**ITNE 2005R**

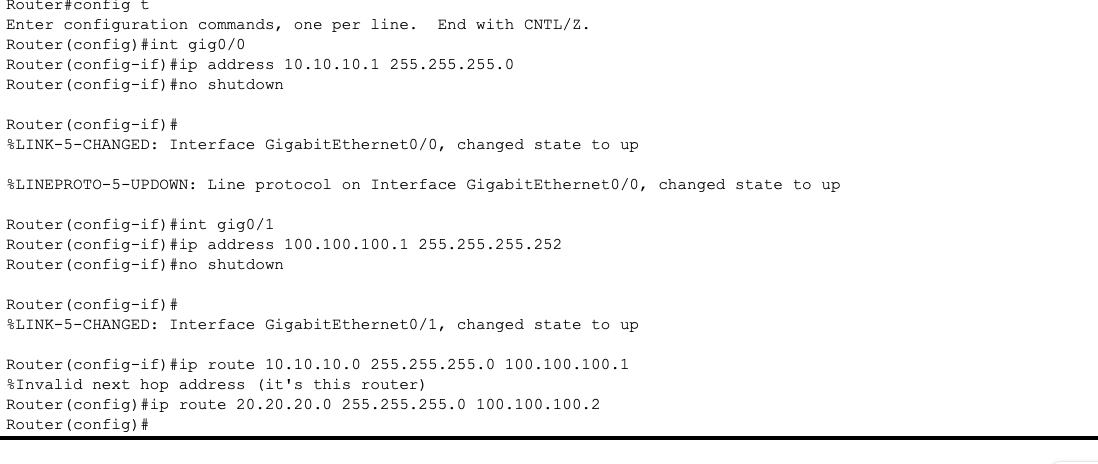
**Network Security Implementation**  
**Lab Tutorial 3**  
**Configure and verify a Site-to-Site IPsec VPN Tunnel**  
**March 2024**

**Introduction**

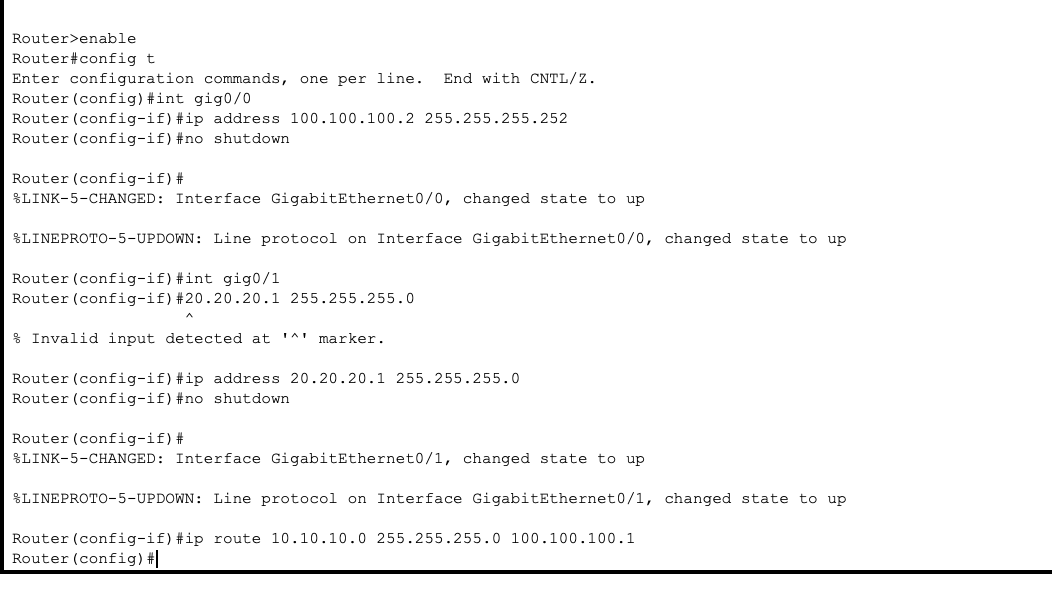
A site-to-site IPSec VPN tunnel is used to establish a secure communication link between two different locations, such as branch offices. This tunnel operates across the public Internet but relies on strong encryption standards to ensure the confidentiality of transmitted data.

