Contents

Introduction

This document describes how to set up a Easy VPN tunnel between a Cisco Adaptive Security Appliance (ASA) and a router that runs Cisco IOS® software using main mode with self signed certificate.

Prerequisites

The sample configuration of the router-to-router Easy VPN Solution is based on the assumptions that the IP address at the Cisco Easy VPN Server is static and that the IP address at the Cisco Easy VPN Client is static.

Requirements

Cisco recommends that you have knowledge of these topics:

- Internet Key Exchange (IKE)
- Certificates and Public Key Infrastructure (PKI)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ASA 5510 Adaptive Security Appliance that runs software version 8.4(7)
- Cisco 2821 Series Integrated Services Router (ISR) that runs Cisco IOS software version 15.2(4)M2

Related Products

This document can also be used with these hardware and software versions:

- Cisco ASA that runs software version 8.4 or later
- Cisco ISR Generation router that runs Cisco IOS software version 15.0 or later

Background Information

The document talks about using EzVPN on main mode which is not supported with pre-shared key. However, we can use main mode with Certificate authentication to overcome the vulnerabilities associated with aggressive mode: CVE-2002-1623.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

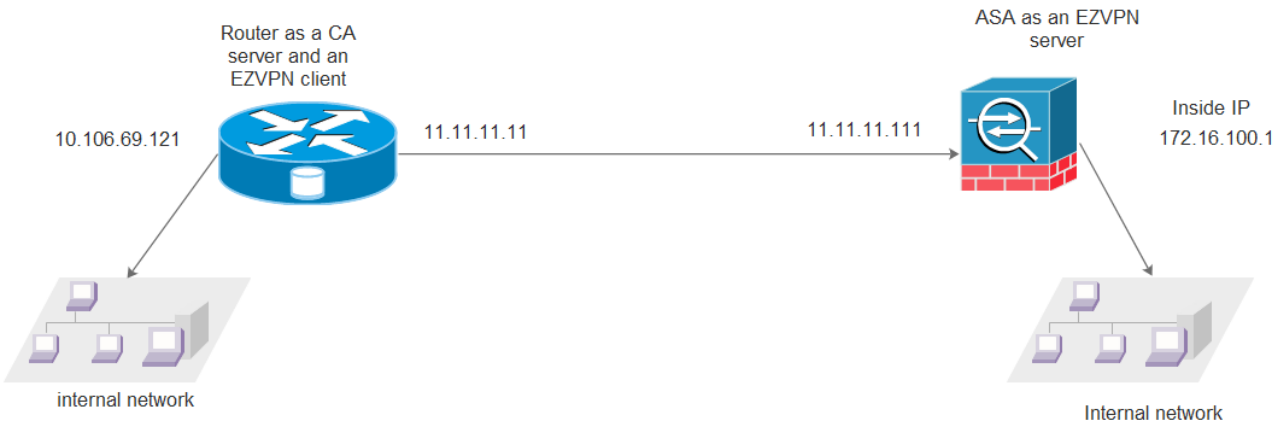
Configure

NTP

Certificate authentication requires that the clocks on all participating devices be synchronized to a common source. While the clock can be set manually on each device, this is not very accurate and can be cumbersome. The easiest method to synchronize the clocks on all devices is to use NTP. NTP synchronizes timekeeping among a set of distributed time servers and clients. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. For more information on how to configure NTP, refer to Network Time Protocol: Best Practices White Paper.

http://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html

Network Diagram



Configurations

Verify

Verify that the devices are enrolled successfully with the CA:

Troubleshoot

Debugs on the ASA

> **Caution**: On the ASA, you can set various debug levels; by default, level 1 is used. If you change the debug level, the verbosity of the debugs might increase.

It is recommended to use conditional debugs to view debugs only for the single peer:

Do this with caution, especially in production environments.

The ASA debugs for tunnel negotiation are:

The ASA debug for certificate authentication is:

Debugs on Router

The router debugs for tunnel negotiation are:

The router debugs for certificate authentication are: