GUIDE

Enterprise IPsec VPN Troubleshooting

V1.0.0

Author:

Eldon Gabriel

August 6, 2025

PORTFOLIO OVERVIEW

0.1 Secure Enterprise VPN Deployment & Diagnostics

This report documents how I built a dynamic network for a medium-sized organization using Cisco Packet Tracer v8.2.2. I followed cybersecurity best practices and documented everything step-by-step.

I created this guide as an extra project portfolio activity so I could further my understanding. Plus, apply system administration and network security skills.

The goal was to design a network that uses secure routing, VLANs, and an IPSec tunnel between two networks. I also made sure internet access and traffic segmentation remained intact.

Specifications

The project included the following setup and configurations:

- Installed Cisco Packet Tracer v8.2.2
- Set up a firewall and a multilayer switch on separate subnets
- Created VLANs
- Deployed VLANs behind the switch
- Built a DMZ with a simple web server
- Configured a working IPsec site-HQ-site VPN
- Set up a secure guest Wi-Fi using a separate switch and router
- Connected the internal networks to the internet using an ISP router

Validation Steps

To make sure everything worked:

- All device links showed green (active) status
- Ran traceroute to confirm the IPsec tunnel was working
- Verified VLAN-HQ-VLAN communication across the network using traceroute

Learning Outcome

This project helped me go from theory to applied skills. I resolved real-world simulation issues—such as configuration persistence, NAT behavior, and crypto map validation—and reinforced my ability to:

- Design secure network topologies
- Troubleshoot misconfigurations and broken tunnels
- Produce structured, technical documentation with command validation

This work lines up with the **Advanced Beginner** level of the ASD Cyber Skills Framework. It shows that I can:

- Write clear and structured technical documentation
- Spot the limits of the tools I'm working with
- Prove my configurations work through testing and command-line outputs

---

Disclaimer: This report is based on hands-on practice conducted in a simulated Cisco Packet Tracer environment. It is intended for demonstration within my cybersecurity portfolio and should not be considered official curriculum content**.**

TABLE OF CONTENTS

REVISION HISTORY

Version	Date	👤 Author	Description of Changes
v1.0.0	08/06/2025	Eldon G.	Initial draft.

1.0 INTRODUCTION AND SETUP

1.1 Project Description

This report documents how I built a dynamic network using cybersecurity best practices. The network connects users across two sites—Headquarters and Branch Office. I used **Cisco Packet Tracer v8.2.2** to simulate the full setup.

The main goal was to create a secure site-HQ-site IPSec VPN tunnel. While the configuration seemed simple at first, the project turned into a deeper learning experience. I ran into unexpected problems with protocol behavior, tool limitations, and human error. Each challenge helped me think more like a system administrator and network troubleshooter.

Packet Tracer was useful for learning, but it sometimes gave confusing results during advanced setups. I learned how to tell the difference between a real misconfiguration and a simulator issue. Many problems weren't my fault—they were caused by how Packet Tracer handles certain protocols.

This project helped me develop a key networking skill: working through problems step-by-step. I used CLI commands, traceroute, and controlled traffic tests to confirm when my setup was working, even when the GUI didn't reflect it. In the end, the process taught me how to troubleshoot and validate configurations with a critical mindset.

1.2 Network Topology Mapping

The implemented topology consists of three primary routing devices:

- Headquarters Firewall (HQ-FW-EX)
- **ISP Router** (Internet Service Provider → ISP-Router)
- Branch Office Firewall (BO-FW-EX)

These devices are linked together to build a secure site-HQ-site IPSec VPN tunnel. The ISP Router acts as a simulated public internet. The Headquarters office has several internal networks that connect to the Branch Office network.

Key Network Components & Interconnections

ISP Server (Internet Simulator)

- **Device Model:** Server-PT
- **Role:** Simulates external public Internet services
- **Interfaces:**

Interface	IP Address	Connected Device
FastEthernet0	8.8.8.1 /30	ISP-Router → Gig2/0

ISP-Router (Internet Backbone Router)

- **Device Model:** PT-Empty
- **Role:** Internet Simulation, routes traffic between Headquarters & Branch Office networks
- **Interfaces:**

Interface	IP Address	Connected Device
GigabitEthernet0/0	203.0.113.1/30	BO-FW-EX → Gig0/0/1
GigabitEthernet1/0	203.0.113.5/30	HQ-FW-EX → Gig0/0/0

Headquarters Firewall (HQ-FW-EX)

- **Device Model:** ISR4331
- **Role:** Edge router for the Headquarters site, VPN endpoint
- **Interfaces:**

Interface	IP Address	Connected Device
GigabitEthernet0/0	203.0.113.6/30 (External)	ISP-Router → Gig1/0
GigabitEthernet0/1	10.0.0.2/30 (Internal)	MSW-HQ-L3 → Gig0/2

Headquarters Multi-Layer Switch (MSW-HQ-L3)

Device Model: 3560 24PS

- **Role:** Routes internal Headquarters VLANs
- **Note:** Guest VLAN is routed via HQ-Guest-Rtr for security segmentation
- **VLAN Configuration:**

