Practical PKI for VPN
BRKSEC-2053
Agenda

- Making the case for Identity-based Digital Certificates
- Using best practices to Simplify the Deployment of Certificates for VPN
- Best Practices Case Study – Cisco Anyconnect SSLVPN with certificates
- Case Study Demo
- Q&A
Making the Case for Digital Certificates

Two-factor VPN Authentication and much more
Certificate Authority (CA)
The source of truth for any PKI

- Responsible for issuing, validating, renewing, revoking and logging certificates
- Establishes and verifies the identities of certificate requestors
- Configures the usage and content of certificates (templates) and issues certificates to users, computers, and services
Types of Client Digital Certificates

1. User/Identity Certificates
   - A certificate that contains a user based attribute
   - Usually in the CN or UPN field

2. Device Certificates
   - A certificate that contains a device specific attribute

3. Hybrid (User plus Device) Certificates
   - Allow for network access of specifically authorized devices used by specifically authorized users.
Certificate File Formats Demystified

- **DER (.der .cer)** – Distinguished Encoding Rules
  - Binary encoded single cert per file
  - Cannot copy / paste

- **PEM (.pem .cer .crt .key)**
  - Base64 encoded txt
  - Can copy / paste

- **PKCS#12 (.pfx .p12)**
  - Certificate Chain usually with private keys
  - Password may be required to open

- **CSR (.csr)** - certificate signing request (PKCS10)

- **PKCS#7 (.p7b .p7c)**
  - Certificate chain without private keys
  - *Cannot import directly into ASA, need to convert
How Identity Certificates Work
VPN Use Case – Exchange of Certificates

- Connection initiated by AnyConnect or browser session to ASA Head end
  1. ASA presents its outside interface SSL Identity Certificate
  2. Client validates ASA certificate
  3. AnyConnect or browser provides client Identity Certificate to ASA
     1. ASA validates Client certificate
        - Optional: ASA requests 2\textsuperscript{nd} factor username + password
        - Optional: ASA evaluates certificate matching rules to set connection policy
How Identity Certificates Work

VPN Use Case – Mutual Validation of Certificates

- Certificate validation steps:
  - Has the digital certificate been **issued by a trusted CA**?
  - Is the certificate **expired**? (start + end date validity check)
  - Has the certificate been **revoked**? (OCSP or CRL check)
  - Does the **VPN URL match** the CN or SAN field in the certificate?

- Protects against Man in the Middle Attacks
  - ASA checks against a known trusted CA
Certificate Revocation Explained
How Identity Certificates Work

VPN Use Case – Parsing of Certificate Attributes

- ASA can parse client identity certificate fields for authorization checks
  - Connection Profile mapping based on email domain (example)
  - VLAN / IP address assignment based on AD domain name (example)

Subject (CN) & Subject Alternative Name (SAN) fields
How Identity Certificates Work
Forcing per user cert auth

- Pre-fill username adds security
- ASA can query AD (LDAP) record of user in certificate

ASA Pre-fill Authentication Configuration
Anyconnect with pre-filled username
Advantages of Certificates

- **Two-factor Authentication** using Identity Certs plus username/password
  - Less expensive TCO alternative to token solutions
  - Simpler end-user experience = Happier users 😊

- **Increased protection** against Phishing, MiTM and Social Engineering Attacks

- Provides a **user friendly experience** for Mobile device VPN
  - Automatic On-demand VPN connectivity

- Establish VPN security **policy per device**
Disadvantages of Certificates

VPN Use Case

- Another mouth to feed!
  - Must maintain PKI server(s) and keep highly available (backups, redundancy, updates)

- Portability and Enrolling **Multiple** Devices
  - Multiple end user devices = multiple identity certificates
  - Can’t use an endpoint for VPN until it has been enrolled first

- General lack of PKI skillset in IT today
  - Steeper learning curve than deploying OTP solutions
  - Incorrect deployments can be insecure
Common x.509 Certificate Myths!

