SHRI RAMDEOBABA COLLEGE OF ENGINEERING AND MANAGEMENT,
NAGPUR.

Computer Network Lab Mini Project Report
(6TH SEM, SESSION 2024-25, ECT 357)

“Site-to-Site IPsec VPN Configuration on Cisco ASA Firewall”

Submitted By
Batch: A1
Aditi Thakre (Roll No.-02)
Bhumi Shah (Roll No.-07)

Guide Name: Prof. Puja Agrawal

Department of Electronics and Communication Engineering

Contents

1. Introduction :

In today's interconnected business environment, organizations frequently need to establish secure communications between geographically dispersed locations. Site-to-site VPNs provide a cost-effective solution by creating encrypted tunnels over public networks like the internet, eliminating the need for expensive dedicated leased lines. This project demonstrates the implementation of a site-to-site IPsec VPN between headquarters (HQ) and branch offices using Cisco ASA firewalls.

The demonstrated configuration establishes a secure tunnel that creates a virtual connection between two physically separate networks, allowing resources to be shared securely across locations. This approach is particularly valuable for organizations that need to maintain security while connecting multiple office locations. The implementation uses Cisco ASA 5506 firewalls, which are purpose-built security appliances designed to provide comprehensive protection for network environments1.

The configuration includes not only the VPN tunnel itself but also proper routing, access controls, and security policies to ensure that only authorized traffic traverses the tunnel while maintaining security boundaries between internal and external networks. By implementing this solution, organizations can ensure that sensitive data remains protected when transmitted between locations while allowing necessary business communications to continue unimpeded.

2. Objectives of the project

The primary goal of this project is to establish secure communication between headquarters and branch networks using Cisco ASA firewalls. This involves several specific objectives that collectively contribute to creating a robust, secure networking environment:

Secure Network Connectivity
The foremost objective is to establish encrypted communication between the HQ and branch networks, ensuring that all data transmitted between these locations remains confidential and protected from interception. As stated in the tutorial, "The objective here is to obtain a secure communication between HQ and the branch Network"1. This encrypted connection must protect all traffic originating from either location when crossing the public network (represented by the ISP in the demonstration).

Implementation of IPsec VPN

The project specifically aims to implement an IPsec VPN tunnel between two Cisco ASA 5506 firewalls. IPsec (Internet Protocol Security) provides a framework for secure IP communications by authenticating and encrypting each IP packet during a communication session. The tutorial emphasizes this objective: "We Implement IPsec VPN between the two firewalls such that any communication originating from HQ to branch is encrypted and secured, and vice versa"1.

Proper Network Segmentation and Security
Another key objective is to configure appropriate network segmentation with distinct security zones (inside and outside) on each firewall. This segmentation helps maintain proper security boundaries between trusted internal networks and untrusted external networks. The project demonstrates configuring security levels (100 for inside networks, 0 for outside networks) to enforce these boundaries1.

Functional Routing Between Networks
The configuration must ensure proper routing between the networks, allowing devices on one network to communicate with devices on the remote network. This includes implementing OSPF (Open Shortest Path First) routing protocol on both the firewalls and intermediate routers to establish dynamic routing paths across the network infrastructure1.

Inspection and Access Policies
A critical objective is to implement appropriate inspection policies and access control lists (ACLs) that allow only specific authorized traffic types to traverse the VPN tunnel. The project demonstrates configuring access lists to permit ICMP (ping) and web traffic (HTTP/HTTPS) while implicitly denying other traffic types1.

3. Important concepts used in the Mini Project

Cisco ASA Firewall Architecture

The Cisco Adaptive Security Appliance (ASA) is a security device that combines firewall, VPN concentrator, and intrusion prevention capabilities. ASA firewalls operate using a security-level concept where interfaces are assigned security levels from 0 (least trusted) to 100 (most trusted). By default, traffic is allowed to flow from higher security levels to lower security levels but blocked in the reverse direction unless explicitly permitted1.

Network Interface Security Zones

In the ASA architecture, interfaces are categorized into security zones that determine traffic flow permissions:

- **Inside interface**: Assigned security level 100, typically connected to the trusted internal network
- **Outside interface**: Assigned security level 0, typically connected to untrusted networks like the internet
- **DMZ interface**: (Not used in this project but commonly configured) Typically assigned an intermediate security level for partially trusted services1

Network Address Translation (NAT)

NAT is a critical concept implemented in this project through object networks. The configuration demonstrates using NAT to allow internal private IP addresses to be translated when communicating across the VPN. This is configured using the "object network" command followed by the "nat" command specifying the translation parameters1.

Access Control Lists (ACLs)

ACLs are used to create inspection policies that filter traffic based on specific criteria. In this project, extended ACLs are configured to permit specific traffic types (ICMP and TCP ports 80/443) while implicitly denying all other traffic. These ACLs are then bound to interfaces using the "access-group" command to enforce the policy at specific network entry points1.

Open Shortest Path First (OSPF) Routing Protocol

OSPF is a link-state routing protocol used in the project to dynamically share routing information between network devices. The configuration demonstrates implementing OSPF on both the ASA firewalls and the interconnecting routers to ensure proper routing table construction and maintenance. OSPF enables the networks to automatically learn paths to remote networks and adapt to topology changes1.

IPsec VPN Concepts

IPsec (Internet Protocol Security) is a framework of open standards that provides secure, encrypted communications over IP networks. Key IPsec concepts employed in this project include:

- **Encryption**: Protecting data confidentiality by making it unreadable to unauthorized parties
- **Authentication**: Verifying the identity of communicating parties
- **Tunneling**: Encapsulating original IP packets within new IP packets for secure transmission

- **Key exchange**: Establishing shared encryption keys securely between VPN endpoints1

Default Static Routes

Default static routes are configured on the ASA firewalls to direct traffic destined for unknown networks to the next-hop router (in this case, the ISP router). This ensures that traffic destined for remote networks can properly leave the local network through the appropriate gateway

4. Configuration of major components used

Sr. No.	Device name	IP Configuration	Subnet mask	Default gateway	DNS Server
1	Router0	G0/0 100.50.10.1 G0/1 100.50.10.5	255.255.255.252	-	-
2	Router1	G0/0 100.50.10.1 G0/1 192.168.10.1	255.255.255.252 255.255.255.0	-	-
3	Router2	G0/0 10.10.10.5 G0/1 192.168.20.1	255.255.255.252 255.255.255.0	-	-
4	PC0	192.168.10.10	255.255.255.0	192.168.10.1	-
5	PC1	192.168.10.20	255.255.255.0	192.168.10.1	-
6	PC2	192.168.20.10	255.255.255.0	192.168.20.1	-
7	PC3	192.168.20.20	255.255.255.0	192.168.20.1	-

8	ASA OSPF routing	10.10.10.0 192.168.10.0	255.255.255.252 255.255.255.0	-	-
9	ASA0	G1/1 10.10.10.2 G1/2 192.168.10.2	255.255.255.252 255.255.255.0	-	-
10	ASA1	G1/1 100.50.10.2 G1/2 10.10.150.2	255.255.255.252 255.255.255.0	-	-

5. Working of Project

Traffic Flow and Routing

The site-to-site VPN solution works through several coordinated mechanisms:

1. Routing Establishment: OSPF routing protocol running on all devices (routers and ASA firewalls) ensures that each network has knowledge of remote subnets. When OSPF adjacencies form, as confirmed in the transcript showing "it has formed two neighbors"1, routing tables are populated with paths to reach remote networks.