VLAN ID	NAME	Subnet	Ports
10	Workstation	192.168.10.0/24	Fa0/7, Fa0/8
20	Server Closet	192.168.20.0/24	Fa0/3, Fa/04
30	DMZ	192.168.30.0/24	Fa0/9
40	Guest Wi-Fi	192.168.41.0/24	Fa0/10
50	Reserved	192.168.50.0/24	*Future Use

Note: *VLAN 50 is reserved for future segmentation, such as a secure wireless network for a project-specific team.*

Branch Office Firewall (`BO-FW-EX`)

- **Device Model:** `ISR4331`
- **Role:** Branch Office firewall and VPN endpoint
- **Interfaces:**

Interface	IP Address	Connection Device	Network
GigabitEthernet0/0/0	192.168.2.1/24	MSW-BO-L3 → Fa0/1	NY Internal LAN
GigabitEthernet0/0/1	203.0.113.2/30	ISP-Router → Gig0/0	NY WAN

1.2.1 Network Segments

Headquarters Internal LANs (behind `MSW-HQ-L3`)

VLAN ID	VLAN Name	Device Name	IP Address	Subnet	Default Gateway
10	Workstation	`HQ-PC-1`	192.168.10.10/24	192.168.10.0/24	192.168.10.1
10	Workstation	`HQ-PC-2`	192.168.10.11/24	192.168.10.0/24	192.168.10.1
20	Server Closet	`HQ-Server1`	192.168.20.10/24	192.168.20.0/24	192.168.20.1
20	Server Closet	`HQ-Server2`	192.168.20.11/24	192.168.20.0/24	192.168.20.1
30	DMZ	`HQ-Web-Server`	192.168.30.10/24	192.168.30.0/24	192.168.30.1
40	Guest Wi-Fi	`HQ-Guest-Rtr`	192.168.41.2/24	192.168.41.0/24	*N/A
40	Guest Wi-Fi	`HQ-Guest-SW`	*N/A	*N/A	*N/A
40	Guest Wi-Fi	`HQ-Guest-AP`	*N/A	*N/A	*N/A
40	Guest Wi-Fi	`HQ-Guest-PC`	192.168.41.3/24	192.168.41.0/24	192.168.41.2
50	Reserved	*N/A	*N/A	*N/A	*N/A

Note: VLAN 50 is reserved for future segmentation and is currently unused. Devices marked *N/A do not have IP configurations, as they are Layer 2 infrastructure or unassigned.

Branch Office Internal LAN

Network Segment	Subnet	Connected Devices
TO Internal Link	10.0.0.0/30	HQ-FW-EX and MSW-HQ-L3
NY Internal LAN	192.168.2.0/24	BO-FW-EX (Gig0/0/0), BO-PC-1
TO Public WAN Segment	203.0.113.4/30	HQ-FW-EX and ISP-Router
NY Public WAN Segment	203.0.113.0/30	BO-FW-EX and ISP-Router

IPsec VPN Tunnel Parameters

VPN Endpoint (Local)	VPN Endpoint (Remote)	Networks Secured (Interesting Traffic)
BO-FW-EX (203.0.113.2)	HQ-FW-EX (203.0.113.6)	**Local:** 192.168.2.0/24 **Remote:** 192.168.X.0/24 (All HQ subnets)

1.3 Comprehensive Configuration Steps

This section outlines the core setup procedures completed across all routing devices. It covers physical topology validation, static IP assignments and interface configuration, NAT and VPN ACL design, and license activation.

1.3.1 Initial Setup and Licensing Activation

This step ensured all devices were connected according to the logical diagram. This prepared the routers for advanced configuration tasks such as NAT, VPN, and licensing (where applicable).

1.3.1.1 Host Static IP Configuration

Next, I configured the static IP addresses and default gateways for the host machines. This ensures they can communicate within their respective local networks and reach their gateway.

- **HQ-PC:** `192.168.10.100/24` → Gateway of `192.168.10.1`
- **BO-PC:** `192.168.2.100/24` → Gateway of `192.168.2.1`

These settings enable local LAN connectivity. However, initial cross-site ping attempts failed due to improper NAT behavior. I later traced this to a hidden `no ip cef` directive, which I removed to restore correct NAT functionality.

1.3.1.2 Interface IP Assignment and Device Role

All three routers were configured with interface addresses, basic NAT setup, static routes, and ACLs to exempt VPN-bound traffic. Below is a summary of each device's role and commands used.