In this guide, we will configure two Cisco 1941 routers (R1 and R2) to build a permanent site-to-site VPN connection. Both routers are assigned static public IP addresses. The setup employs ISAKMP (Phase 1) for initial key exchange and IPSec (Phase 2) for encrypting traffic and maintaining secure communication.

R1 (Router -1 )



R2



**IPSec VPN Requirements**

The laboratory exercise is organized into two primary phases:

1. Setting up ISAKMP (Phase 1)
2. Configuring IPSec (Phase 2), which includes defining ACLs, creating the transform set, and applying the crypto map

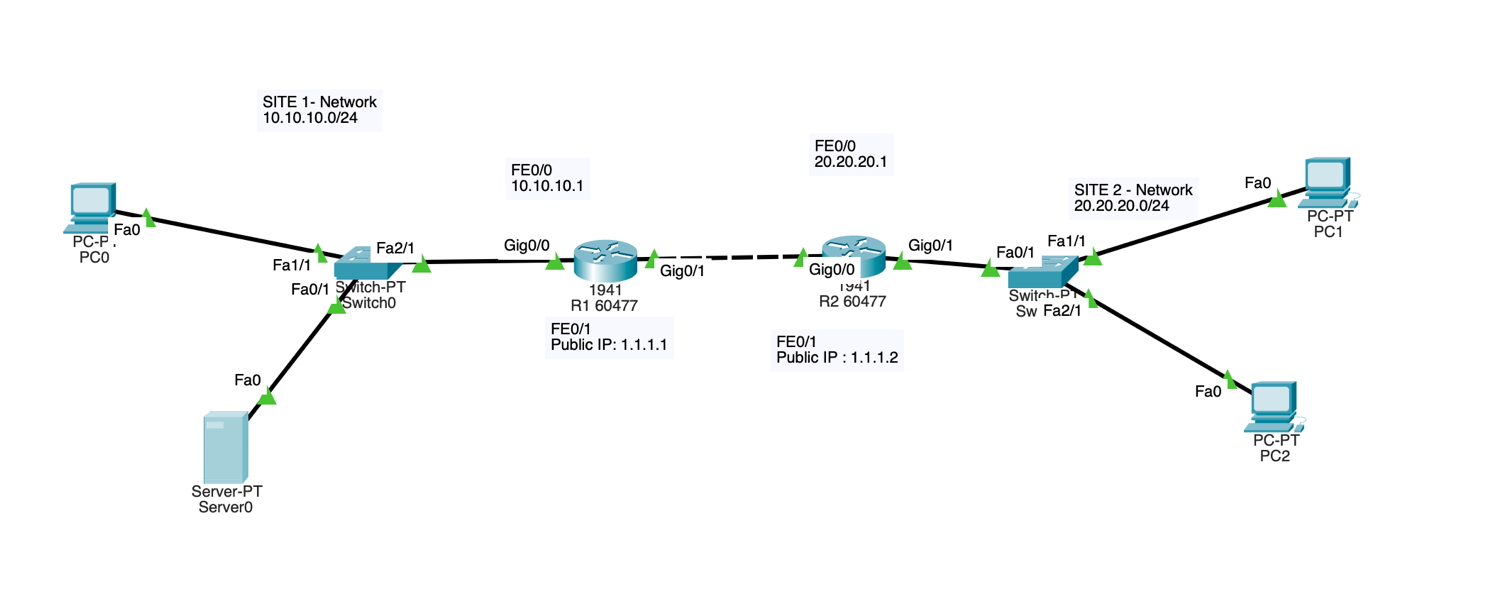
**Topology:**

| **Site** | **LAN Subnet** | **WAN/Public IP** | **Router Interfaces** |
| --- | --- | --- | --- |
| Site 1 (R1) | 10.10.10.0/24 | 1.1.1.1 / 100.100.100.1 | Gig0/0 → LAN, Gig0/1 → WAN to R2 |
| Site 2 (R2) | 20.20.20.0/24 | 1.1.1.2 / 100.100.100.2 | Gig0/0 → WAN to R1, Gig0/1 → LAN |