2. Packet Processing Flow: When a computer in the HQ network (192.168.10.0/24) attempts to communicate with a device in the branch network (10.10.150.0/24), the following process occurs:

    - The packet is first routed to the HQ ASA firewall (default gateway)
    - The ASA firewall consults its routing table to determine the next hop
    - The packet is matched against VPN policies that specify which traffic should be encrypted
    - For matching traffic, the ASA encapsulates and encrypts the original packet within an IPsec tunnel
    - The encrypted packet is forwarded to the ISP router based on the default route
    - The ISP router forwards the packet to the branch ASA

- The branch ASA decrypts the packet and forwards it to the destination1

3. Access Control and Inspection: As packets traverse the firewalls, they are inspected against the configured access control lists. Only ICMP and HTTP/HTTPS traffic (TCP ports 80 and 443) is permitted based on the configured inspection policies1.

NAT Processing

The Network Address Translation configured on both ASA firewalls plays an important role in the communication process:

1. When internal hosts initiate connections to external networks, their private IP addresses are translated to the outside interface address of the respective ASA firewall.

2. This translation ensures that return traffic is properly routed back to the originating host. The "dynamic interface" parameter in the NAT configuration specifies that the outside interface IP address will be used for translation.

3. However, for VPN traffic between the sites, NAT exemptions are typically configured (though not explicitly shown in the transcript) to ensure that traffic between the internal networks is not translated when traversing the VPN tunnel. This allows direct communication between the internal IP addresses across the encrypted tunnel1.

Security Enforcement

The security model implemented in this project enforces several key principles:

1. Interface Security Levels: Traffic is permitted from higher security levels (inside - 100) to lower security levels (outside - 0) by default, but traffic in the reverse direction requires explicit permission through access lists.

2. Access Control Lists: The configured ACLs specifically permit ICMP (ping) and web traffic (HTTP/HTTPS) while implicitly denying all other traffic types. This ensures that only authorized traffic types can traverse the network.

3. Encryption: All traffic flowing between the HQ and branch networks through the VPN tunnel is encrypted, protecting it from interception or tampering while traversing the public network (ISP

6. Result and Conclusion

The final part of the configuration process involves testing end-to-end communication between the two sites. The transcript shows the beginning of a ping test from one site to the other, which would verify basic connectivity through the VPN tunnel1. While the complete test results aren't shown in the transcript, a successful implementation would demonstrate:

1. Successful ping (ICMP) connectivity between hosts on the HQ network (192.168.10.0/24) and hosts on the branch network (10.10.150.0/24)
2. Successful HTTP/HTTPS connectivity between web servers and clients across the two networks
3. Encrypted traffic transmission across the ISP network, protecting the data from unauthorized access
4. Proper routing through the established OSPF adjacencies, ensuring optimal path selection

The implementation achieves the primary objective of establishing secure, encrypted communication between two geographically separated networks using Cisco ASA firewalls and IPsec VPN technology.

7. Future Scope

Enhanced Security Features

The current implementation can be extended with additional security features to further strengthen the VPN solution:

1. **Advanced Encryption Standards**: Implementing newer encryption algorithms (such as AES-256) and stronger key exchange methods would enhance the security of the VPN tunnel against modern cryptographic attacks.
2. **IPS/IDS Integration**: Incorporating Intrusion Prevention System and Intrusion Detection System capabilities would add another layer of security by identifying and blocking malicious traffic patterns attempting to traverse the VPN.
3. **Multi-factor Authentication**: Implementing certificate-based authentication or other multi-factor authentication methods for VPN establishment would strengthen the authentication process beyond simple pre-shared keys.

Scalability Enhancements

The solution could be scaled to accommodate growing network requirements:

1. **Hub-and-Spoke VPN Topology**: Extending the current point-to-point VPN to a hub-and-spoke model would allow additional branch offices to connect securely through a central headquarters location.
2. **Route-Based VPN**: Implementing route-based VPNs instead of policy-based VPNs would provide more flexibility in routing decisions and better integration with dynamic routing protocols.

3. **High Availability Configuration**: Implementing firewall redundancy with stateful failover would ensure continuous VPN availability even in the event of hardware failures.

Advanced Management and Monitoring

Implementing comprehensive management and monitoring would improve operational efficiency:

1. **Centralized Management**: Deploying Cisco Security Manager or similar tools would enable centralized configuration, monitoring, and management of multiple ASA firewalls.
2. **Traffic Analysis and Reporting**: Implementing NetFlow or similar traffic analysis tools would provide visibility into VPN utilization, performance metrics, and potential security anomalies.
3. **Automated Deployment**: Creating templates and automation scripts for ASA configuration would streamline the deployment of consistent VPN configurations across multiple sites.

Technology Integration

Future implementations could integrate with complementary technologies:

1. **SD-WAN Integration**: Combining the IPsec VPN with Software-Defined WAN technologies would provide more intelligent path selection and traffic optimization capabilities.
2. **Cloud VPN Extensions**: Extending the VPN architecture to include connections to cloud service providers would create a comprehensive secure network encompassing on-premises and cloud resources.
3. **Zero Trust Network Access**: Implementing principles of Zero Trust architecture alongside the VPN would further enhance security by verifying every access request regardless of source location.