> ***Note:*** *For more reliable results in Cisco Packet Tracer, all configuration steps in Section 1.3 were ultimately consolidated and applied using full configuration block pastes. See [Section 1.4.2.1](#) for details on this workaround.*

Headquarters Firewall Configuration (HQ-FW-EX)

cli

```
configure terminal or conf t
hostname HQ-FW-EX

interface GigabitEthernet0/0/0
ip address 203.0.113.6 255.255.255.252
ip nat outside
no shutdown
exit

interface GigabitEthernet0/0/1
ip address 10.0.0.2 255.255.255.252
ip nat inside
no shutdown
exit

! Routing
ip route 0.0.0.0 0.0.0.0 203.0.113.5
ip route 192.168.10.0 255.255.255.0 10.0.0.1
ip route 192.168.20.0 255.255.255.0 10.0.0.1
ip route 192.168.30.0 255.255.255.0 10.0.0.1
ip route 192.168.41.0 255.255.255.0 10.0.0.1
ip route 192.168.50.0 255.255.255.0 10.0.0.1

! ACL for VPN traffic exemption
ip access-list extended NO_NAT_VPN_TRAFFIC_TO
deny ip 192.168.10.0 0.0.0.255 192.168.2.0 0.0.0.255
deny ip 192.168.20.0 0.0.0.255 192.168.2.0 0.0.0.255
deny ip 192.168.30.0 0.0.0.255 192.168.2.0 0.0.0.255
deny ip 192.168.41.0 0.0.0.255 192.168.2.0 0.0.0.255
deny ip 192.168.50.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip any any

! NAT with VPN exemption
no ip nat inside source list 100 interface GigabitEthernet0/0/0 overload
ip nat inside source list 100 interface GigabitEthernet0/0/0 overload

end
write memory
```

ISP-Router Configuration (Transit Node)

```cli
configure terminal or conf t
hostname ISP-Router

interface GigabitEthernet0/0
 ip address 203.0.113.1 255.255.255.252
 no shutdown
exit

interface GigabitEthernet0/1
 ip address 203.0.113.5 255.255.255.252
 no shut
exit
```

Branch Office Firewall Configuration (BO-FW-EX)

cli

```
configure terminal or conf t
hostname BO-FW-EX

! Interfaces
interface GigabitEthernet0/0/0
 ip address 192.168.2.1 255.255.255.0
 ip nat inside
 no shutdown
exit

interface GigabitEthernet0/0/1
 ip address 203.0.113.2 255.255.255.252
 ip nat outside
 no shutdown
exit

! Routing
ip route 0.0.0.0 0.0.0.0 203.0.113.1


! ACL for VPN exemption

! For VPN traffic not to be NAT'd:
ip access-list extended NO_NAT_VPN_TRAFFIC
 deny ip 192.168.2.0 0.0.0.255 192.168.10.0 0.0.0.255
 deny ip 192.168.2.0 0.0.0.255 192.168.20.0 0.0.0.255
 deny ip 192.168.2.0 0.0.0.255 192.168.30.0 0.0.0.255
 deny ip 192.168.2.0 0.0.0.255 192.168.41.0 0.0.0.255
 deny ip 192.168.2.0 0.0.0.255 192.168.50.0 0.0.0.255
 permit ip any any

! NAT with VPN exemption
no ip nat inside source list 100 interface GigabitEthernet0/0/1 overload
ip nat inside source list NO_NAT_VPN_TRAFFIC interface
GigabitEthernet0/0/1 overload

end
write memory
```

1.3.1.3 Security License Activation (Optional)

In production environments using Cisco ISR routers, VPN features require a security license. While Cisco Packet Tracer assumes pre-licensed routers, these are the real-world steps.

```
cli

! Verify current license
status show version | include license

! Activate the securityk9 technology package
license boot module ISR4300 technology-package securityk9

copy run start
reload

! Post-reboot verification
show version | include license
```

> **Note:** *Replace* `ISR4300` *with your router's actual model from* `show version` *if different.*

1.3.2 Interface Configuration and Static Routing

This section documents the essential interface and routing configurations applied to the core network devices: Headquarters (`HQ-FW-EX`), Branch Office (`BO-FW-EX`), and the `ISP-Router`. The settings enable IP reachability, prepare the network for NAT, VPN operations, and establish static routes to ensure proper end-to-end packet delivery.

1.3.2.1 Headquarters Firewall - (HQ-FW-EX)

This manages LAN traffic routing, NAT, and VPN termination for the Headquarters network.

```cli
configure terminal or conf t

! --- Interface Configuration ---
interface GigabitEthernet0/0/0
 ip address 203.0.113.6 255.255.255.252
 ip nat outside
 duplex auto
 speed auto
 no shutdown
exit

interface GigabitEthernet0/0/1
 ip address 10.0.0.2 255.255.255.252  router
 ip nat inside
 duplex auto
 speed auto
 no shutdown
exit



! --- Static Routing ---
ip route 0.0.0.0 0.0.0.0 203.0.113.5
ip route 192.168.10.0 255.255.255.0 10.0.0.1
ip route 192.168.20.0 255.255.255.0 10.0.0.1
ip route 192.168.30.0 255.255.255.0 10.0.0.1
ip route 192.168.41.0 255.255.255.0 10.0.0.1
ip route 192.168.50.0 255.255.255.0 10.0.0.1

end
write memory
```