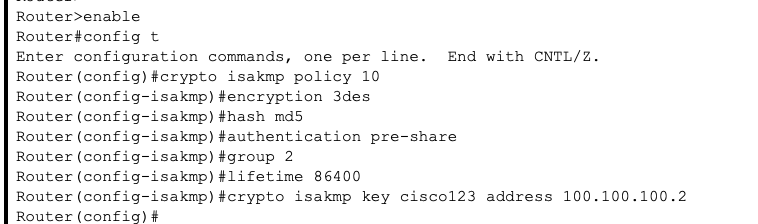
**Objective:** Establish a secure link between the two LAN segments, ensuring that devices on both sides can communicate seamlessly.

**Step 1: Configure ISAKMP (Phase 1)**

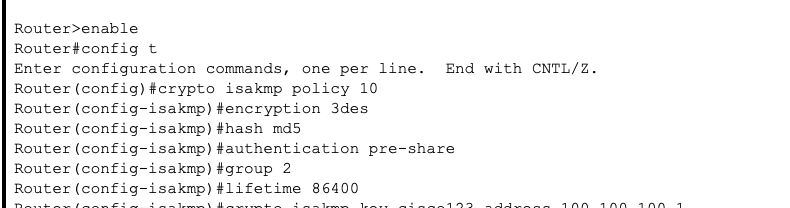
ISAKMP Phase 1 establishes the initial security association for IPSec.