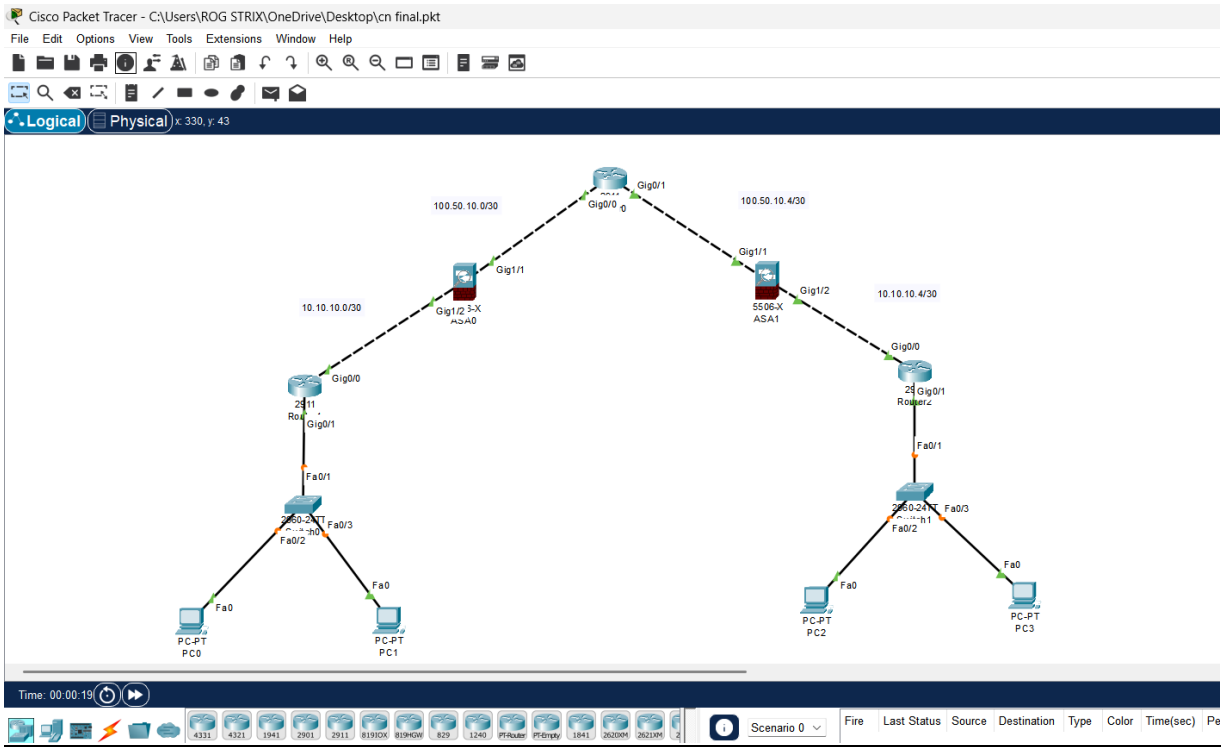
These future enhancements would build upon the solid foundation established in the current implementation, creating an even more robust, secure, and manageable inter-site communication infrastructure.

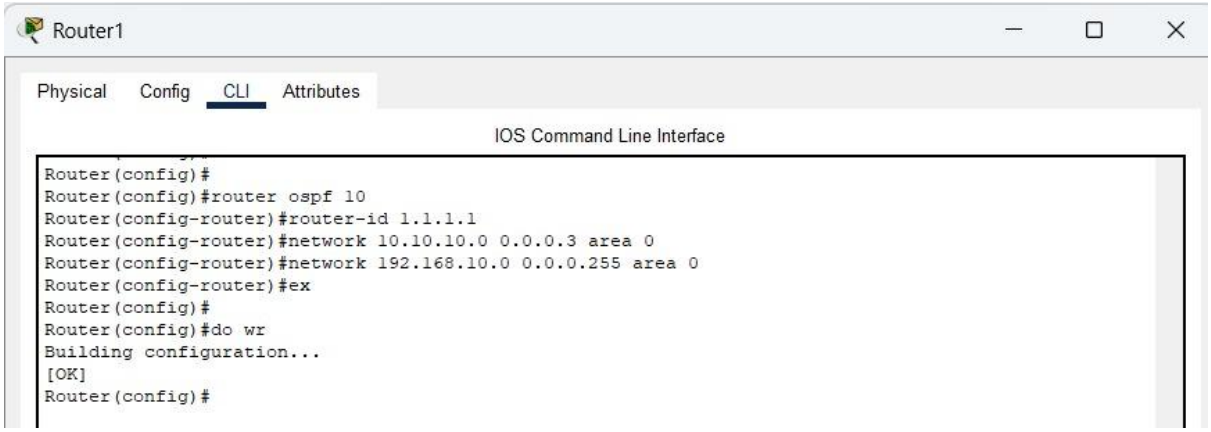
8. References

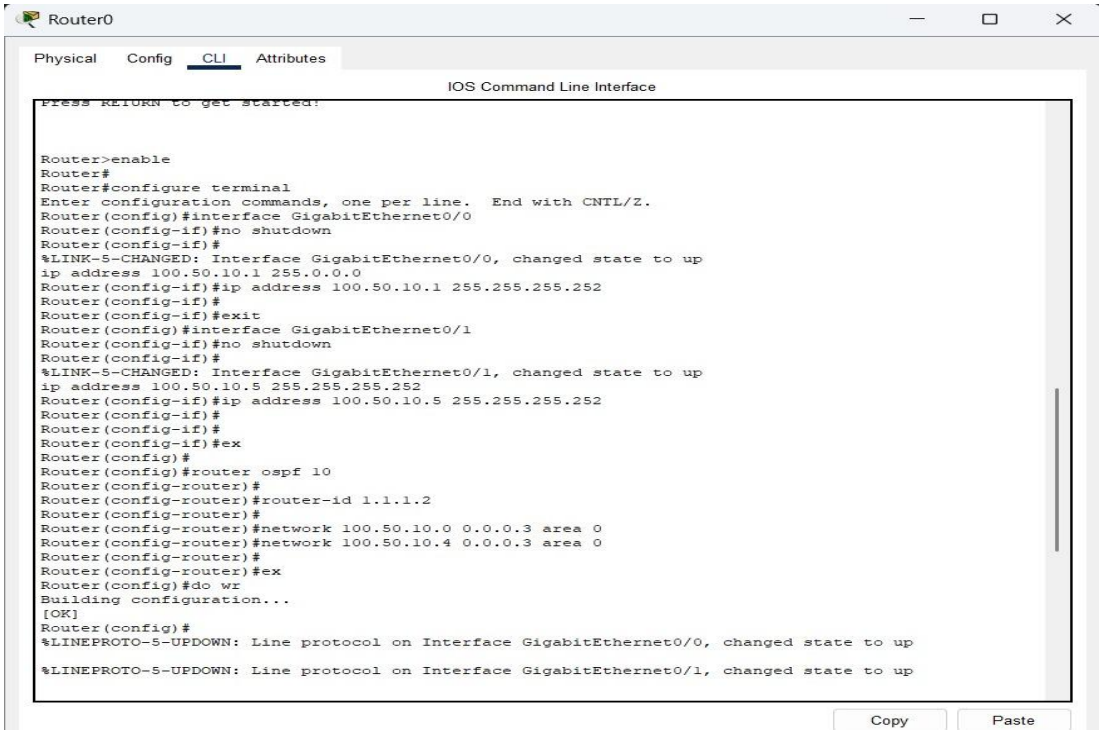
1. Cisco Systems. (n.d.). *Cisco ASA 5500-X Series Configuration Guides*. Cisco Documentation Hub. Retrieved from https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/tsd-products-support-series-home.html