1.3.2.2 Branch Office Firewall - (BO-FW-EX)

This router serves as the VPN peer in the Branch Office and handles traffic from its internal LAN.

```
cli

configure terminal or conf t

! --- Interface Configuration ---
interface GigabitEthernet0/0/0
 ip address 192.168.2.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
 no shutdown
exit

interface GigabitEthernet0/0/1
ip address 203.0.113.2 255.255.255.252
 ip nat outside
 duplex auto
 speed auto
 no shutdown
exit

! --- Static Routing ---
ip route 0.0.0.0 0.0.0.0 203.0.113.1

end
write memory
```

1.3.2.3 ISP Router - (Internet Transit Device)

The ISP router acts as the bridge between the Branch Office and Headquarters networks, forwarding public traffic.

cli

```
configure terminal
! --- Interface Configuration ---
interface GigabitEthernet0/0/0
 ip address 203.0.113.1 255.255.255.252
 duplex auto
 speed auto
 no shutdown
exit

interface GigabitEthernet0/0/1
 ip address 203.0.113.5 255.255.255.252
 duplex auto
 speed auto
 no shutdown
exit

! --- Static Routing ---
ip route 192.168.2.0 255.255.255.0 203.0.113.2
ip route 192.168.10.0 255.255.255.0 203.0.113.6
ip route 192.168.20.0 255.255.255.0 203.0.113.6
ip route 192.168.30.0 255.255.255.0 203.0.113.6
ip route 192.168.41.0 255.255.255.0 203.0.113.6
ip route 192.168.50.0 255.255.255.0 203.0.113.6

end
write memory
```

1.3.3 NAT Configuration and VPN Traffic Exemption

This section outlines the NAT settings applied to both edge routers. NAT allows internal devices to access external networks using public IPs. However, for the VPN to function correctly, **specific traffic must be able to bypass NAT**. This is accomplished using extended access control lists (ACLs) to define and exempt "interesting traffic" destined for the VPN tunnel.

1.3.3.1 NAT and VPN Bypass Rules (HQ-FW-EX)

This router handles NAT for outbound internet access and excludes VPN-bound traffic using an external ACL.

cli

```
configure terminal
! --- Standard NAT Rule for General Internet Access ---
access-list 100 permit ip 192.168.10.0 0.0.0.255 any
access-list 100 permit ip 192.168.20.0 0.0.0.255 any
access-list 100 permit ip 192.168.30.0 0.0.0.255 any
access-list 100 permit ip 192.168.41.0 0.0.0.255 any
access-list 100 permit ip 192.168.50.0 0.0.0.255 any

! --- Extended ACL to Exempt VPN Traffic from NAT ---
ip access-list extended NO_NAT_VPN_TRAFFIC_TO
 deny ip 192.168.10.0 0.0.0.255 192.168.2.0 0.0.0.255
 deny ip 192.168.20.0 0.0.0.255 192.168.2.0 0.0.0.255
 deny ip 192.168.30.0 0.0.0.255 192.168.2.0 0.0.0.255
 deny ip 192.168.41.0 0.0.0.255 192.168.2.0 0.0.0.255
 deny ip 192.168.50.0 0.0.0.255 192.168.2.0 0.0.0.255
 permit ip any any

! Apply NAT with VPN exemption ---
ip nat inside source list NO_NAT_VPN_TRAFFIC_TO interface
GigabitEthernet0/0/0 overload

end
write memory
```

1.3.3.2 NAT and VPN Bypass Rules (BO-FW-EX)

The router uses a similar approach, applying NAT for general outbound traffic while exempting VPN traffic destined for Headquarters subnets.

```cli
configure terminal
! --- Standard NAT Rule for General Internet Access ---
access-list 100 permit ip 192.168.2.0 0.0.0.255 any

! --- Extended ACL to Exempt VPN Traffic from NAT ---
ip access-list extended NO_NAT_VPN_TRAFFIC
 deny ip 192.168.2.0 0.0.0.255 192.168.10.0 0.0.0.255
 deny ip 192.168.2.0 0.0.0.255 192.168.20.0 0.0.0.255
 deny ip 192.168.2.0 0.0.0.255 192.168.30.0 0.0.0.255
 deny ip 192.168.2.0 0.0.0.255 192.168.41.0 0.0.0.255
 deny ip 192.168.2.0 0.0.0.255 192.168.50.0 0.0.0.255
 permit ip any any

! Apply NAT with VPN exemption ---
ip nat inside source list NO_NAT_VPN_TRAFFIC interface
GigabitEthernet0/0/1 overload

end
write memory
```

1.3.4 ISAKMP (Phase 1) Policy Configuration

This section defines **ISAKMP Phase 1 security parameters** used to establish a secure tunnel between the Headquarters (`HQ-FW-EX`) and the Branch Office (`BO-FW-EX`) firewall routers. The ISAKMP policy ensures both devices agree on foundational key exchange settings before proceeding to IPSec Phase 2 negotiations.

Key attributes configured:

- **Encryption**: AES
- **Authentication**: Pre-shared key
- **Diffie-Hellman Group**: Group 5
- **Hashing Algorithm**: SHA
- **Lifetime**: 86400 seconds

To avoid legacy misconfigurations or simulator-induced residual states, all existing ISAKMP policies and keys were explicitly cleared before applying the updated configuration.

