Configuring the Cisco ASA to Support Client Certificate Authentication for IPSec -v2

Introduction

Configuring certificate authentication support for IPSec connections includes several basic steps. Some portions of the configuration may already be in place, depending on your environment. This guide assumes that the Cisco ASA SSL VPN has been configured to support SecureAuth enrollment and access.

In order for certificate based authentications to work the server side, the ASA must have a certificate installed that can be validated by the client. In the SSL VPN world this is most often a certificate that has been purchased from an established provider. This means that the server's identity certificate can be validated by a 'root' certificate that is already installed on the client system. The same identity certificate that is used for the SSL VPN can usually be used for the IPSec connections. There are some IPSec-specific requirements for the identity certificate used by the ASA. The 'CN' of the certificate and the 'fqdn' fields in the certificate must match exactly what is configured as the 'host' on the IPSec client. See the following guides for further information:

- Requesting an Identity Certificate for a Cisco ASA
- Requesting an Identity Certificate for a Cisco ASA - Entrust trial cert


An additional tool that we are going to use, similar to how the SSL VPN is configured, is certificate to tunnel-group mappings. Mappings for IPSec are configured separately from SSL VPN mappings, and mappings replace the Group Name and Group Password, which is how most Cisco IPSec connections are configured. Certificate Group Matching is details on page 27-10 of the above named guide.

Configuration Steps

Configuring Certificate Authentication using ASDM

Note that ASDM has a separate section for configuring IPSec Connection Profiles.

Enable IPSec on an Interface

1. Check the box in the Allow Access column.
Configuring IKE Policies to Support Certificate Authentication

IKE Policies dictate how the ASA will handle the initial setup of an IPSec session. In order for certificates to be used for authentication, the lowest-priority numbered policy must specify RSA signature authentication.

The default configuration of the ASA has a policy with priority 1 using pre-share authentication. This either needs to be set to a higher number (preferred) or removed. The lowest priority policy should be configured for rsa-sig.

Ensure that the ASA is identifying itself properly to the client. This is done on the IKE Parameters page and should be set to Automatic.
Configure the IPSec Connection Profile

Note that in ASDM, the SSL VPN Connection Profiles and the IPSec Connection Profiles mirror each other. That is, if a SSL VPN Profile exists then an IPSec Profile of the same name will also exist, even if it is not configured to allow access. Some of the settings will be common to both, such as the AAA group.

You will need to bind an Identity Certificate to the Profile and enable IPSec for the Profile.

Next, configure some of the Advanced > IPSec settings of the Profile.

Check the Send certificate chain box to Enable this behavior (in most environments this will be unnecessary, but it is still useful to select).

Set the IKE Peer ID Validation to Check if supported by certificate.
For the IKE Authentication setting of the profile, select XAUTH (Extended user authentication) as the Default Mode so that AAA user authentication is required along with the certificate.
Configure a Certificate to Profile Map

The final step is to bind the certificate to a particular connection profile. This will bind a connection attempt with a certificate to a specific profile, and replaces the group mapping. Typically a group name and pre-shared key is configured for IPSec. Since profiles are stored as text files they can be transported from system to system, and since a group name is configured, the group/pre-share does not provide an user identity information. Replacing the group/pre-share in the client connection profile eliminates the easy portability of the connection profile, and binds the connection to the identity of the enrolled user.

To create an IPSec profile mapping:

1. In ASDM, go to Configuration > Network (Client) Access > Advanced > IPSec > Certificate to Connection Profile Maps.

2. Change the Policy settings to Use the configured rules to match a certificate to a group.

2a. Additionally, a Default to group may be assigned. One use of a default group can be to provide information to an end user about certificate problems. A certificate that cannot map properly will be assigned the default group, and a banner message with support information can be configured. You can also assign a Deny Any ACL to the group to prevent improperly mapped certificates from having any access to the network.
Once the mapping policy is configured, Rules are set up to match information contained in the certificate and assign a connection profile. If SSL VPN has been configured with certificate to profile mappings they will show up here, but will indicate —Not Mapped—. You can reuse the existing mapping and assign the same or a different profile for use with certificate to IPSec connection profile maps.

**Changing the Identity Associate with a Cisco IPSec Connection Profile**

Configure a certificate matching rule and associate it with a connection profile. The rule priority uniquely identifies the certificate matching rule and assigns a priority to the rule with lower values having greater priority. Rules that are not mapped will be ignored.

Map: MFA-Demo3-IPSEC
Priority: 10
Mapped to Connection Profile: MFA-Demo3-IPSec

Configure a certificate matching rule criterion

Rule Priority: 10
Mapped to Connection Profile: MFA-Demo3-IPSec

<table>
<thead>
<tr>
<th>Field</th>
<th>Component</th>
<th>Operator</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>Organizational Unit (OU)</td>
<td>Equals</td>
<td>-bf32e19e2345</td>
</tr>
</tbody>
</table>
When an integration requires multiple user identities, reassigning the certificate associated with a connection profile is easier than re-enrolling.

Assigning the identity certificate is a simple task done within the IPSec client:

1. Open the client
2. Select a connection profile and choose Modify

The properties window for the profile will open; the certificate binding appears at the bottom.

Expand the drop-down menu to select an alternate identity to be used by the IPSec client.

Note that choosing a certificate within the IPSec client does not affect the certificates. Any certificates issued on a system are independent of applications that use them, such as the Cisco Ipsec client. Certificates will remain usable until they expire.