

Network Architecture: Site-to-Site IPsec VPN Implementation.

The objective is to design and configure an encrypted Site-to-Site VPN to establish a secure communication tunnel between two remote branch office networks.

To practically apply network security principles, I developed a Proof of Concept (PoC) lab simulating a corporate network requiring secure remote connectivity. This hands-on project required configuring Cisco IOS devices from the ground up. By implementing routing protocols, Access Control Lists (ACLs), and establishing an IPsec VPN tunnel utilizing IKE phase 1 and 2, I successfully validated the encrypted transmission of data across a simulated public infrastructure.

Skills & Technologies: Cisco IOS, IPsec, IKE phase 1 & 2, Routing, Access Control Lists

To outline the architecture of the simulated multi-site environment, internal client endpoints, local switches, and edge routers were placed. Then to protect cross-site traffic, the edge routers were configured with IKE and IPsec to establish a secure, encrypted tunnel across a central routing simulated public ISP.

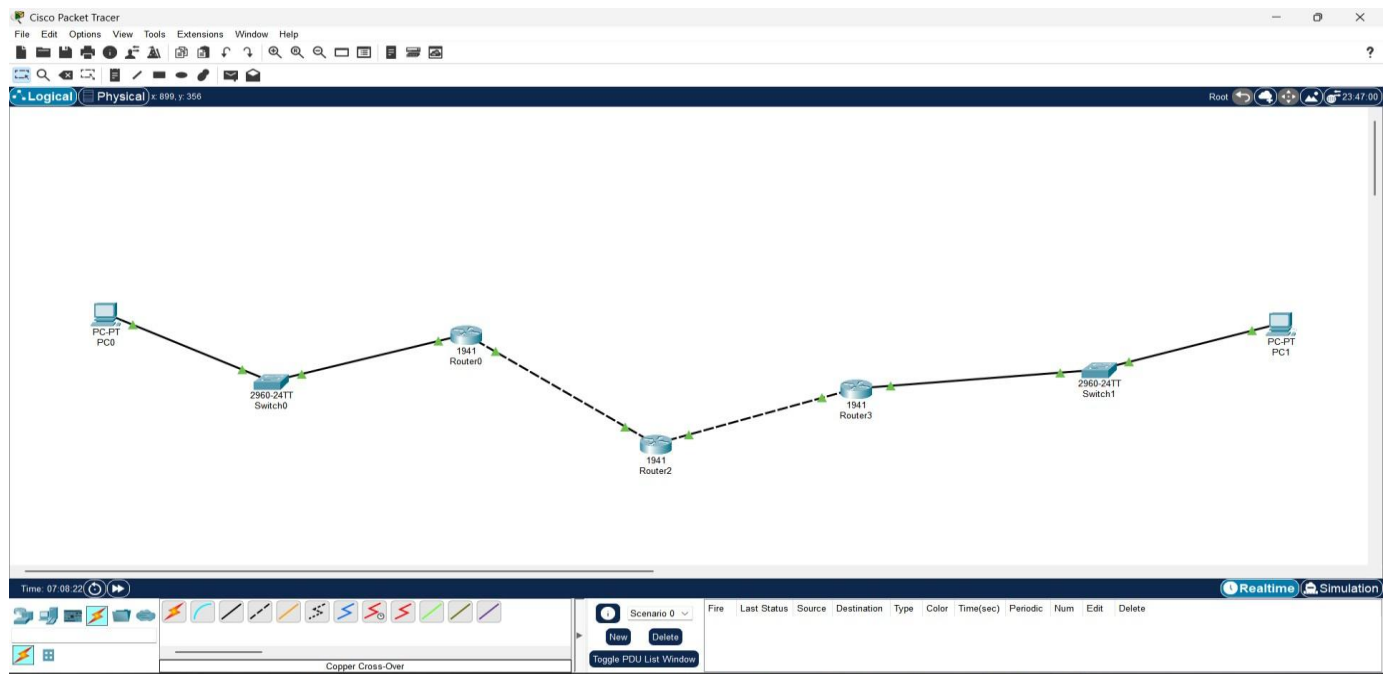


Figure 1 Topology

Configured local switches to establish by establishing the internal routing environment. That way we can make sure the endpoints are properly connected with correct gateways before starting cross-site traffic. Validated with ICMP pinging test.

