

cisco vpn configuration guide step by step configuration of cisco vpns for asa and routers by harris andrea 2014 07 23

Published: September 27, 2026 | Index ID: #-

Introduction

In today's interconnected world, secure remote access and reliable site to site connectivity are essential for businesses of all sizes. Cisco's Adaptive Security Appliance (ASA) and its line of routers have long been the backbone of enterprise VPN solutions. Whether you're a seasoned network engineer or a junior administrator looking to deepen your knowledge, a clear, step by step approach to configuring VPNs on both ASA and router platforms is indispensable.

This article serves as a **comprehensive Cisco VPN configuration guide** that follows the methodology outlined in *"Cisco VPN Configuration Guide Step by Step Configuration of Cisco VPNs for ASA and Routers by Harris Andrea 2014 07 23."* While the original publication dates back to 2014, the core concepts remain relevant, and the instructions have been updated to reflect current best practices and the latest Cisco IOS and ASA software versions.

By the end of this guide, you will be able to:

- Set up both site to site and remote access VPNs on Cisco ASA appliances.
- Configure IPsec tunnels on Cisco routers using IOS or XR platforms.
- Apply essential security measures such as NAT exemption, access list filtering, and AAA authentication.
- Troubleshoot common connectivity problems and verify tunnel integrity.

Let's dive into the world of secure networking and build a robust VPN infrastructure that safeguards your organization's data.

Understanding Cisco VPN Fundamentals

Before we jump into configuration commands, it's helpful to grasp the foundational concepts that underpin Cisco VPNs.

What Is a VPN?

A Virtual Private Network (VPN) extends a private network across a public network, allowing users to send and receive data as if their devices were directly connected to the private network. VPNs encrypt traffic, ensuring confidentiality and integrity.

IPsec vs. SSL/TLS VPNs

While Cisco offers both IPsec (Internet Protocol Security) and SSL/TLS VPNs, the majority of site to site and remote access scenarios on ASA and routers rely on IPsec due to its strong security and performance characteristics. SSL/TLS VPNs, typically delivered through Cisco Secure Web Gateway or Cisco AnyConnect Secure Mobility Client, are more user friendly for end users but are outside the scope of this guide.

Key Terms

- Crypto Map – Associates a set of security parameters with a specific interface.
- Transform Set – Defines the cryptographic algorithms (encryption, authentication, and hashing) used in the tunnel.
- NAT Exemption – Prevents Network Address Translation from modifying VPN traffic.
- ACL (Access Control List) – Filters traffic destined for the VPN.
- AAA (Authentication, Authorization, Accounting) – Controls user access and tracks usage.

Preparing for Configuration

Successful VPN deployment requires careful planning and preparation. Below are the essential steps before you start typing commands.

Hardware and Software Requirements

1. Ensure the ASA or router model supports the desired VPN features. Refer to Cisco's product documentation for compatibility.
2. Install the latest software image that includes the necessary VPN modules. For ASA, use the asa image with the ipsec and vpn packages. For routers, use the latest IOS or XR release with the crypto and vpn packages.
3. Verify that you have a valid license for IPsec VPN. Some features, such as large scale remote access, may require an additional license.

Network Topology and Design

Draw a clear diagram of your network. Identify:

- Public IP addresses of the ASA or router interfaces that will participate in the VPN.
- Internal networks (subnets) that need to be reachable over the tunnel.
- Any firewalls or security devices that will sit between the VPN endpoints.
- Routing protocols or static routes that will direct traffic into the VPN.

Security Policies and Compliance

Define your organization's security policies regarding:

- Encryption strength (AES 256, 128, etc.).
- Authentication methods (pre shared key, digital certificates, RADIUS, TACACS+).
- Key exchange protocols (IKEv1 vs. IKEv2).
- Logging and monitoring requirements.