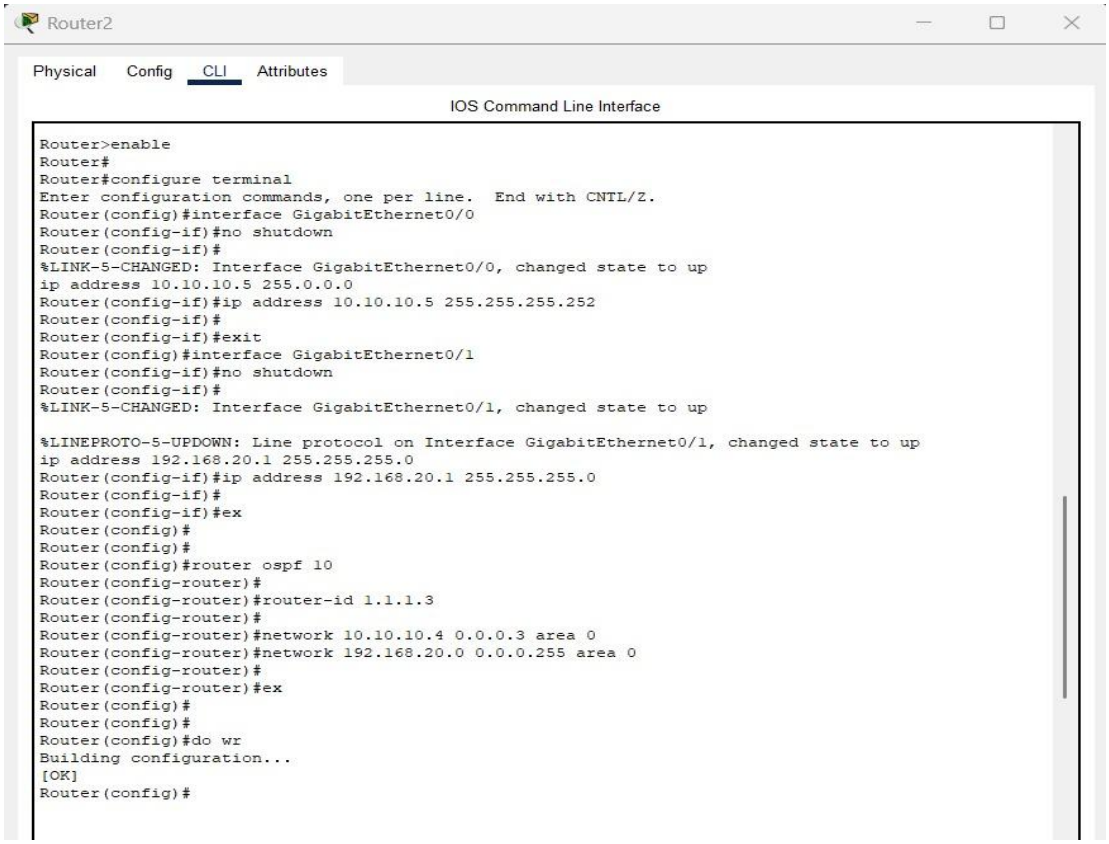
2. Cisco Systems. (n.d.). *ASA Command Reference Guide*. Retrieved from https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-command-reference-list.html

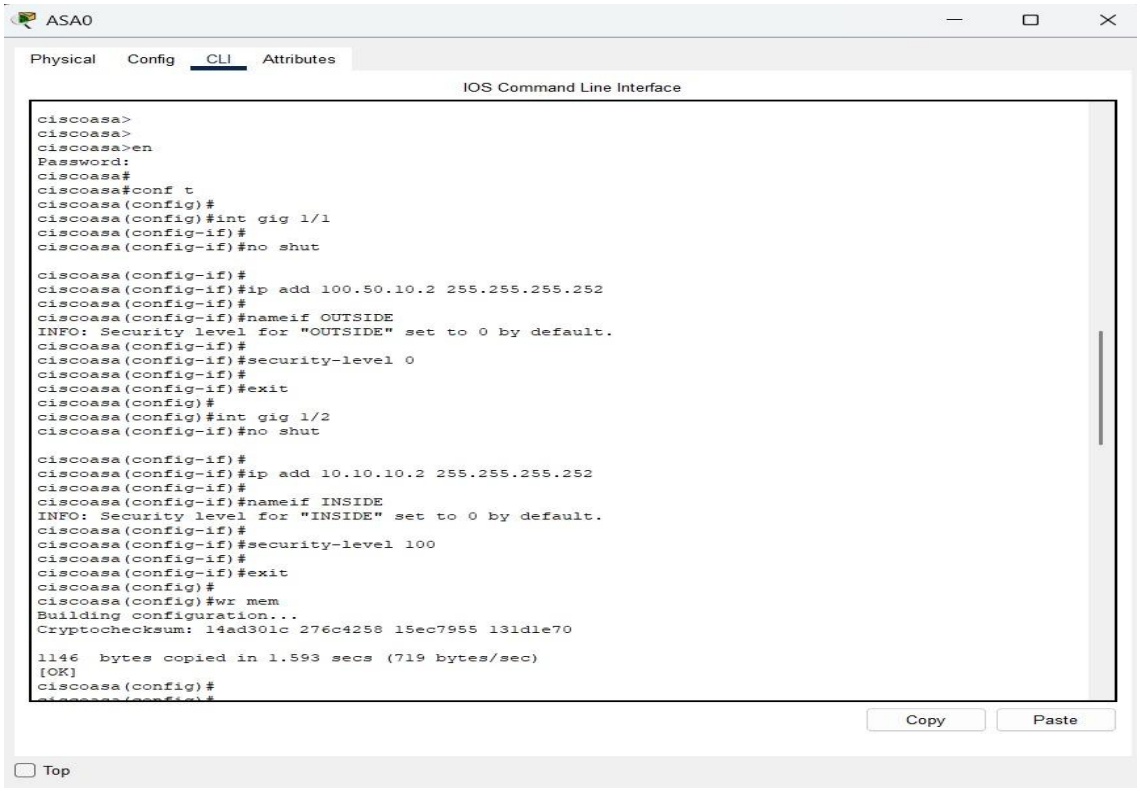
3. Cisco Systems. (n.d.). *Cisco ASA REST API Guide (9.3.2+)*. Retrieved from https://www.cisco.com/c/en/us/td/docs/security/asa/api/asa_rest_api.html

