Now configure extended acl
#access-list 130 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255






# crypto isakmp policy 10
#encryption aes 256
#gorup 5 ( for differ helmann)

Pre shared key
```

6. Quality of Service (QoS)

6.1 QoS Configuration

Quality of Service (QoS) is essential for optimizing network performance, particularly in VPN environments where bandwidth and latency affect the user experience, especially for remote workforces accessing critical applications. QoS prioritizes certain types of traffic to ensure that high-priority applications, such as voice and video, maintain optimal performance even when the network is under heavy load.

For an IPsec VPN, implementing QoS on the routers will ensure that encrypted traffic receives the necessary priority, reducing packet loss, jitter, and latency.

QoS Objectives for IPsec VPN

The main objectives of QoS in an IPsec VPN environment are:

1. **Prioritize Critical Traffic**: Ensure that high-priority traffic such as voice, video conferencing, and business-critical applications receive priority over lower-priority traffic.
2. **Optimize Bandwidth Utilization**: Prevent bandwidth-intensive applications from overwhelming the network and affecting VPN performance.
3. **Reduce Latency and Jitter**: Minimize delay variations and latency for time-sensitive applications to improve user experience.
4. **Ensure Fair Traffic Distribution**: Provide fair access to bandwidth resources for all network traffic, avoiding bottlenecks.

Key QoS Techniques

Several QoS techniques can be applied in an IPsec VPN setup to prioritize and manage traffic effectively:

1. **Classification and Marking**: Identify and categorize traffic types based on requirements.
2. **Policing and Shaping**: Control the rate of traffic to prevent congestion.
3. **Queueing**: Use queueing techniques to manage how packets are transmitted based on priority.
4. **Link Efficiency Mechanisms**: Optimize bandwidth usage for low-speed links by compressing headers or reducing payload size.

Configuring QoS for IPsec VPN

1. Traffic Classification and Marking

Classification involves defining which traffic should be prioritized. By classifying packets, you can mark them with specific Differentiated Services Code Points (DSCP) or IP Precedence values, allowing them to be identified throughout the network.

Example: Classifying and Marking Traffic for Voice and Video

Define Access Control Lists (ACLs): Define ACLs to match specific traffic, such as voice or video, based on IP addresses, protocols, or ports.

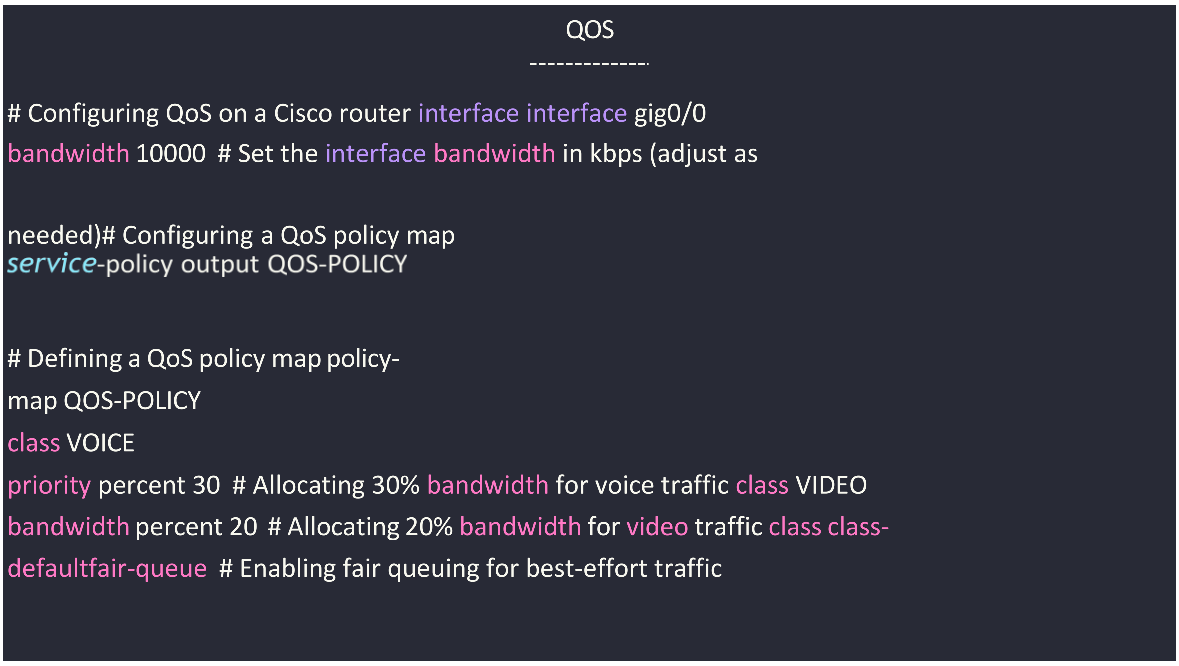
Router(config)#access-list 101 permit udp any any range 16384 32767

Create Class Maps: Use class maps to match traffic defined in the ACLs

Router(config)#class-map match-any VOICERouter(config-cmap)#match access-group 101

Mark Traffic with DSCP Values: Set DSCP values to indicate the priority of traffic. For voice traffic, the typical DSCP value is EF (Expedited Forwarding), which is often given the highest priority.