Switch configuration

The image displays four screenshots of Cisco IOS Command Line Interface (CLI) windows, arranged in a 2x2 grid. Each window shows the configuration of a different switch.

- Top Left (Switch1):** Shows the configuration for Switch1. The configuration includes enabling Encapsulation, setting the hostname to 'encapsulation', and configuring various interfaces (FastEthernet0/1 through FastEthernet0/14). The configuration is saved to the startup configuration.
- Top Right (Switch0):** Shows the configuration for Switch0. The configuration includes enabling Encapsulation, setting the hostname to 'encapsulation', and configuring various interfaces (FastEthernet0/1 through FastEthernet0/14). The configuration is saved to the startup configuration.
- Bottom Left (Switch1):** Shows the configuration for Switch1. The configuration includes enabling Encapsulation, setting the hostname to 'encapsulation', and configuring various interfaces (FastEthernet0/1 through FastEthernet0/24). The configuration is saved to the startup configuration.
- Bottom Right (Switch0):** Shows the configuration for Switch0. The configuration includes enabling Encapsulation, setting the hostname to 'encapsulation', and configuring various interfaces (FastEthernet0/1 through FastEthernet0/24). The configuration is saved to the startup configuration.

Each window has a 'Physical' tab selected, and the 'CLI' tab is active. The 'Attributes' tab is also visible. The 'Physical' tab shows the physical configuration of the switch, including the hostname and the configuration of the interfaces. The 'CLI' tab shows the command-line interface, where the configuration is entered. The 'Attributes' tab shows the attributes of the switch, including the hostname and the configuration of the interfaces.

After defining encryption policies, transform sets, and crypto maps, then deploy strict Access Control Lists (ACLs) to permit authorized traffic to cross for the simulated public network. Both edge routers have complementary IP sec and ISAKMP (IKE) configs for a secure VPN.

The image displays two side-by-side screenshots of a Cisco IOS Command Line Interface (CLI) window, likely from a Packet Tracer simulation. Both windows show the configuration of a Cisco 1900 router.

Left Window: The title bar reads "Router3". The tabs are "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, showing the "IOS Command Line Interface". The configuration text is as follows:

```
mclunge-r2#enable
mclunge-r2#show running-config
Building configuration...

Current configuration : 1155 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname mclunge-r2
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISC01941/K9 on FTK1524568W-
license boot module c1900 technology-package securityk9
!
!
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
!
crypto isakmp key Fullaill! address 10.0.0.1
!
!
crypto ipsec transform-set R1 esp-aes 256 esp-sha-hmac
!
crypto map IPSEC 10 ipsec-isakmp
set peer 10.0.0.1
set pfa group5
set security-association lifetime seconds 86400
set transform-set R1
match address 100
```

At the bottom of the window, there are "Copy" and "Paste" buttons.

Right Window: The title bar reads "Router0". The tabs are "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, showing the "IOS Command Line Interface". The configuration text is as follows:

```
rod
mclunge-r1# show running-config
Building configuration...

Current configuration : 1155 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname mclunge-r1
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISC01941/K9 on FTK1524568T2-
license boot module c1900 technology-package securityk9
!
!
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
!
crypto isakmp key Fullaill! address 10.0.1.1
!
!
!
crypto ipsec transform-set R3 esp-aes 256 esp-sha-hmac
!
crypto map IPSEC 10 ipsec-isakmp
set peer 10.0.1.1
set pfa group5
set security-association lifetime seconds 86400
set transform-set R3
match address 100
```

At the bottom of the window, there are "Copy" and "Paste" buttons.

[illegible]

Network Architecture: Site-to-Site IPsec VPN Implementation.

To verify the integrity of the IPsec VPN, the show crypto ipsec sa command confirmed the tunnel was actively encapsulating packets. Finally, ICMP ping tests were executed to successfully validate end-to-end encrypted communication between the remote clients.

The image displays four screenshots of network devices, arranged in a 2x2 grid, showing the configuration and verification of an IPsec VPN.