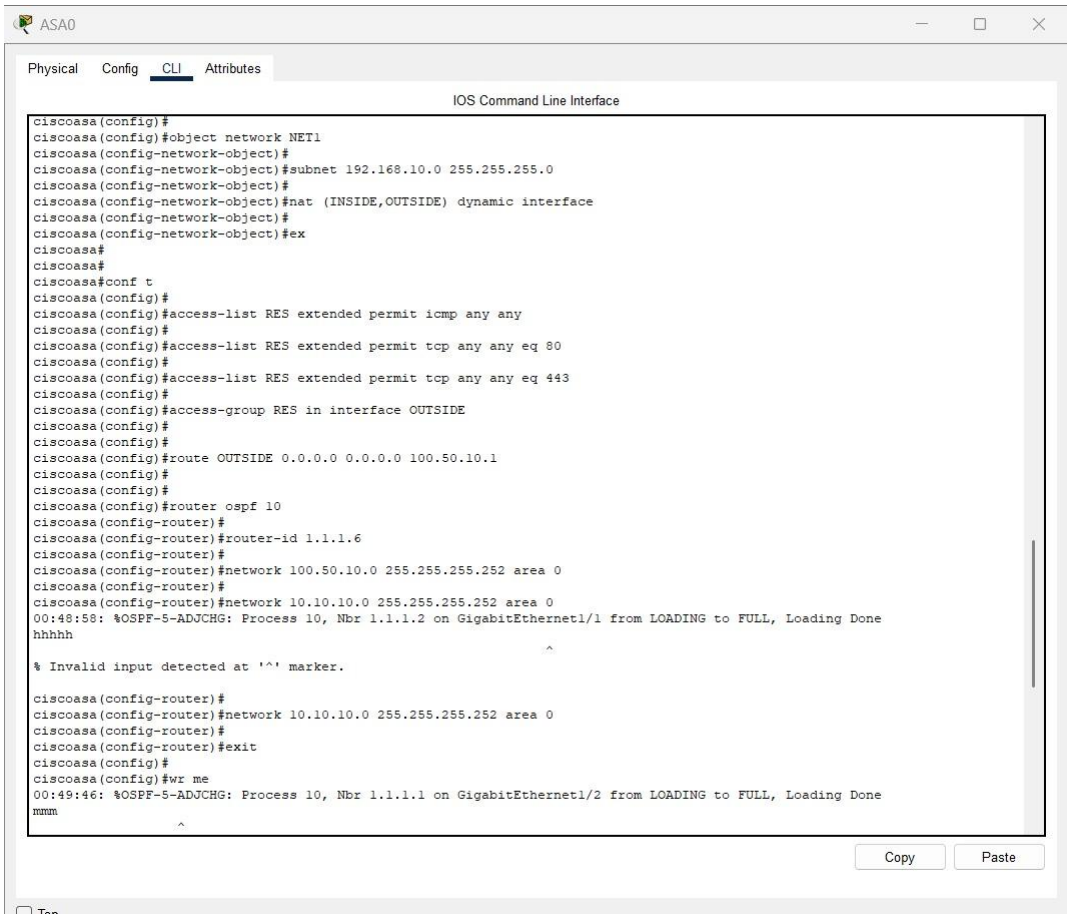


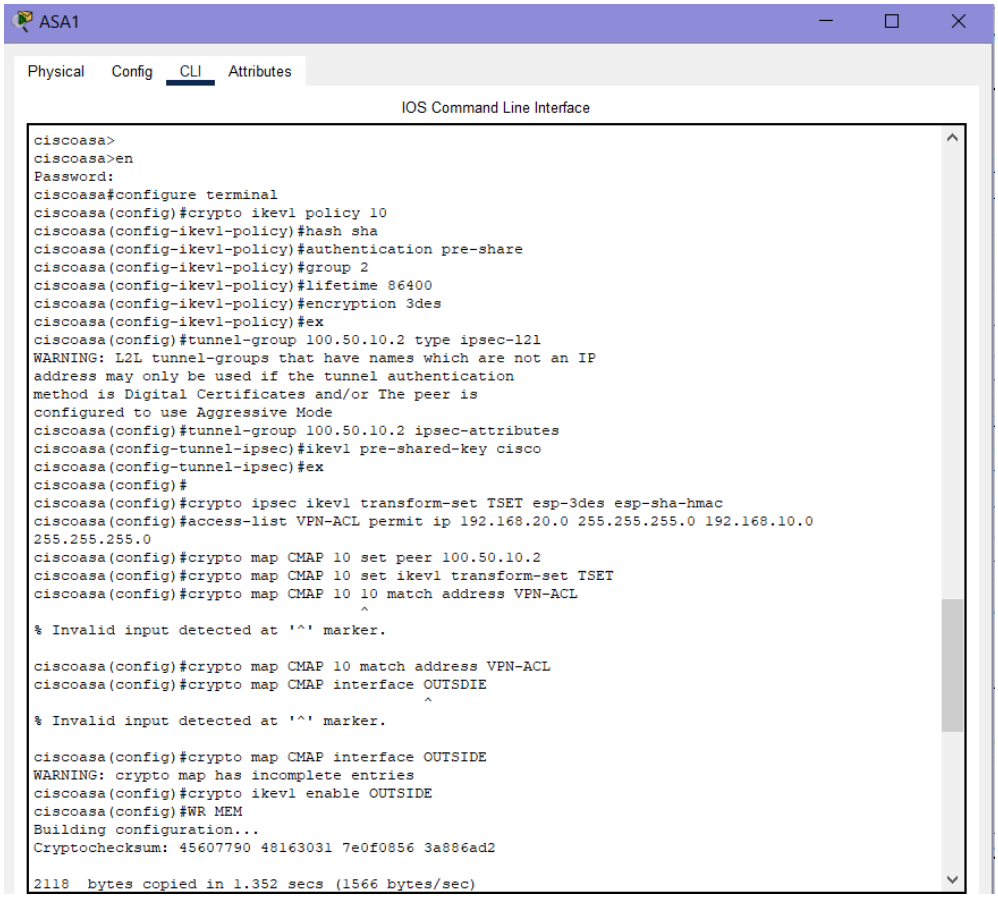

Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router(config)#
Router(config)#router ospf 10
Router(config-router)#router-id 1.1.1.1
Router(config-router)#network 10.10.10.0 0.0.0.3 area 0
Router(config-router)#network 192.168.10.0 0.0.0.255 area 0
Router(config-router)#ex
Router(config)#
Router(config)#do wr
Building configuration...
[OK]
Router(config)#