> ***Note on Simulator Behavior:*** *During initial testing, attempts to configure* `hash sha256` *failed. See Section 1.4.2.1 for details on this workaround.*

1.3.4.1 ISAKMP Configuration (HQ-FW-EX)

```cli
configure terminal
! Clear any existing Phase 1 configuration
no crypto isakmp policy 10
no crypto isakmp key MCSI_SecureVPN2025! address 203.0.113.2

! Define updated ISAKMP Policy
crypto isakmp policy 10
 encryption aes
 authentication pre-share
 group 5
 hash sha
 lifetime 86400
exit
```

1.3.4.2 ISAKMP Configuration (BO-FW-EX)

```cli
configure terminal
! Remove any existing Phase 1 configuration
no crypto isakmp policy 10

! Define ISAKMP Policy
crypto isakmp policy 10
 encryption aes
 authentication pre-share
 group 5
 hash sha
 lifetime 86400
exit

! Define pre-shared key for Headquarters peer
crypto isakmp key MCSI_SecureVPN_2025! address 203.0.113.6
end
```

Note on Simulator Behavior: *During initial testing, attempts to configure* `hash sha256` *failed. See [Section 1.4.2.1](#) for details on this workaround.*

1.3.5 Crypto IPSec (Phase 2) Transform-Set Configuration

This sector defines the IPSec Phase 2 settings used to secure traffic across the VPN tunnel after it is established. The transform-set specifies how packets are encrypted and authenticated across the tunnel between Headquarters (`HQ-FW-EX`) Firewall and Branch Office (`BO-FW-EX`) Firewall.

During testing, the `mode tunnel` command repeatedly failed with `% Invalid input detected at '^' marker` error continued to persist when entered line-by-line in Cisco Packet Tracer. This was due to known limitations in the simulator's command retention behavior.

> ***Workaround Implementation:*** *See [Section 1.4.2.1](#) for details on this workaround.*

1.3.5.1 IPSec Settings (HQ-FW-EX)

```cli
configure terminal
! --- Clear any existing Phase 2 configuration
interface GigabitEthernet0/0/0
no crypto isakmp policy 10
no crypto isakmp key MCSI_SecureVPN2025! address 203.0.113.2

! --- Remove existing transform-set to ensure clean config ---
no crypto ipsec transform-set MCSI-Transform2025 esp-aes esp-sha-hmac

crypto ipsec transform-set MCSI-Transform2025 esp-aes esp-sha-hmac
exit

! --- Re-apply crypto map (will be done in step 5) ---
end
```

1.3.5.2 IPSec Settings (BO-FW-EX)

```cli
configure terminal
! Remove crypto map temporarily (required to modify transform-set)
interface GigabitEthernet0/0/1
 no crypto map MCSI-Map2025
exit

! Remove existing transform-set
no crypto ipsec transform-set MCSI-Transform2025 esp-aes esp-sha-hmac

! Define transform-set with explicit tunnel mode
crypto ipsec transform-set MCSI-Transform2025 esp-aes esp-sha-hmac
 mode tunnel
exit
end
```

1.3.6 Define ACL for Interesting Traffic

This section defines the Access Control Lists (ACLs) that determine which traffic should be protected by the IPSec tunnel. Only the traffic matching these rules (often referred to as "interesting traffic" will trigger tunnel negotiation and be encapsulated by IPSec.

To simplify troubleshooting and improve readability, custom-named ACLs (`VPN_TRAFFIC_TO` and `VPN_TRAFFIC`) were used instead of default numeric ACLs like 100 or 101. These ACLs match local-HQ-remote IP subnets on both edge routers and are later referenced in the crypto map configuration.

> ***Note:*** *For full paste consistency and to prevent simulator conflicts, ensure any legacy ACLs (e.g., numbered 100/101) are removed prior to applying the configuration.*

Headquarters Firewall (`HQ-FW-EX`)

```
cli

configure terminal or conf t
access-list extended VPN_TRAFFIC_TO
 permit ip 192.168.10.0 0.0.0.255 192.168.2.0 0.0.0.255
 permit ip 192.168.20.0 0.0.0.255 192.168.2.0 0.0.0.255
 permit ip 192.168.30.0 0.0.0.255 192.168.2.0 0.0.0.255
 permit ip 192.168.41.0 0.0.0.255 192.168.2.0 0.0.0.255
 permit ip 192.168.50.0 0.0.0.255 192.168.2.0 0.0.0.255
end
```

Branch Office Firewall (`BO-FW-EX`)

```
cli

configure terminal or conf t
access-list extended VPN_TRAFFIC
 permit ip 192.168.2.0 0.0.0.255 192.168.10.0 0.0.0.255
 permit ip 192.168.2.0 0.0.0.255 192.168.20.0 0.0.0.255
 permit ip 192.168.2.0 0.0.0.255 192.168.30.0 0.0.0.255
 permit ip 192.168.2.0 0.0.0.255 192.168.41.0 0.0.0.255
 permit ip 192.168.2.0 0.0.0.255 192.168.50.0 0.0.0.255
end
```

1.3.7 Crypto Map Definition and Interface Binding

This section defines and attaches the IPSec crypto maps that bind together all previously configured elements: ISAKMP policies (Phase 1), transform-sets (Phase 2), and ACLs for interesting traffic. The crypto map is applied directly to the appropriate WAN-facing interface on each edge device to activate IPSec tunnel negotiation and enforcement.