- **Hard to deploy!**
  - Takes forever to setup and get right
  - Hard to create a robust PKI in house, huge project
  - Hard to get certificate to user / device

- **Hard to manage!**
  - Takes several FTE to run this thing
  - Lots of care and feeding
  - Troubleshooting is a nightmare

- **Confusing end user experience!**
  - Which certificate do I choose and when?
  - Certificate warning pop-ups
  - Tedious and confusing certificate enrollment process for each device!

- **Not true two-factor authentication!**
  - Anyone on the PC can use my VPN
  - Everyone has the same certificate
Common Myths Busted!

- **Hard to deploy!**
  - Usually a skillset issue not a technology issue
  - Can be deployed in about a day using MSFT AD CA
  - Complete automation for AD domain PC’s

- **Hard to manage!**
  - Once deployed there is very little on-going maintenance or management
  - Cisco ASA provides easy to understand error logs when something goes wrong

- **Confusing end user experience!**
  - In most cases the user will not interact with a certificate
  - Even enrollment can be made completely transparent to the end-user
  - Certificates = Happy Users 😊

- **Not true two-factor authentication!**
  - Accepted by PCI, FISMA, NIST…
  - Needs to be identity based certs not shared certs
SCEP and SCEP Proxy Overview

- SCEP stands for Simple Certificate Enrollment Protocol
- SCEP provides an easy and secure mechanism to deploy certificates
- SCEP is supported by MSFT CA’s, IOS CA, others
- SCEP embedded into Cisco AnyConnect Client on all Platforms

SCEP Proxy hides CA Server from Client
Certificate Use Cases

VPN is just one use case!

- User and Machine certificates are **the gift that keeps on giving**
- Quickly increase corporate security in other areas
- Deploy once, use everywhere*
AnyConnect Secure Mobility

- SSL and IPSec VPN Client
  - Certificate and two factor authentication support

- 802.1x network supplicant
  - EAP-TLS support

- Broad client device support
  - Windows, Mac, Apple iOS, Android

- Built-in SCEP support
  - Easy deployment of certificates
Cisco Jabber for iPhone/Android

- Enterprise VoIP calling
  - “Office” like VoIP calling and directory services

- Embedded Anyconnect
  - Allows certificate based ‘embedded’ SSL VPN for seamless user experience

- Broad mobile device support
  - Apple iOS, Android

- Built-in SCEP support
  - Easy deployment of certificates
Wired and Wireless 802.1x Security

- EAP-TLS uses certificates for authentication to wireless
- Wired 802.1x uses certificates for authentication and device authorization
- Network Admission Control (NAC) can use certificates as part of a device security posture check
Many Other Use Cases for Identity Certs!

- **Secure Email** – Use identity certificate to sign and encrypt email

- **Document Signing** – Ensure Authenticity and Integrity of sensitive docs

- **Secure Login to Web Services** – Identity Certificates provide a single-sign-on experience or provide two-factor authentication
Agenda

✓ Making the case for Identity-based Digital Certificates

✧ Using best practices to Simplify the Deployment of Certificates for VPN

- Best Practices Case Study – Cisco Anyconnect SSLVPN with certificates

- Case Study Demo

- Q&A
Our Two Deployment Goals

- **Easy to Use**
  - Minimize the interaction end users have in the whole process

- **Easy to Deploy**
  - Setup a CA deployment quickly and easily
  - Deploy Identity certificates quickly to end users
What Certs do we need to Deploy?

1. **One or more CA Trusted Root Certificates:**
   - Used to establish a chain of trust for Identity Certificates
   - Both sides, ASA and VPN clients, need proper certificate chains in place

2. **Cisco ASA Device Identity Certificate:**
   - Presented to remote users to identify Cisco ASA
   - Only one Device Certificate per interface allowed
   - Should be signed by a *Public CA* to ease deployment

3. **User Identity Certificate:**
   - Presented by remote users to identify themselves to the ASA
   - ASA can authenticate either User or Machine certificates
   - Usually signed by an *internal CA* to decrease costs and ease deployment
Certificate Deployment Considerations