Step by Step Configuration on Cisco ASA

1. Accessing the ASA

Connect to the ASA via console cable, SSH, or ASDM (Adaptive Security Device Manager). For command line configuration, use:

```
ssh admin@
```

Once logged in, enter privileged EXEC mode:

```
enable
```

2. Basic Interface Configuration

Define the inside and outside interfaces and assign IP addresses:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address
```

3. Enabling VPN Features

Enable the necessary VPN services:

```
crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
!
crypto ipsec transform-set TS-1 esp-aes-256 esp-sha-hmac
 mode tunnel
!
crypto map VPN-MAP 10 match address VPN-ACL
crypto map VPN-MAP 10 set pfs
crypto map VPN-MAP 10 set peer
crypto map VPN-MAP 10 set transform-set TS-1
crypto map VPN-MAP 10 set ikev1-pre-shared-key
!
access-list VPN-ACL extended permit ip
!
interface GigabitEthernet0/0
 crypto map VPN-MAP
```

4. Configuring Pre Shared Key (PSK)

For IKEv1, define a PSK that both ends of the tunnel will share:

```
tunnel-group type ipsec-l2l
tunnel-group ipsec-attributes
 ikev1 pre-shared-key
```

5. NAT Exemption

Prevent NAT from altering VPN traffic:

```
access-list NAT-EXEMPT extended permit ip  
nat (inside) 1 0 access-list NAT-EXEMPT
```

6. AAA Authentication (Optional)

For remote access VPNs, integrate RADIUS or TACACS+:

```
aaa authentication host VPN local  
aaa authentication host VPN radius  
radius-server host auth-port 1812 acct-port 1813 key
```

7. Logging and Monitoring

Enable logging for troubleshooting:

```
logging enable  
logging trap debugging  
logging host inside
```

8. Verifying the Tunnel

Use the following commands to check tunnel status:

```
show crypto ikev1 sa  
show crypto ipsec sa  
show vpn-sessiondb detail
```

Ensure the IKE and IPsec SAs are established and that traffic is being forwarded between the two subnets.

Step by Step Configuration on Cisco Routers (IOS & XR)

1. Accessing the Router

Connect via console or SSH:

```
ssh admin@  
enable
```

2. Interface Configuration

Assign IP addresses to the interfaces that will be part of the tunnel:

```
interface GigabitEthernet0/0
 ip address
 no shutdown
!
interface GigabitEthernet0/1
 ip address
 no shutdown
```

3. Defining the Transform Set

Specify encryption and authentication algorithms:

```
crypto ipsec transform-set TS-1 esp-aes-256 esp-sha-hmac
 mode tunnel
```

4. Creating the Crypto Map

Associate the transform set with a match ACL and peer address:

```
crypto map VPN-MAP 10 ipsec-isakmp
 set peer
 set transform-set TS-1
 match address VPN-ACL
 set security-association lifetime seconds 3600
 set pfs group2
 set ikev1 pre-share-key
```

5. Applying the Crypto Map to the Interface

Attach the crypto map to the outside interface:

```
interface GigabitEthernet0/0
 crypto map VPN-MAP
```

6. Access List for Tunnel Traffic

Permit traffic that should traverse the tunnel:

```
access-list VPN-ACL extended permit ip
```

7. NAT Exemption

Exclude VPN traffic from NAT:

```
ip nat inside source list 1 interface GigabitEthernet0/0 overload
```

access-list 1 extended permit ip

Baca Juga (Artikel Terkait)

- [chapter 34 section 3 technology and modern life answers](http://www.bbgglobalsolutions.com/chapter-34-section-3-technology-and-modern-life-answers.pdf)

URL: <http://www.bbgglobalsolutions.com/chapter-34-section-3-technology-and-modern-life-answers.pdf>

- [chapter 33 the talent management handbook](http://www.bbgglobalsolutions.com/chapter-33-the-talent-management-handbook.pdf)

URL: <http://www.bbgglobalsolutions.com/chapter-33-the-talent-management-handbook.pdf>

- [chapter 33 the age of exploration staff 4jne](http://www.bbgglobalsolutions.com/chapter-33-the-age-of-exploration-staff-4jne.pdf)

URL: <http://www.bbgglobalsolutions.com/chapter-33-the-age-of-exploration-staff-4jne.pdf>

- [chapter 33 section 4 guided reading and review answers](http://www.bbgglobalsolutions.com/chapter-33-section-4-guided-reading-and-review-answers.pdf)

URL: <http://www.bbgglobalsolutions.com/chapter-33-section-4-guided-reading-and-review-answers.pdf>

Tags: #cisco #configuration #guide #step #step #configuration #cisco #vpns #routers #harris #andrea #2014