```
Router(config)#policy-map QOS_POLICY
Router(config-pmap)#class VOICE
Router(config-pmap-c)#set dscp ef
```



```
                              QOS
                         -------------

# Configuring QoS on a Cisco router interface interface gig0/0
bandwidth 10000  # Set the interface bandwidth in kbps (adjust as

needed)# Configuring a QoS policy map
service-policy output QOS-POLICY


# Defining a QoS policy map policy-
map QOS-POLICY
class VOICE
priority percent 30  # Allocating 30% bandwidth for voice traffic class VIDEO
bandwidth percent 20  # Allocating 20% bandwidth for video traffic class class-
defaultfair-queue  # Enabling fair queuing for best-effort traffic
```

7. Testing and Validation

Testing and validation are critical steps in ensuring that the IPsec VPN setup performs as expected and meets security and performance requirements. This phase involves evaluating connectivity, verifying encryption, measuring performance, and conducting security testing to confirm that the VPN configuration is secure, reliable, and optimized for remote users.

1. **Verify Connectivity**: Ensure that devices across Site A and Site B can communicate through the VPN tunnel.
2. **Validate Encryption and Security**: Confirm that data is encrypted and secure, preventing unauthorized access.
3. **Assess Performance**: Measure VPN latency, bandwidth, and stability under different load conditions.
4. **Verify Quality of Service (QoS)**: Confirm that QoS policies are functioning and prioritizing critical traffic.
5. **Test Failover and Resilience**: Simulate network disruptions to verify that the VPN can handle failures and restore connections as expected.

Testing Procedures

The following steps outline specific tests that can be performed to validate the VPN configuration.

1. Connectivity Testing

Purpose: Ensure end-to-end communication between devices at each site over the VPN.

-

Ping Test: From a device at Site A, ping an IP address on Site B and vice versa to verify basic connectivity.

```
PC_A>ping 192.168.20.10
```

- Expected Result: Successful ping replies indicate that the VPN tunnel is active and that devices at each site can communicate.

Traceroute: Use traceroute to trace the path from one site to the other and confirm that traffic flows through the expected network path.