Easy as 1-2-3 😊

1. Choosing a Certificate Authority Solution

2. Best Practice Configuration of CA Server

3. Best practices for deploying device and user certificates on various device types
Cisco Certificate Authorities

- Cisco IOS Router CA [*recommended for small/medium sized S2S VPNs]*
  - Well suited for Site to Site IPSEC VPN deployments
  - Supports Secure Device Provisioning (SDP) for easy router cert deployment

- **Cisco ASA CA** [*recommended for small SSLVPN deployments]*
  - Remote Access AnyConnect usage only
  - Integrates basic CA operation into the ASA

- **Cisco Identity Services Engine (ISE)**
  [*recommended for provisioning non-AD PCs and mobile devices]*
  - Provides Certificate and Client Provisioning (Summer 2012 release)
  - Not a CA!... It is a SCEP Proxy
Microsoft Certificate Authority

- **Active Directory Certificate Services**
  - Built into Windows Server OS (Save$)
  - Windows Server 2008 R2 Enterprise is recommended

- **Automatic Certificate Enrollment!!!**
  - AD Group Policy cert push to domain computers
  - Fully Active Directory Integrated
  - SCEP support for easy deployment to mobile / non-AD
# Microsoft 2008 R2 Editions

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Network Device Enrollment Service</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Online Responder service</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CA Web Enrollment</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Certificate Enrollment Web Service</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Certificate Enrollment Policy Web Service</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>AD CS features</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customizable version 2 and version 3 certificate templates</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Key archival</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Role separation</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Certificate manager restrictions</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Delegated enrollment agent restrictions</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Certificate enrollment across forest boundaries</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Other Certificate Authorities

- **On Premise**
  - Appliance based
  - Broad feature support
  - Windows & Non-Windows focus

- **Hosted**
  - Cloud based SaaS offering
  - Less care and feeding
  - Usually more expensive
Certificate Authority Recommendations

If Mostly AD Domain Joined Computers:

- Microsoft Windows 2008 R2 Enterprise Certificate Authority
  - Low cost, most Windows Server customers already own this
  - User and Machine certificates can be auto deployed using Group Policy
  - SCEP and Web enrollment support for mobile / non domain devices

Mostly non-domain joined computers and non-windows devices

- MSFT or 3\(^{rd}\) party on premise or cloud service
  - Tightly integrated with Cisco ASA
  - Streamlined enrollment process
Best Practice Configuration of CA Servers

VPN Use Case
Cisco ASA Certificate Authority
Configuration Best Practices for Small Businesses

- Considerations with using ASA CA
  - Small deployments only <50
  - No support for High Availability (LB or FO)
  - Cannot be subordinate CA, only root
  - Web enrollment via email invitation only
  - OTP is only enrollment validation method
  - Does not support CSR files only copy/paste
  - No SCEP support

From: asa-ca@cisco.com
Subject: Reminder: Certificate Enrollment Invitation
Date: April 3, 2012 9:02:30 PM EDT
To: jfanelli@cisco.com

You have been granted access to enroll for a certificate.

The credentials below can be used to obtain your certificate.

Username: jfanelli
One-time Password: 7036DE559A8E8CF6
Enrollment is allowed until: 22:04:40 EDT Wed Apr 4 2012

NOTE: The one-time password is also used as the passphrase to unlock the certificate file.

Please visit the following site to obtain your certificate:
https://asa-ca.std-dc-lab.cisco.com/+CSCOA+/enroll.html

You may be asked to verify the fingerprint/thumbprint of the CA certificate during installation of the certificate. The fingerprint/thumbprint should be:

MD5: 5D134D5 561B1179 EF2FBBB3 2C67A6D7
SHA1: DCA6E7A FDF448A6 7489ABE6 2A2E9436 214D27D5
**Cisco ASA CA Configuration**

**Minimum configuration steps:**

1. **Passphrase to secure CA key files**
2. **Email server settings to notify users of enrollment**
ASA CA Operations and User Enrollment

1) Add a New User and Email OTP


3) User logs on to SSLVPN
Cisco ASA SSLVPN Connection Log

Successful certificate authentication should show:

- Certificate validation showing Cert username
- Certificate chain validation with CRL check
- Tunnel Group Certificate Matching Rule (optional)
- DAP rule matches + IP address assignment