Note: *Before defining the crypto map, any existing crypto map entries should be removed to prevent misconfigurations.*

Headquarters Firewall (HQ-FW-EX)

```cli
configure terminal or conf t
! Remove any existing crypto map instance for a clean start
no crypto map MCSI-Map2025 10 ipsec-isakmp

! Define crypto map and bind relevant components
crypto map MCSI-Map2025 10 ipsec-isakmp
 set peer 203.0.113.2
 set pfs group5
 set security-association lifetime seconds 86400
 set transform-set MCSI-Transform2025
 match address VPN_TRAFFIC_TO
exit

! Apply the crypto map to the external interface
interface GigabitEthernet0/0/0
 crypto map MCSI-Map2025
end
write memory
```

Branch Office Firewall (`BO-FW-EX`)

```cli
configure terminal

! Remove any existing crypto map instance for a clean start
no crypto map MCSI-Map2025 10 ipsec-isakmp


! Define crypto map and bind relevant components
crypto map MCSI-Map2025 10 ipsec-isakmp
 set peer 203.0.113.6
 set pfs group5
 set security-association lifetime seconds 86400
 set transform-set MCSI-Transform2025
 match address VPN_TRAFFIC
exit

! Apply the crypto map to the external interface
interface GigabitEthernet0/0/1
 crypto map MCSI-Map2025
end
write memory
```

Summary: *Crypto maps were applied on `HQ-FW-EX` (Gi0/0/0) and `BO-FW-EX` (Gi0/0/1), using transform-set `MCSI-Transform2025` and ACLs `VPN_TRAFFIC_TO` / `VPN_TRAFFIC`.*

1.4 VPN Deployment Challenges and Troubleshooting Log

During the complex implementation and validation of the IPsec tunnel in Cisco Packet Tracer, a major challenge arose that necessitated persistent and methodical troubleshooting. This challenge revealed the unique complexities of working within a simulated environment.

Problem 1: Simulator Limitations and Non-Standard Configuration

Problem: The biggest challenge was adapting to real-world best practices due to simulation limitations. At first, I used a couple of ASA (Adaptive Security Appliances) device model `5505` for firewalling. To allow ICMP traffic, I had to create a special access list and remove NAT on the ASAs. This workaround was needed for the simulation to work. But it made it unrealistic. Eventually, I replaced the ASAs with `ISR4331` routers acting as firewalls to finish the configuration.

Impact: This showed an important difference between real network devices, design, and simulation comparisons. It forced me to document a non-standard setup. I learned that real network devices are more functionally accepting with more reliable command outputs.

Problem 2: Packet Tracer CLI and Configuration Instability

- **Problem:** The simulation environment often behaved unpredictably. I saw many “`% Invalid input detected at '^' marker`” errors, even with correct commands. This meant internal parser bugs were causing problems. Also, critical commands like `mode tunnel` inside the crypto transform set were accepted but did not save in the running config. The simulator dropped or misapplied these commands silently. To fix this, I stopped entering commands line-by-line. Instead, I used full configuration blocks pasted at once to make sure all settings, including `mode tunnel`, were applied.

  - **Workaround: Full Block Paste via CLI**

    To fix the problem where commands didn’t apply or stick properly, I used a full copy-paste method with pre-written configuration blocks. This made sure key settings—like `hash sha256` in the transform-set and NAT exemption rules—were saved correctly.

- **What I Did:**
  - **Routers Affected:** Headquarters Firewall (`HQ-FW-EX`) and Branch Office Firewall (`BO-FW-EX`)
  - **Problem:** Singular command line typing caused missing or dropped commands.
  - **Fix:** I created complete command blocks and pasted them into the router's CLI in one go.
- **Impact:** This method helped get around Packet Tracer bugs by avoiding line-by-line input. It stopped issues like the CLI skipping prompts or not recognizing commands. The next sections show the full configs used for both routers. These can be reused or rolled back if needed. This approach made the tunnel setup more stable across multiple test runs.

Problem 3: Hidden `no ip cef` Command and NAT Troubleshooting

- **Problem:** A major roadblock was a hidden `no ip cef` command breaking NAT silently. After setting IPs and routes right, pings to public IPs worked. But the packets did not translate properly. I had to dig deep into routing and config to find and remove this `no ip cef` command. That fixed the NAT problem.
- **Impact:** This showed how a single command, even if unrelated, can cause big network problems. It was a key moment in my troubleshooting. It taught me to review configs deeply, not just surface settings.