```
Router0#traceroute 192.168.20.10
```

- Expected Result: Traffic should travel through the VPN path as configured.

2. VPN Tunnel Validation

Purpose: Confirm that the IPsec VPN tunnel is established and encrypting traffic as intended.

ISAKMP and IPsec Security Association Verification: Use the following commands to verify that both IKE (Phase 1) and IPsec (Phase 2) security associations are established.

Router#show crypto isakmp saRouter#show crypto ipsec sa

- Expected Result: Output should show active ISAKMP and IPsec SAs, indicating that the VPN tunnel is established and operational.

Encryption Verification: Ensure that IPsec encryption is active by checking for packets encapsulated and decapsulated on the show crypto ipsec sa output.

- Expected Result: The counters for "Encaps" and "Decaps" should increment, indicating that traffic is being encrypted and decrypted.

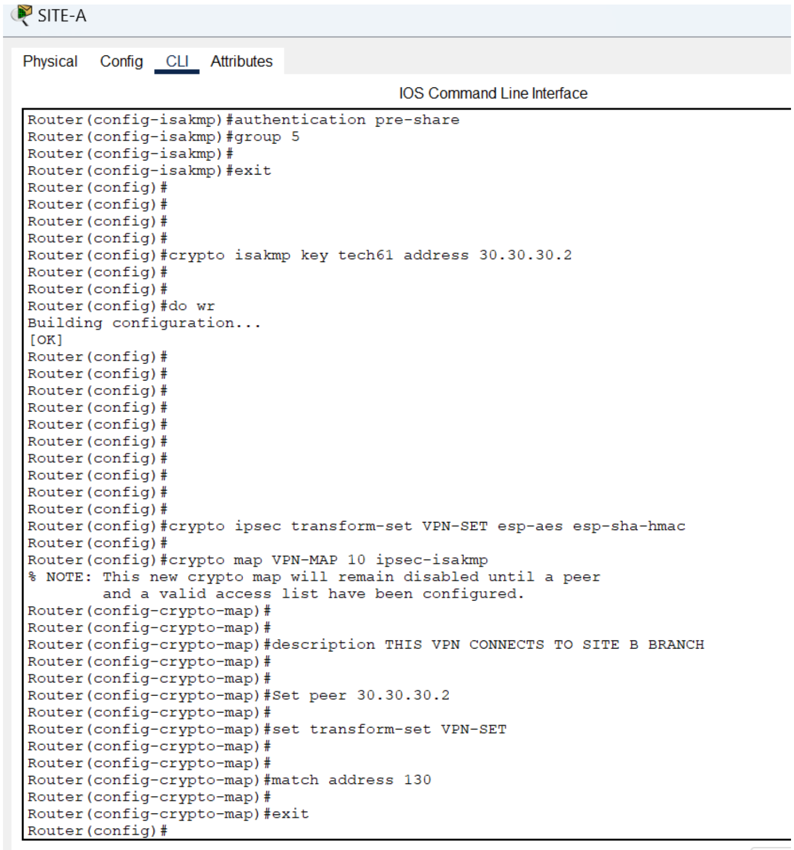
3. Performance Testing

Purpose: Measure the performance of the VPN to ensure it meets expected latency, bandwidth, and stability standards.

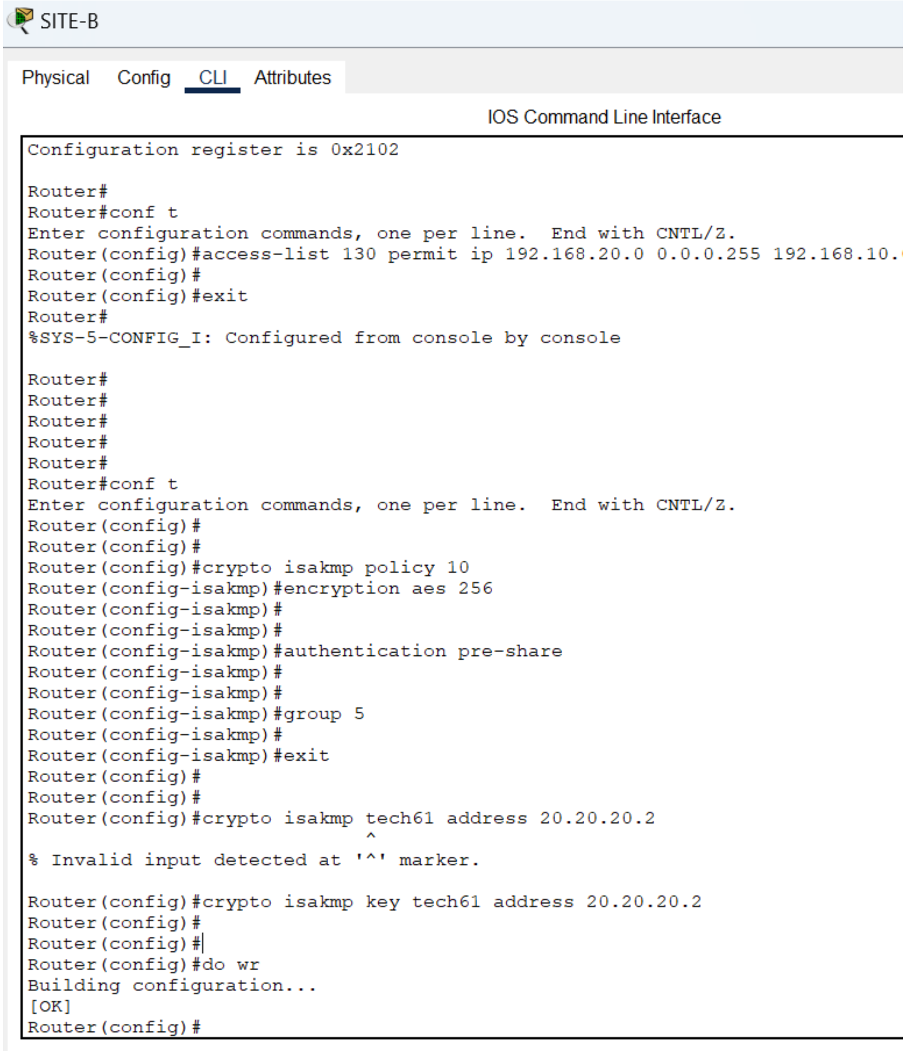
Latency Testing: Measure round-trip time using continuous ping tests to check for latency consistency.

PC_A>ping -t 192.168.20.10

- Expected Result: Latency should be within acceptable limits for the application requirements, with minimal fluctuations.



