Mobile ID
Cisco ASA/Anyconnect

Solution guide

Version: 1.1

Swisscom (Schweiz) AG
IAM & Security

Swisscom (Schweiz) AG
IAM & Security

Contents

Swisscom (Schweiz) AG
IAM & Security

1 Introduction

The purpose of this document is to provide clarifications **how** to interface Mobile ID with Cisco ASA to authenticate a user with Mobile while using Cisco AnyConnect.

This manual assumes that you are familiar with Cisco ASA, Cisco Anyconnect and Swisscom Mobile ID

More details about Mobile ID can be found in the Mobile ID SOAP client reference guide [1].

Terms and abbreviations

Abbreviation	Definition
	Please note:
	Be careful, important:
AP	Application Provider
DataToBeDisplayed DTBD	Data to be displayed
DataToBeSigned DTBS	Data to be signed
MSSP	Mobile Signature Service Provider
M-ID or MID	Mobile ID platform providing the mobile signature service
MSISDN	Number uniquely identifying a subscription in a GSM/UMTS mobile network
SOAP	Simple Object Access Protocol (SOAP) is a protocol specification for exchanging structured information in the implementation of Web Services relying on Extensible Markup Language (XML)
WS	A Web service (WS) is a method of communication between two electronic devices over the Web (Internet).

1.1 Referenced documents

[1] SOAP Client Reference Guide
[2] RADIUS Integration Guide
[3] ASA 8.0: Configure RADIUS Authentication for WebVPN Users
http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/98594-configure-radius-authentication.html#asa
[4] Configuring AnyConnect VPN Client Connections
http://www.cisco.com/c/en/us/td/docs/security/asa/asa80/configuration/guide/conf_gd/svc.html
[5] CISCO configuration examples and technotes
http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-configuration-examples-list.html

Swisscom (Schweiz) AG
IAM & Security

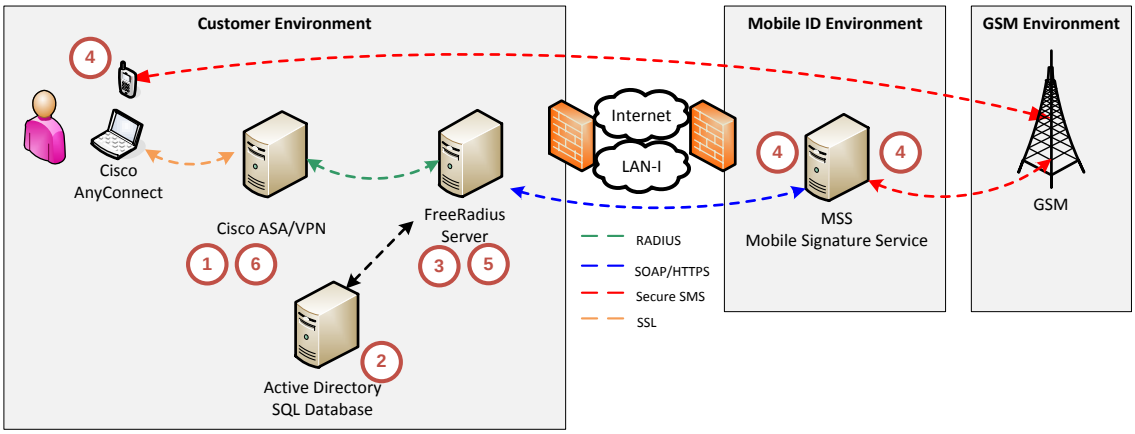
2 Overview and main scenario

This chapter describes a possible solution to interface a Cisco ASA product with Mobile ID.

The solution detailed in this guide is based on the available Radius interface at the Cisco ASA side. This interface communicates with a Radius server, in our case an on premise FreeRADIUS server. Basically it can be done with any Radius server that is extensible and would allow the integration of the Mobile ID. We documented such a Mobile ID integrated server based on FreeRADIUS in [2].

Scenario - Strong Authentication with Cisco ASA/VPN:

Before entering into more technical details, let's have a short look at the main solution:



This picture shows a user who request remote access with AnyConnect to the Cisco ASA. The ASA/VPN then sends the RADIUS requests to the FreeRADIUS server to authenticate the user. FreeRADIUS will invoke the Swisscom Mobile ID service over SOAP and provide the answer back to the RADIUS client interface of the ASA. FreeRADIUS server may also be connected to an external user store, like Microsoft Active Directory, where the end users details like phone number or credentials are stored.