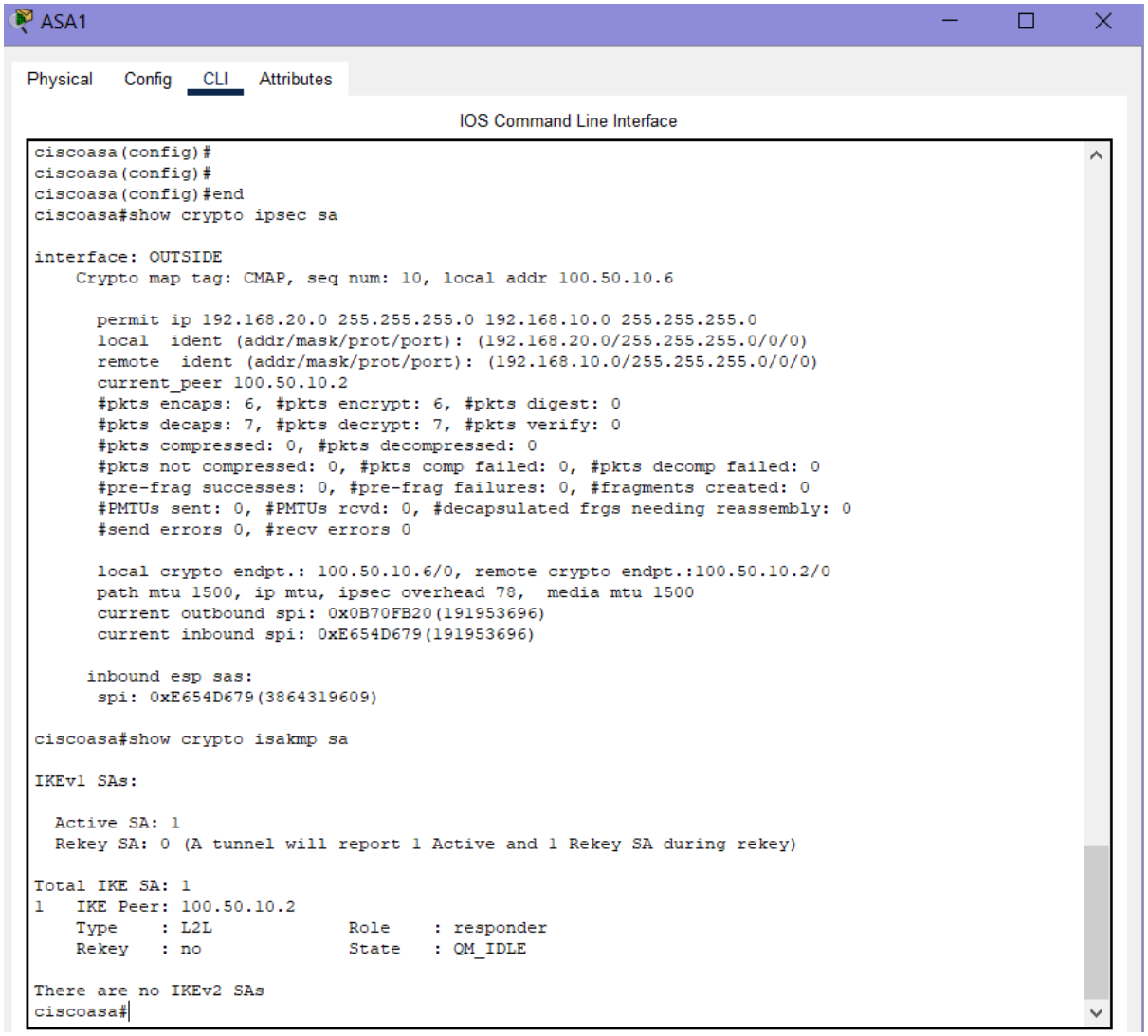

Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started!
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
ip address 100.50.10.1 255.0.0.0
Router(config-if)#ip address 100.50.10.1 255.255.255.252
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
ip address 100.50.10.5 255.255.255.252
Router(config-if)#ip address 100.50.10.5 255.255.255.252
Router(config-if)#
Router(config-if)#
Router(config-if)#ex
Router(config)#
Router(config)#router ospf 10
Router(config-router)#
Router(config-router)#router-id 1.1.1.2
Router(config-router)#
Router(config-router)#network 100.50.10.0 0.0.0.3 area 0
Router(config-router)#network 100.50.10.4 0.0.0.3 area 0
Router(config-router)#
Router(config-router)#ex
Router(config)#do wr
Building configuration...
[OK]
Router(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Copy
Paste

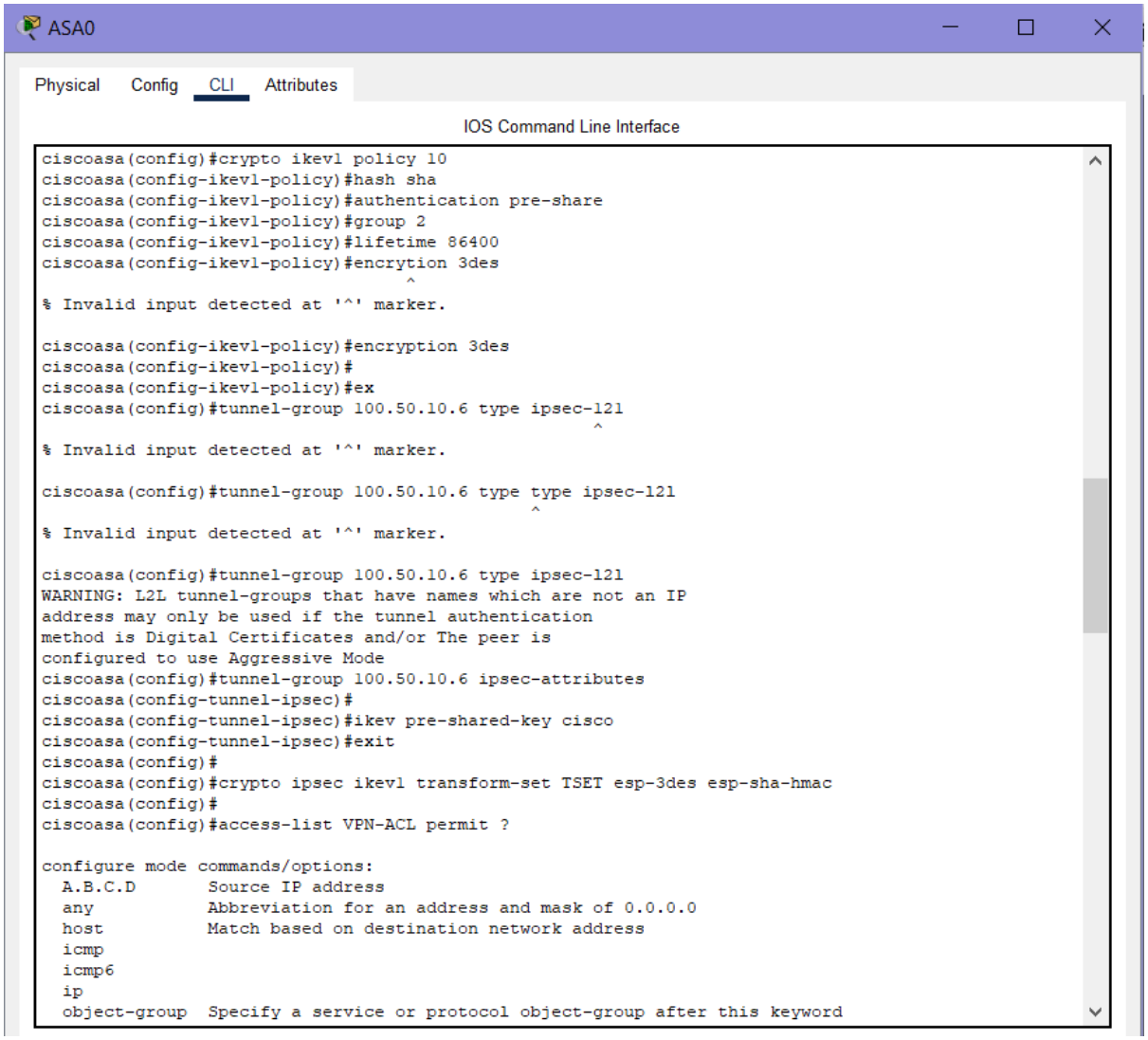

Router2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
ip address 10.10.10.5 255.0.0.0
Router(config-if)#ip address 10.10.10.5 255.255.255.252
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
ip address 192.168.20.1 255.255.255.0
Router(config-if)#ip address 192.168.20.1 255.255.255.0
Router(config-if)#
Router(config-if)#ex
Router(config)#
Router(config)#
Router(config)#router ospf 10
Router(config-router)#
Router(config-router)#router-id 1.1.1.3
Router(config-router)#
Router(config-router)#network 10.10.10.4 0.0.0.3 area 0
Router(config-router)#network 192.168.20.0 0.0.0.255 area 0
Router(config-router)#
Router(config-router)#ex
Router(config)#
Router(config)#
Router(config)#do wr
Building configuration...
[OK]
Router(config)#