Problem 4: Critical Crypto Parameter Non-Persistence

- **Problem:** Another hard issue was that advanced crypto settings—like `hash sha256`, `lifetime 86400`, and certain transform sets—did not save on both routers. They seemed accepted, but vanished from running configs. I switched to full-text block inputs for all crypto settings to get them saved.

- **Impact:** This method also helped get around Packet Tracer bugs by avoiding `“% Invalid input detected at '^' marker”` errors. I had to lower crypto settings (e.g., to `hash sha` and `esp-sha-hmac`) to make sure commands stayed, then updated with full text block commands accordingly. This showed me the importance of checking command persistence and adapting when needed in simulators.

Problem 5: VPN Negotiation Failures and Simulator Quirks

- **Problem:** The IPSec tunnel kept failing to start Phase 1. The command `show crypto isakmp sa` showed states like `MM_NO_STATE` and `ACTIVE (deleted)`. This meant a security association (SA) was formed, but then dropped immediately. The Headquarters Firewall (`HQ-FW-EX`) sometimes showed no ISAKMP SA entries at all.

- **Impact:** Without a stable Phase 1, no key exchange could finish. No encrypted traffic passed. This caused `show crypto ipsec sa` to report zero packets encrypted. I had to run deep diagnostics to prove my config was correct, and the simulator was giving false status outputs.

Problem 6: Unrelated Local LAN Connectivity Issues

- **Problem:** During testing, I found a persistent Layer 2/ARP problem on the Branch Office Firewall’s (`BO-FW-EX`) public link (203.0.113.2/30→Gig0/0/1). To fix this, I replaced the `ISR2911` router with a fresh `ISR4331` in the topology.

- **Impact:** Though unrelated to the IPSec tunnel, this problem slowed my troubleshooting. It taught me to isolate issues and not to let one problem block overall progress.

Problem 7: Misinterpretation of Traceroute Behavior and Resulting Troubleshooting Loop

- ➢ **Problem:** The primary issue was a persistent failure of the `traceroute` command to show intermediate hops between the Branch Office and Headquarters networks. The traceroute output showed `Request timed out` messages for the hops on the public internet, but the final destination was always reachable.
- ➢ **Impact:** This behavior was initially misinterpreted as a failure in the VPN configuration. The assumption was that a correctly configured IPSec tunnel should not produce timeouts and that every hop should be visible. This led to a series of flawed troubleshooting attempts aimed at forcing the `traceroute` to show all hops, which broke the working IPSec tunnel.

1.4.1 Flawed Troubleshooting Efforts

Based on the initial misinterpretation, a series of incorrect corrective actions were attempted, including:

- **Permitting ICMP traffic:** I attempted to create and apply new access control lists (ACLs) to explicitly allow ICMP traffic through the firewalls.
- **Modifying VPN ACLs:** I provided commands to alter the `VPN_TRAFFIC` ACLs to allow ICMP through the encrypted tunnel.
- **Resetting Configurations:** When these changes led to a complete loss of network connectivity, I provided commands to reset the router configurations, which temporarily restored the IPSec tunnel but did not solve the traceroute issue.

These efforts created more problems than they solved, culminating in a complete loss of ping and `tracert` connectivity, as the core issue was never addressed.

1.4.2 Root Cause Discovery and Final Resolution

The true root cause of the issue was not a VPN misconfiguration, but a fundamental misunderstanding of how a secure IPsec VPN should behave when a diagnostic tool like `traceroute` is used. The `Request timed out` messages were, in fact, the correct and expected behavior for a secure tunnel.

- **The Nature of `Traceroute`:** The `traceroute` command relies on ICMP Time Exceeded packets being returned from each router along the path.
- **The Nature of an IPsec VPN:** An IPsec tunnel encrypts the entire packet, including the ICMP Time Exceeded messages, preventing intermediate routers from inspecting the packet's contents. As a result, the intermediate routers drop the packet and cannot send back a Time Exceeded message, causing a timeout.

The final breakthrough came when it was discovered that the core network infrastructure was functioning correctly, and the issue was an end-device misconfiguration that was not correctly performing the traceroute. The `tracert` output showing timeouts on the intermediate hops but success at the final destination was proof that the VPN tunnel was properly encrypting traffic.

The definitive solution was to stop attempting to alter the working VPN and to restore the firewalls to a correct and secure configuration. This involved applying the crypto map to the external interfaces again, ensuring the VPN traffic was correctly encrypted, and confirming that the `ping` and `tracert` commands from a properly configured PC validated a working tunnel.

1.5 Tunnel Traffic Initiation and Final Checks

To test and activate the IPsec tunnel, I sent pings (ICMP echo requests) between two computers on different networks:

- **From** HQ-PC (`192.168.10.100`)**:** `ping 192.168.2.100`
- **From** BO-PC (`192.168.2.100`)**:** `ping 192.168.10.100`

At first, the pings may have failed while the IPSec tunnel was being built. After that, repeated ping attempts were successful. This confirmed that the two private networks — Headquarters and Branch Office — were connected securely through the tunnel.