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group &lt;Split_Policy&gt; User &lt;cisco\jefanell&gt; IP &lt;166.147.96.128&gt; UDP SVC connection established without compression</td>
</tr>
<tr>
<td>Group &lt;Split_Policy&gt; User &lt;cisco\jefanell&gt; IP &lt;166.147.96.128&gt; First UDP SVC connection established for SVC session.</td>
</tr>
<tr>
<td>DAP: User cisco\jefanell, Addr 166.147.96.128, Connection AnyConnect: The following DAP records were selected for this connection: DfitAccessPolicy</td>
</tr>
<tr>
<td>Group &lt;Split_Policy&gt; User &lt;cisco\jefanell&gt; IP &lt;166.147.96.128&gt; Address &lt;192.168.52.1&gt; assigned to session</td>
</tr>
<tr>
<td>Group &lt;Split_Policy&gt; User &lt;cisco\jefanell&gt; IP &lt;166.147.96.128&gt; TCP SVC connection established without compression</td>
</tr>
<tr>
<td>Group &lt;Split_Policy&gt; User &lt;cisco\jefanell&gt; IP &lt;166.147.96.128&gt; First TCP SVC connection established for SVC session.</td>
</tr>
<tr>
<td>TunnelGroup &lt;AC_Split_Profile&gt; GroupPolicy &lt;Split_Policy&gt; User &lt;cisco\jefanell&gt; IP &lt;166.147.96.128&gt; No IPv6 address available for SVC connection</td>
</tr>
<tr>
<td>IPAA: Local pool request succeeded for tunnel-group 'AC_Split_Profile'</td>
</tr>
<tr>
<td>IPAA: Client assigned 192.168.52.1 from local pool</td>
</tr>
<tr>
<td>Group &lt;Split_Policy&gt; User &lt;cisco\jefanell&gt; IP &lt;166.147.96.128&gt; WebVPN session started.</td>
</tr>
</tbody>
</table>

Group <DfltCrlPolicy> User <cisco\jefanell> IP <166.147.96.128> Authentication: successful, Session Type: WebVPN. |
Tunnel group search using certificate maps failed for peer certificate: serial number: 02, subject name: cn=cisco\jefanell,ou=Borderless Security Team,... |
AAA retrieved default group policy (Split_Policy) for user = cisco\jefanell |
Certificate chain was successfully validated with revocation status check. |
Certificate was successfully validated. serial number: 02, subject name: cn=cisco\jefanell,ou=Borderless Security Team,o=Cisco,c=US,st=MI,ea=jefan,
Configuring Microsoft CA
Best Practices!
Windows 2008 R2 Certificate Services
On a AD plus IIS server…

- Add administrator or SCEP_User to IIS_IUSRS group
- Add AD-CS Role plus Role Services to your Domain Controller

Server Manager

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Role Status:
- Messages: None
- System Services: All Running
- Events: None in the last 24 hours
- Best Practices Analyzer: 1 noncompliant; 0 excluded; 7 compliant
  Last Scan: 4/15/2012 1:05:09 PM

Role Services: 4 installed
- Certification Authority: Installed
- Certification Authority Web Enrollment: Installed
- Online Responder: Installed
- Network Device Enrollment Service: Installed
- Certificate Enrollment Web Service: Not installed
- Certificate Enrollment Policy Web Service: Not installed
Create Your Certificate Template

1. Open MMC > Certificates Snap-in

2. Certificate Templates Console

3. Duplicate Template

Properties of New Template:
- Template display name: User Identity Cert
- Minimum Supported CAs: Windows Server 2008 Enterprise
- Template name: UserIdentityCert
- Validity period: 6 months
- Renewal period: 6 weeks
- Publish certificate in Active Directory
Certificate Template Changes

Check Extensions/App Policies

Disable Export of Certs
Certificate Template Final Steps

- Select the subject criteria
  - must have email populated in accounts for Auto-enroll
- Publish Template!
Enable GPO Auto-enrollment User Certs

1-Step Deployment!!! Who says certs are hard?