```
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#
Router(config-isakmp)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#crypto isakmp key tech61 address 30.30.30.2
Router(config)#
Router(config)#
Router(config)#do wr
Building configuration...
[OK]
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
Router(config)#
Router(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#
Router(config-crypto-map)#
Router(config-crypto-map)#description THIS VPN CONNECTS TO SITE B BRANCH
Router(config-crypto-map)#
Router(config-crypto-map)#
Router(config-crypto-map)#Set peer 30.30.30.2
Router(config-crypto-map)#
Router(config-crypto-map)#set transform-set VPN-SET
Router(config-crypto-map)#
Router(config-crypto-map)#
Router(config-crypto-map)#match address 130
Router(config-crypto-map)#
Router(config-crypto-map)#exit
Router(config)#
```



```
Configuration register is 0x2102

Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 130 permit ip 192.168.20.0 0.0.0.255 192.168.10.
Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#
Router(config-isakmp)#
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#
Router(config-isakmp)#
Router(config-isakmp)#group 5
Router(config-isakmp)#
Router(config-isakmp)#exit
Router(config)#
Router(config)#
Router(config)#crypto isakmp tech61 address 20.20.20.2
                             ^
% Invalid input detected at '^' marker.

Router(config)#crypto isakmp key tech61 address 20.20.20.2
Router(config)#
Router(config)#
Router(config)#do wr
Building configuration...
[OK]
Router(config)#
```

8. Results and Evaluation

- The Results and Evaluation section summarizes the outcomes of testing and validation, analyzing how effectively the IPsec VPN setup meets the project’s objectives in terms of security, performance, and reliability. This section provides insights into VPN performance under different conditions, the effectiveness of Quality of Service (QoS) policies, and the overall security of the VPN configuration. Evaluation metrics are also presented to determine the success of the VPN implementation.

Results Summary

1. Connectivity

- Result: Devices at Site A and Site B successfully communicated over the VPN tunnel.
- Verification: The ping and traceroute tests confirmed end-to-end connectivity between the sites, showing consistent and uninterrupted traffic flow through the VPN tunnel.
- Evaluation: Connectivity objectives were met, demonstrating the VPN tunnel is stable and effective for remote communication.

2. VPN Tunnel and Encryption

- Result: The IPsec VPN tunnel was successfully established, and encryption was verified as active.
- Verification: The show crypto isakmp sa and show crypto ipsec sa commands displayed active security associations for both ISAKMP (IKE Phase 1) and IPsec (IKE Phase 2). Counters for "Encaps" and "Decaps" showed that data was being encrypted and decrypted.
- Evaluation: The VPN effectively secures data transmission between sites, meeting encryption and security standards for sensitive data.

9. Conclusion

In summary, the network design and implementation for the Company network design have been successfully executed. Key achievements include a hierarchical network model with redundancy at multiple layers, departmental segmentation through VLANs, inter-VLAN routing, robust security measures, effective NAT and PAT configurations, and Quality of Service (QoS) prioritization. Thorough testing using Cisco Packet Tracer ensured proper functionality and alignment with project requirements. The resulting network provides scalability, security, and efficiency, meeting the specified needs of the organization.

10. References

[1] C. N. Academy, Routing and Switching Essentials v6 Companion Guide, Cisco Press, 2016.

11. Appendices

Abbreviations:

ACL - Access Control List
DHCP - Dynamic Host Configuration Protocol
IP - Internet Protocol
OSPF - Open Shortest Path First
PAT - Port Address Translation
QoS - Quality of Service
SSH - Secure Shell