Here the authentication dataflow:

1. When a user tries to connect on ASA/VPN Gateway, the ASA makes a request to the defined FreeRADIUS server to authenticate the end user with Mobile ID.
2. FreeRADIUS server, optionally, verifies the user credentials against internal user stores and/or maps to a valid mobile phone user
3. FreeRADIUS server (which enabled the Mobile ID plugin) calls the Mobile ID service
4. The Mobile ID platform ensures that the end-user signature request is allowed and forwards the signature request to the end-user's mobile phone
5. The end-user answer will be processed by the Mobile ID platform and provided to FreeRADIUS server
6. After verification of Mobile ID response by FreeRADIUS server, the answer will be forwarded to the ASA (over its Radius client interface). This answer will be processed by the ASA to grant or reject the Cisco Anyconnect connection requests.

3 Configuration and Best Practices

In this reference guide we assume that:

1. The preconditions defined in [1] are met.
2. The customer has built an intermediate protocol gateway like the FreeRADIUS server described in [2] (with the Mobile ID plugin).

3.1 Configuration of FreeRADIUS on ASA/VPN server

To allow an ASA to perform a Mobile ID authentication, the ASA authentication must be configured to reroute the user requests towards the FreeRADIUS server. The configuration of the ASA must be performed as described by Cisco in [3].

Basically, the ASA must define a new AAA server as such:

1. The "server name or IP address" is the IP address that refers to your "on premise" FreeRADIUS server.
2. The "Timeout" should be configured to 90sec in order to give enough time to Mobile ID to handle the authentication requests.
3. The "Server Authentication Port" is the authentication port that you defined in your "on premise" FreeRADIUS server.
4. The "Server Accounting Port" is the accounting port that you defined in your "on premise" FreeRADIUS server.
5. The "Server secret key" is the shared secret that you defined in your "on premise" FreeRADIUS server.

3.2 Configuration of Cisco AnyConnect on the ASA to support Mobile ID

The only adaptation to support Mobile ID authentication with AnyConnect is the proper configuration of the timeout.

IPsec IKEv2 mode does NOT support a timeout higher than 25sec, therefore this mode cannot be used. The alternative is to use the SSL mode to support an authentication timeout of 90 sec.

1. The configuration of Anyconnect on the ASA must be performed as described by Cisco in [4].
2. The configuration of the customer xml Profile in the ASA of AnyConnect, should allow the Client to wait for at least 90sec before getting a response on authentication request.

   ```
   <AuthenticationTimeout>90</AuthenticationTimeout>
   ```

   See chapter 4 for a profile example.

3.3 Radius Gateway and end-users details

The document [2] describes as well how to inter-connect an external user store to the FreeRADIUS server, like Microsoft Active Directory (where the end users details like phone number or credentials are stored).

3.4 Additional documentation

Refer to [3], [4] and [5] for additional documentation and information regarding this setup.

Swisscom (Schweiz) AG
IAM & Security

4 Example of Cisco AnyConnect configuration profile (xml profile)

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
        <ClientInitialization>
               <UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
               <AutomaticCertSelection UserControllable="false">true</AutomaticCertSelection>
               <ShowPreConnectMessage>false</ShowPreConnectMessage>
               <CertificateStore>All</CertificateStore>
               <CertificateStoreOverride>false</CertificateStoreOverride>
               <ProxySettings>IgnoreProxy</ProxySettings>
               <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
               <AuthenticationTimeout>90</AuthenticationTimeout>
               <AutoConnectOnStart UserControllable="false"> false</AutoConnectOnStart>
               <MinimizeOnConnect UserControllable="false"> true</MinimizeOnConnect>
               <LocalLanAccess UserControllable="false">true</LocalLanAccess>
               <ClearSmartcardPin UserControllable="false"> false</ClearSmartcardPin>
               <AutoReconnect UserControllable="false">true
                      <AutoReconnectBehavior UserControllable="false">
                          DisconnectOnSuspend</AutoReconnectBehavior>
               </AutoReconnect>
               <AutoUpdate UserControllable="false">false</AutoUpdate>
               <RSASecurIDIntegration UserControllable="false">
                   Automatic</RSASecurIDIntegration>
        <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
        <WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
               <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
               <PPPExclusion UserControllable="false">Disable
                      <PPPExclusionServerIP UserControllable="false"> </PPPExclusionServerIP>
               </PPPExclusion>
               <EnableScripting UserControllable="false"> false</EnableScripting>
               <EnableAutomaticServerSelection UserControllable="false">false
                      <AutoServerSelectionImprovement> 20</AutoServerSelectionImprovement>
                      <AutoServerSelectionSuspendTime> 4</AutoServerSelectionSuspendTime>
               </EnableAutomaticServerSelection>
               <RetainVpnOnLogoff>false</RetainVpnOnLogoff>
        </ClientInitialization>
        <ServerList>
               <HostEntry>
                      <HostName>xxx.xxx.net</HostName>
                      <UserGroup>CUSTOMER-XY</UserGroup>
               </HostEntry>
        </ServerList>
</AnyConnectProfile>
```