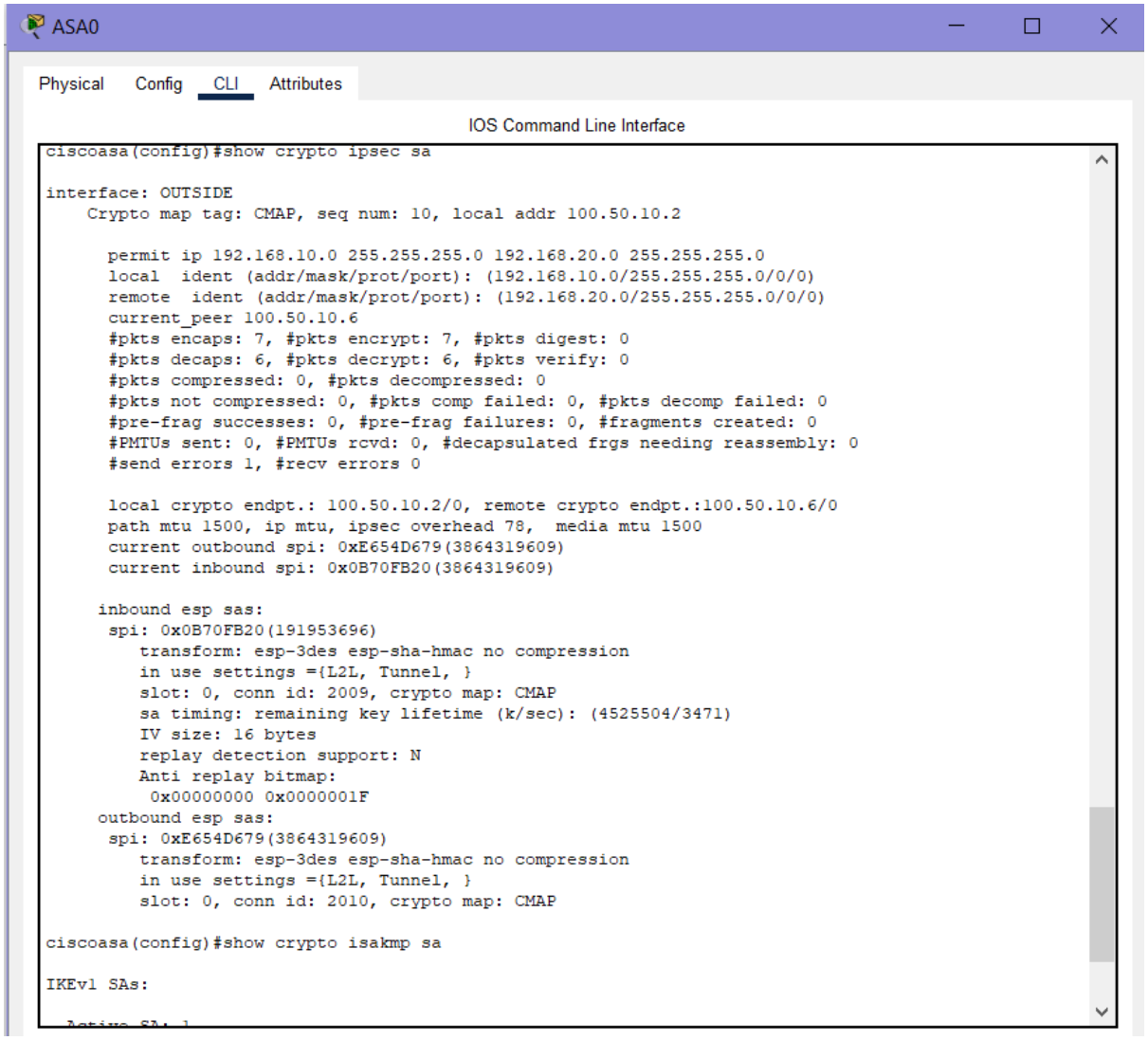

ASA0
Physical
Config
CLI
Attributes
IOS Command Line Interface
ciscoasa>
ciscoasa>
ciscoasa>en
Password:
ciscoasa#
ciscoasa#conf t
ciscoasa(config)#
ciscoasa(config)#int gig 1/1
ciscoasa(config-if)#
ciscoasa(config-if)#no shut
ciscoasa(config-if)#
ciscoasa(config-if)#ip add 100.50.10.2 255.255.255.252
ciscoasa(config-if)#
ciscoasa(config-if)#nameif OUTSIDE
INFO: Security level for "OUTSIDE" set to 0 by default.
ciscoasa(config-if)#
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#
ciscoasa(config)#int gig 1/2
ciscoasa(config-if)#no shut
ciscoasa(config-if)#
ciscoasa(config-if)#ip add 10.10.10.2 255.255.255.252
ciscoasa(config-if)#
ciscoasa(config-if)#nameif INSIDE
INFO: Security level for "INSIDE" set to 0 by default.
ciscoasa(config-if)#
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#
ciscoasa(config)#wr mem
Building configuration...
Cryptochecksum: 14ad301c 276c4258 15ec7955 131d1e70
1146 bytes copied in 1.593 secs (719 bytes/sec)
[OK]
ciscoasa(config)#
Copy
Paste
Top


ASA0
Physical
Config
CLI
Attributes
IOS Command Line Interface
ciscoasa(config)#
ciscoasa(config)#object network NET1
ciscoasa(config-network-object)#
ciscoasa(config-network-object)#subnet 192.168.10.0 255.255.255.0
ciscoasa(config-network-object)#
ciscoasa(config-network-object)#nat (INSIDE,OUTSIDE) dynamic interface
ciscoasa(config-network-object)#
ciscoasa(config-network-object)#ex
ciscoasa#
ciscoasa#
ciscoasa#conf t
ciscoasa(config)#
ciscoasa(config)#access-list RES extended permit icmp any any
ciscoasa(config)#
ciscoasa(config)#access-list RES extended permit tcp any any eq 80
ciscoasa(config)#
ciscoasa(config)#access-list RES extended permit tcp any any eq 443
ciscoasa(config)#
ciscoasa(config)#access-group RES in interface OUTSIDE
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#route OUTSIDE 0.0.0.0 0.0.0.0 100.50.10.1
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#router ospf 10
ciscoasa(config-router)#
ciscoasa(config-router)#router-id 1.1.1.6
ciscoasa(config-router)#
ciscoasa(config-router)#network 100.50.10.0 255.255.255.252 area 0
ciscoasa(config-router)#
ciscoasa(config-router)#network 10.10.10.0 255.255.255.252 area 0
00:48:58: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.2 on GigabitEthernet1/1 from LOADING to FULL, Loading Done
hhhhh
^
% Invalid input detected at '^' marker.
ciscoasa(config-router)#
ciscoasa(config-router)#network 10.10.10.0 255.255.255.252 area 0
ciscoasa(config-router)#
ciscoasa(config-router)#exit
ciscoasa(config)#
ciscoasa(config)#wr me
00:49:46: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1 on GigabitEthernet1/2 from LOADING to FULL, Loading Done
mmm
^
Copy
Paste