**R1 Phase 1 Configuration:**



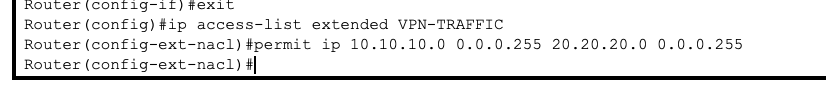
**R2 Phase 1 Configuration:**



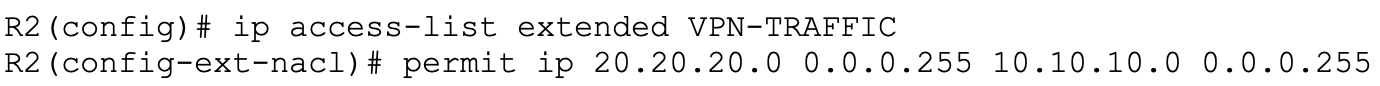
**Step 2: Configure IPSec (Phase 2)**

**Step 2.1: Create Extended ACL for VPN Traffic**

**R1:**

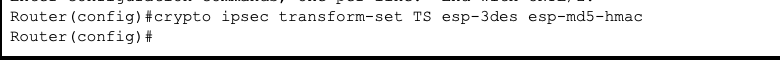


**R2**



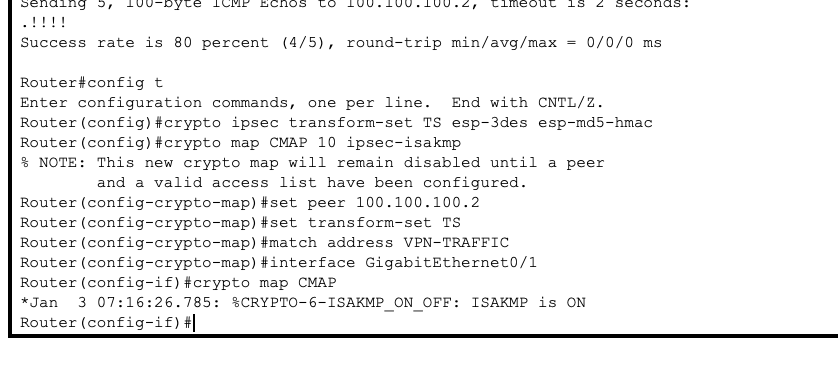
**Step 2.2: Create Transform Set**

**R1 & R2:**

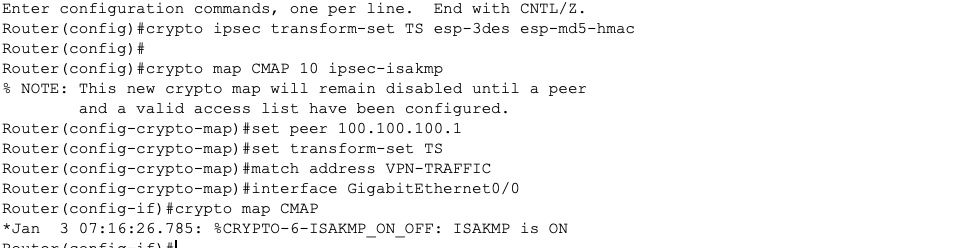


**Step 2.3: Create Crypto Map**

**R1:**

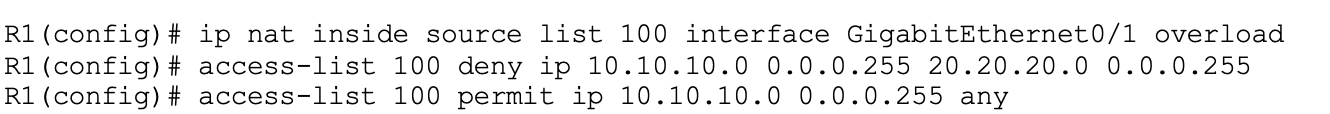


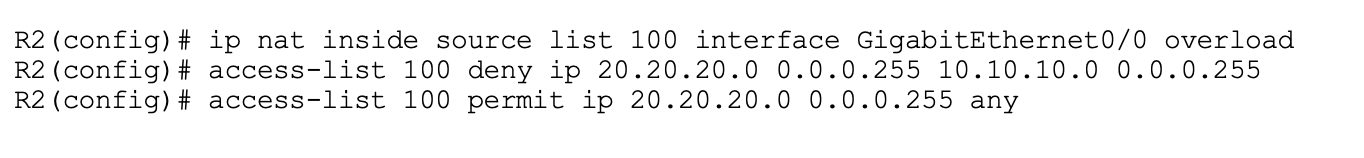
**R2:**



**Step 3: NAT Configuration**

Ensure that VPN traffic is not affected by NAT.

**R1:**

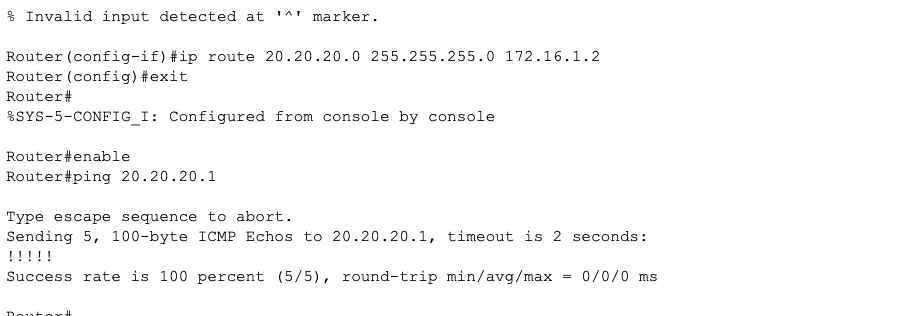
**R2:****Step 4: Verify VPN Tunnel**

**Ping Test:**

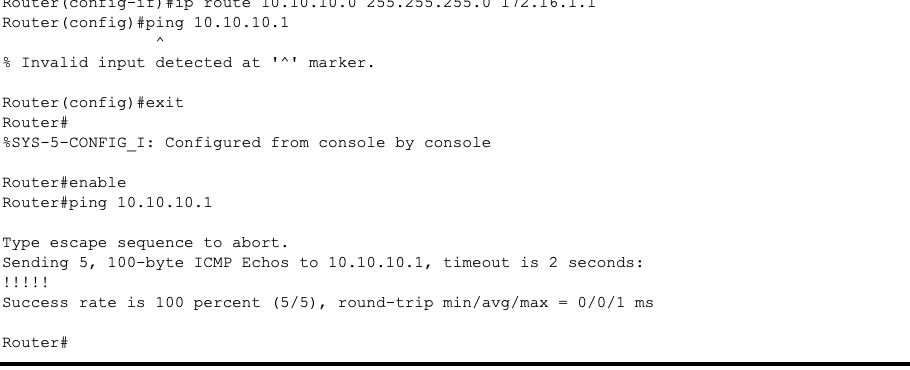
R1# ping 20.20.20.1 source 10.10.10.1

* First packet may timeout → tunnel negotiation
* Subsequent packets → success

**R1:**

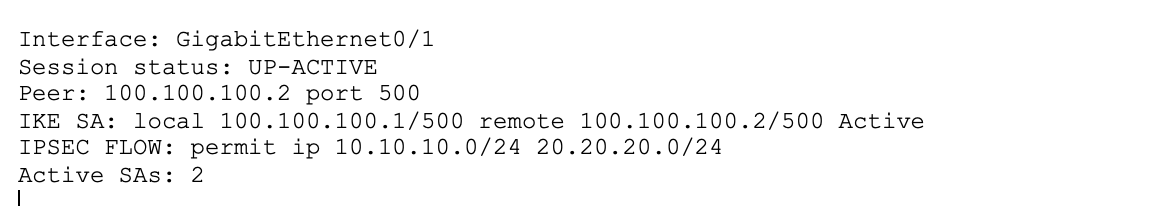


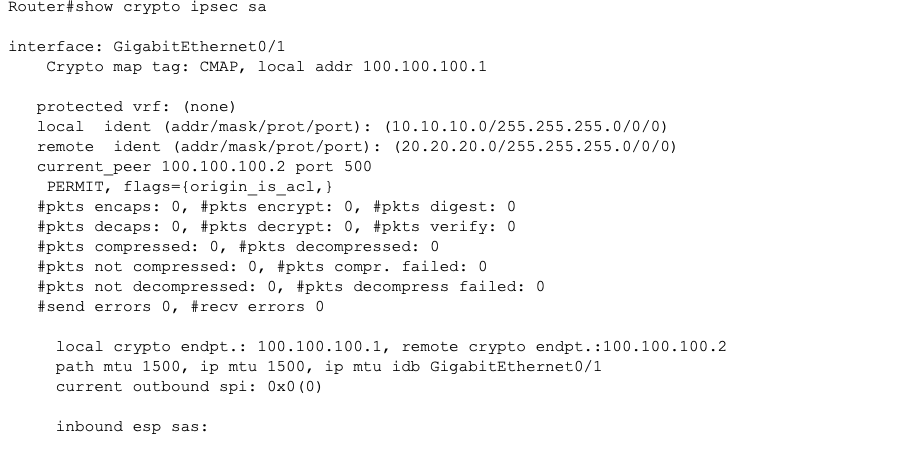
**R2:**

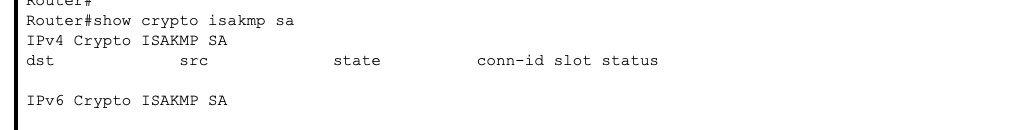


**Show Crypto Session:**

R1# show crypto session

**Output** 





**Conclusion**

* A site-to-site IPSec VPN tunnel was successfully established between R1 and R2 with the help of Cisco 1941 routers.
* Secure communication was achieved between the LANs of both locations.
* The tunnel functionality was validated through ping tests and the use of the **show crypto session** command.
* NAT settings were properly configured to ensure they did not interfere with VPN traffic.