1.5.1 Tunnel Verification Commands

To check that the VPN tunnel was working, I ran the following command on both the Headquarters Firewall and the Branch Office Firewall:

```
cli

show crypto ipsec sa
```

This command showed details about encryption, security associations (SAs), and traffic flow between the networks. The output grouped results by source and destination subnet.

Device	Packets Encrypted	Packets Decrypted	SPI (Outbound)	SPI (Inbound)	Status
HQ-FW-EX	7	7	0x1BAC53A8	0x567FA704	ACTIVE
BO-FW-EX	7	7	0x567FA704	0x1BAC53A8	ACTIVE

- **Transform Set Used:** `esp-aes 256 esp-sha-hmac`
- **Mode:** Tunnel
- **Replay Detection:** Disabled (simulator limitation)
- **Key Lifetime Remaining:** ~64,000–70,000 seconds

- This confirms **bidirectional encrypted traffic** and tunnel integrity for the primary subnet pair.

Dormant Tunnels – SAs Defined but Inactive (No Matching Traffic Yet)

These Security Associations (SAs) exist but have **not been triggered** due to a lack of “interesting traffic”:

Local Subnet (BO-FW-EX)	Remote Subnet (HQ-FW-EX)	Packets Encrypted/Decrypted	Status
192.168.2.0/24	192.168.20.0/24	0 / 0	Inactive
192.168.2.0/24	192.168.30.0/24	0 / 0	Inactive
192.168.2.0/24	192.168.41.0/24	0 / 0	Inactive
192.168.2.0/24	192.168.50.0/24	0 / 0	Inactive

- These subnet pairs are fully defined in ACLs and crypto maps.
- Here is how the IOS acts: **IPsec Phase 2 tunnels do not come alive until traffic flows** between the matched subnets.
- To usher in traffic (e.g., `ping` or `traceroute`) from those subnets would activate the respective SAs.

Summary & Operational Status

- The **Phase 2 IPsec VPN tunnel** is active and working correctly for the tested subnet pair: `192.168.10.0/24` ↔ `192.168.2.0/24`.
- This is confirmed by **increasing the encrypt and decrypt counters** on both devices.
- Other subnet pairs are also configured properly but are currently inactive. This is expected, since no traffic has been sent from those networks.
- The current setup supports **on-demand SA creation** for all defined subnet pairs — meaning the tunnel will activate automatically when traffic is initiated.

2.0 CONCLUSION

2.1 Final VPN Status Verification and Wrap-Up

This section confirms the troubleshooting process concluded with the successful deployment and verification of the IPsec site-HQ-site VPN tunnel. The final outputs confirmed:

- **Pinging the destination:** The pings were successful from both ends of the tunnel, indicating that Layer 3 connectivity had been restored.

- **Validating the `tracert`:** The `tracert` output showed `Request timed out` for intermediate hops, but successfully reached the final destination. This output confirmed that the VPN was functioning securely by encrypting all traffic, as expected.

This project reinforced the critical skill of how secure networks should behave. It highlighted the importance of a step-by-step, systematic troubleshooting approach. I learned to trust the foundational principles of network security even when simulated tools gave unclear results.

This experience aligns with the "Advanced Beginner" level of the ASD Cyber Skills Framework. It proves my ability to troubleshoot misconfigurations. I can also write and produce clear, structured technical documents. Plus, I can show a working solution using command-line outputs.

2.1.1 Traceroute Verification

The first clear sign of IPSec tunnel success came from a traceroute test. I ran this test from `HQ-PC1` and aimed it at the Branch Office gateway (`BO-FW-EX`). The traceroute showed that packets were being routed correctly through the encrypted tunnel. It also bypassed the ISP router, which confirmed that the tunnel was active and functioning properly.

> ***Note**: This live routing result helped resolve any confusion caused by earlier simulator issues. It confirmed the IPSec tunnel was working.*

2.1.2 Validation via `show crypto` Commands

Next, I ran the following CLI commands on both the Headquarters and Branch Office firewalls:

- `show crypto isakmp sa`
- `show crypto ipsec sa`

Headquarters Firewall (`HQ-FW-EX`) Results

- *Outgoing traffic was being encrypted.*
- *Tunnel status showed as **ACTIVE**.*
- *Matching transform-sets and SPI values were confirmed.*

Branch Office Firewall (`BO-FW-EX`) Results

- *Inbound traffic was being decrypted properly.*
- *Packet counters showed traffic was being received and processed securely.*
- *Security Associations (SAs) matched the Headquarters firewall's output.*

> ***Note**: Both firewalls showed nearly identical counters, matching settings, and active tunnel status—confirming full end-HQ-end encryption and decryption were working.*

Final Reflection

This project demonstrated the importance of testing a network setup using multiple tools. Even in a lab with limited features, I was able to confirm VPN functionality using simple commands and step-by-step checks. Using traceroute to test packet flow and then checking encryption status with `show crypto` gave me strong proof that the tunnel worked.

> **Takeaway**: Don't depend on just one method. Use both command-line checks and live network testing together to make sure your IPSec tunnel is up and working.
