Contenu

Introduction

Ce document décrit comment installer un tunnel Easy VPN entre une appliance de sécurité adaptable Cisco (ASA) et un routeur qui exécute le logiciel de Cisco IOSÂ® utilisant le mode principal avec le certificat signé d'individu.

Conditions préalables

La configuration d'échantillon de la solution d'Easy VPN de routeur à routeur est fondée sur les hypothèses que l'adresse IP au serveur de Solution Cisco Easy VPN est statique et que l'adresse IP au client de Solution Cisco Easy VPN est statique.

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Échange de clés Internet (IKE)
- Certificats et Infrastructure à clés publiques (PKI)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Serveur de sécurité adaptatif dédié de la gamme Cisco ASA 5510 qui exécute la version de logiciel 8.4(7)
- L'Integrated Services Router de gamme Cisco 2821 (ISR) ce exécute la version de logiciel 15.2(4)M2 de Cisco IOS

Produits connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

- Cisco ASA qui exécute la version de logiciel 8.4 ou plus tard
- Routeur de génération de Cisco ISR qui exécute la version de logiciel 15.0 de Cisco IOS ou plus tard

Informations générales

Le document parle utilisant l'EzVPN sur le mode principal qui n'est pas pris en charge avec la clé pré-partagée. Cependant, nous pouvons employer le mode principal avec l'authentification de certificat pour surmonter les vulnérabilités associées avec le mode agressif : CVE-2002-1623.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

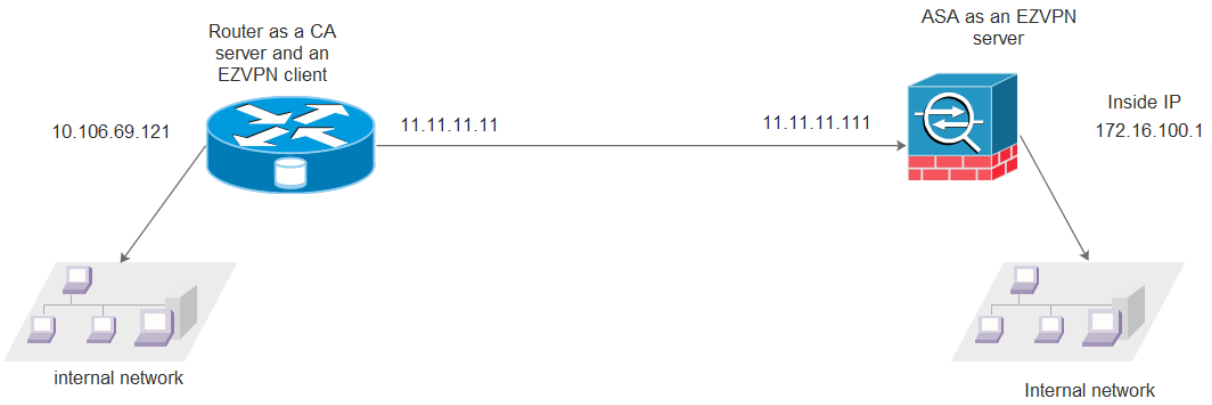
Configurez

NTP

L'authentification de certificat exige que les horloges sur tous les périphériques participants soient synchronisées à une source commune. Tandis que l'horloge peut être réglée manuellement sur chaque périphérique, ce n'est pas très précise et peut être encombrante. La méthode facile pour synchroniser les horloges sur tous les périphériques est d'utiliser le NTP. Le NTP synchronise la ponctualité parmi un ensemble de Serveurs de synchronisation et de clients distribués. Cette synchronisation permet des événements à corréler quand des logs système sont créés et quand d'autres événements de temps-particularité se produisent. Pour plus d'informations sur la façon configurer le NTP, référez-vous au Network Time Protocol : Livre Blanc de pratiques recommandées.

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

Diagramme du réseau



Configurations

Vérifiez

Pour vérifier que les périphériques sont inscrits avec succès avec le CA :

Routeur

ASA

Pour vérifier que le tunnel est

Routeur

Vérification de Phase 1 :

Vérification de Phase 2 :

ASA

Vérification de Phase 1 :

Vérification de Phase 2 :

Dépannez

Debugs sur l'ASA

> **Attention** : Sur l'ASA, vous pouvez placer divers mettez au point des niveaux ; par défaut, le niveau 1 est utilisé. Si vous changez le niveau de débogage, la verbosité du met au point pourrait augmenter.

Il est recommandé pour utiliser conditionnel met au point pour visualiser met au point seulement pour le pair simple :

Faites ceci avec prudence, particulièrement dans les environnements de production.

L'ASA met au point pour la négociation de tunnel sont :

L'ASA mettent au point pour l'authentification de certificat est :

Debugs sur le routeur

Le routeur met au point pour la négociation de tunnel sont :

Le routeur met au point pour l'authentification de certificat sont :