Top Left (PC1): A Windows Command Prompt window showing the results of a series of ping tests. The tests show successful communication (0% loss) for 192.168.1.1 and 192.168.1.100, and a 100% loss for 192.168.1.101.

```
PC1 Command Prompt
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 192.168.1.100
Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 192.168.1.101
Pinging 192.168.1.101 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128
Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
```

Top Right (PC0): A Windows Command Prompt window showing the results of a series of ping tests. The tests show successful communication (0% loss) for 192.168.1.1 and 192.168.1.100, and a 100% loss for 192.168.1.101.

```
PC0 Command Prompt
C:\>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=255
Reply from 192.168.0.1: bytes=32 time=1ms TTL=255
Reply from 192.168.0.1: bytes=32 time=1ms TTL=255
Reply from 192.168.0.1: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.1: bytes=32 time=1ms TTL=254
Reply from 192.168.1.1: bytes=32 time=1ms TTL=254
Reply from 192.168.1.1: bytes=32 time=1ms TTL=254
Reply from 192.168.1.1: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.1: bytes=32 time=1ms TTL=254
Reply from 192.168.1.1: bytes=32 time=1ms TTL=254
Reply from 192.168.1.1: bytes=32 time=1ms TTL=254
Reply from 192.168.1.1: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Bottom Left (Router3): A Windows Command Prompt window showing the output of the 'show crypto ipsec sa' command. The output shows the configuration and status of the IPsec SA for the tunnel between 192.168.1.1 and 192.168.1.100.

```
Router3 Command Prompt
mccolunje-r2# show crypto ipsec sa
interface: GigabitEthernet0/0
Crypto map tag: IPSEC, local addr 10.0.1.1
protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.0.0/0)
remote ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0)
current_peer 10.0.1.1 port 500
PERMIT, flags=(origin_is_acl, )
  #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
  #pkts decaps: 7, #pkts decrypt: 7, #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.: 10.0.1.1, remote crypto endpt.: 10.0.1.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current_outbound spi: 0x6D5A450C(1837778188)
inbound esp sa:
spi: 0x5B203A3(3853648805)
transform: esp-aes 256 esp-sha-hmac ,
in use settings = (Tunnel, )
conn id: 2005, flow_id: FPGAI1, crypto map: IPSEC
sa timing: remaining key lifetime (k/sec): (4523504/84692)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE
inbound ah sa:
inbound pop sa:
outbound esp sa:
spi: 0x6D5A450C(1837778188)
transform: esp-aes 256 esp-sha-hmac ,
in use settings = (Tunnel, )
conn id: 2006, flow_id: FPGAI1, crypto map: IPSEC
sa timing: remaining key lifetime (k/sec): (4523504/84692)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE
outbound ah sa:
outbound pop sa:
```

Bottom Right (Router0): A Windows Command Prompt window showing the output of the 'show crypto ipsec sa' command. The output shows the configuration and status of the IPsec SA for the tunnel between 192.168.1.1 and 192.168.1.100.

```
Router0 Command Prompt
mccolunje-r1# show crypto ipsec sa
interface: GigabitEthernet0/0
Crypto map tag: IPSEC, local addr 10.0.0.1
protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.0.0/0)
current_peer 10.0.1.1 port 500
PERMIT, flags=(origin_is_acl, )
  #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
  #pkts decaps: 7, #pkts decrypt: 7, #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 1, #recv errors 0
local crypto endpt.: 10.0.0.1, remote crypto endpt.: 10.0.1.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current_outbound spi: 0x5B203A3(3853648805)
inbound esp sa:
spi: 0x6D5A450C(1837778188)
transform: esp-aes 256 esp-sha-hmac ,
in use settings = (Tunnel, )
conn id: 2005, flow_id: FPGAI1, crypto map: IPSEC
sa timing: remaining key lifetime (k/sec): (4523504/84717)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE
inbound ah sa:
inbound pop sa:
outbound esp sa:
spi: 0x5B203A3(3853648805)
transform: esp-aes 256 esp-sha-hmac ,
in use settings = (Tunnel, )
conn id: 2006, flow_id: FPGAI1, crypto map: IPSEC
sa timing: remaining key lifetime (k/sec): (4523504/84717)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE
outbound ah sa:
outbound pop sa:
```

Network Architecture: Site-to-Site IPsec VPN Implementation.

By simulating the deployment of a Site-to-site IPsec VPN using robust routing configuration and strict cryptographic policies, this project successfully demonstrated the engineering of a secure, encrypted tunnel for an enterprise network architecture.