ASA1
Physical
Config
CLI
Attributes
IOS Command Line Interface
ciscoasa>
ciscoasa>en
Password:
ciscoasa#configure terminal
ciscoasa(config)#crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)#hash sha
ciscoasa(config-ikev1-policy)#authentication pre-share
ciscoasa(config-ikev1-policy)#group 2
ciscoasa(config-ikev1-policy)#lifetime 86400
ciscoasa(config-ikev1-policy)#encryption 3des
ciscoasa(config-ikev1-policy)#ex
ciscoasa(config)#tunnel-group 100.50.10.2 type ipsec-l2l
WARNING: L2L tunnel-groups that have names which are not an IP
address may only be used if the tunnel authentication
method is Digital Certificates and/or The peer is
configured to use Aggressive Mode
ciscoasa(config)#tunnel-group 100.50.10.2 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#ikev1 pre-shared-key cisco
ciscoasa(config-tunnel-ipsec)#ex
ciscoasa(config)#
ciscoasa(config)#crypto ipsec ikev1 transform-set TSET esp-3des esp-sha-hmac
ciscoasa(config)#access-list VPN-ACL permit ip 192.168.20.0 255.255.255.0 192.168.10.0
255.255.255.0
ciscoasa(config)#crypto map CMAP 10 set peer 100.50.10.2
ciscoasa(config)#crypto map CMAP 10 set ikev1 transform-set TSET
ciscoasa(config)#crypto map CMAP 10 10 match address VPN-ACL
^
% Invalid input detected at '^' marker.
ciscoasa(config)#crypto map CMAP 10 match address VPN-ACL
ciscoasa(config)#crypto map CMAP interface OUTSDIE
^
% Invalid input detected at '^' marker.
ciscoasa(config)#crypto map CMAP interface OUTSIDE
WARNING: crypto map has incomplete entries
ciscoasa(config)#crypto ikev1 enable OUTSIDE
ciscoasa(config)#WR MEM
Building configuration...
Cryptochecksum: 45607790 48163031 7e0f0856 3a886ad2
2118 bytes copied in 1.352 secs (1566 bytes/sec)


ASA1
Physical
Config
CLI
Attributes
IOS Command Line Interface
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#end
ciscoasa#show crypto ipsec sa
interface: OUTSIDE
Crypto map tag: CMAP, seq num: 10, local addr 100.50.10.6
permit ip 192.168.20.0 255.255.255.0 192.168.10.0 255.255.255.0
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 100.50.10.2
#pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 0
#pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors 0, #recv errors 0
local crypto endpt.: 100.50.10.6/0, remote crypto endpt.:100.50.10.2/0
path mtu 1500, ip mtu, ipsec overhead 78, media mtu 1500
current outbound spi: 0x0B70FB20(191953696)
current inbound spi: 0xE654D679(191953696)
inbound esp sas:
spi: 0xE654D679(3864319609)
ciscoasa#show crypto isakmp sa
IKEv1 SAs:
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
1 IKE Peer: 100.50.10.2
Type : L2L Role : responder
Rekey : no State : QM_IDLE
There are no IKEv2 SAs
ciscoasa#


ASA0
Physical
Config
CLI
Attributes
IOS Command Line Interface
ciscoasa(config)#crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)#hash sha
ciscoasa(config-ikev1-policy)#authentication pre-share
ciscoasa(config-ikev1-policy)#group 2
ciscoasa(config-ikev1-policy)#lifetime 86400
ciscoasa(config-ikev1-policy)#encrytion 3des
^
% Invalid input detected at '^' marker.
ciscoasa(config-ikev1-policy)#encryption 3des
ciscoasa(config-ikev1-policy)#
ciscoasa(config-ikev1-policy)#ex
ciscoasa(config)#tunnel-group 100.50.10.6 type ipsec-l21
^
% Invalid input detected at '^' marker.
ciscoasa(config)#tunnel-group 100.50.10.6 type type ipsec-l21
^
% Invalid input detected at '^' marker.
ciscoasa(config)#tunnel-group 100.50.10.6 type ipsec-l21
WARNING: L2L tunnel-groups that have names which are not an IP
address may only be used if the tunnel authentication
method is Digital Certificates and/or The peer is
configured to use Aggressive Mode
ciscoasa(config)#tunnel-group 100.50.10.6 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#
ciscoasa(config-tunnel-ipsec)#ikev pre-shared-key cisco
ciscoasa(config-tunnel-ipsec)#exit
ciscoasa(config)#
ciscoasa(config)#crypto ipsec ikev1 transform-set TSET esp-3des esp-sha-hmac
ciscoasa(config)#
ciscoasa(config)#access-list VPN-ACL permit ?
configure mode commands/options:
A.B.C.D Source IP address
any Abbreviation for an address and mask of 0.0.0.0
host Match based on destination network address
icmp
icmp6
ip
object-group Specify a service or protocol object-group after this keyword




```
ciscoasa(config)#show crypto ipsec sa

interface: OUTSIDE
    Crypto map tag: CMAP, seq num: 10, local addr 100.50.10.2

      permit ip 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0
      local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
      remote  ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
      current_peer 100.50.10.6
      #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
      #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors 1, #recv errors 0

      local crypto endpt.: 100.50.10.2/0, remote crypto endpt.:100.50.10.6/0
      path mtu 1500, ip mtu, ipsec overhead 78,  media mtu 1500
      current outbound spi: 0xE654D679(3864319609)
      current inbound spi: 0x0B70FB20(3864319609)

     inbound esp sas:
      spi: 0x0B70FB20(191953696)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, }
         slot: 0, conn id: 2009, crypto map: CMAP
         sa timing: remaining key lifetime (k/sec): (4525504/3471)
         IV size: 16 bytes
         replay detection support: N
         Anti replay bitmap:
          0x00000000 0x0000001F
     outbound esp sas:
      spi: 0xE654D679(3864319609)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, }
         slot: 0, conn id: 2010, crypto map: CMAP

ciscoasa(config)#show crypto isakmp sa

IKEv1 SAs:

  Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)

Total IKE SA: 1
1   IKE Peer: 100.50.10.6
    Type    : L2L             Role    : Initiator
    Rekey   : no              State   : QM_IDLE

There are no IKEv2 SAs
ciscoasa(config)#
```