- Enable Auto-enrollment in the MMC>Default Domain Policy > User Configuration
- Done!

- Users get certs as soon as GPO refreshes on their PC
- By Default this is ~90 minutes max
Enable GPO Auto-enrollment Computer Certs

Yep still a 1-step deployment. Bang!

- Enable Auto-enrollment in the Default Domain Policy > Computer Configuration
GPO Authorization

Just in case

Verify GPO policies allow certificates to be used for authentication
Enable SCEP for non-AD joined Hosts

Optional

1. Clone the IPSECIntermediateOffline Template
2. Change Application Policies
3. Issue Certificate Template
4. Open Regedit
5. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP
6. Change GeneralPurposeTemplate to match the new clone
7. Optional: Disable Force OTP for SCEP
8. Reboot CA Server
ASA CA Cert SCEP Enrollment

Adds CA Server Certificate chain to ASA

Default CA SCEP URL:
HTTP://<CA Server>/certserv/mscep/mscep.dll
ASA Identity Cert SCEP Enrollment Example

Go to Remote Access VPN > Certificate Management > Identity Certificates
How to Verify or Revoke a Certificate

- See what certs have been issued
- Revoke Certificates when required
- *CRL Validity is 1 week + 10% by default on 2008R2 CA
- OCSP updates can be near real-time
Certificate Based AnyConnect SSLVPN Monitoring and Troubleshooting
Certificate Troubleshooting

*Chain* of certificates may be incomplete

- Match Authority Key Identifier field to CA Root Cert(s)
MSFT CA Troubleshooting

Server Manager, Event Viewer and Certificate Services are FULL of info
Microsoft CA Event Viewer
Works on Vista/Win7 or CA Server 2008

- For more detailed logs turn on CryptoAPI 2.0 Diagnostics logging

1. In the Event Viewer, navigate to **Application Logs** > **Microsoft** > **Windows** > **CryptoAPI 2.0 or CAPI2** for the CryptoAPI 2.0 channel

2. Right-click, Enable Log
Event Monitoring - Cisco CSM 4.2
Reporting - Cisco ACS 5 and CSM 4.2
## Reporting - ACS 5

### AAA Protocol > RADIUS Authentication

- **Network Device Name:** vpn-sf-ld
- **Access Service:** Default Network Access
- **Authentication Status:** Pass or Fail
- **Date:** March 13, 2012 - April 11, 2012

### Table

<table>
<thead>
<tr>
<th>ACS View Timestamp</th>
<th>ACS Timestamp</th>
<th>RADIUS Status</th>
<th>NAS Failure</th>
<th>Details</th>
<th>Username</th>
<th>MAC/IP Address</th>
<th>Access Service</th>
<th>Authentication Method</th>
<th>Network Device</th>
<th>Failure Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 11,12 2:49:15.573 PM</td>
<td>Apr 11,12 2:49:15.490 PM</td>
<td>✓</td>
<td></td>
<td>jianeli</td>
<td>10.130.2.55</td>
<td>Default Network Access</td>
<td>MSCHAPv2</td>
<td>vpn-sf-ld</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apr 11,12 1:39:12.876 AM</td>
<td>Apr 11,12 1:39:12.793 AM</td>
<td>✓</td>
<td></td>
<td>jianeli</td>
<td>70.91.233.132</td>
<td>Default Network Access</td>
<td>MSCHAPv2</td>
<td>vpn-sf-ld</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apr 11,12 1:39:05.936 AM</td>
<td>Apr 11,12 1:39:05.268 AM</td>
<td>✗</td>
<td></td>
<td>jianeli</td>
<td>70.91.233.132</td>
<td>Default Network Access</td>
<td>MSCHAPv2</td>
<td>vpn-sf-ld</td>
<td>24409 User authentication against Active Directory failed since user has entered the wrong password</td>
<td></td>
</tr>
<tr>
<td>Apr 10,12 3:52:06.296 PM</td>
<td>Apr 10,12 3:52:06.233 PM</td>
<td>✓</td>
<td></td>
<td>jianeli</td>
<td>10.117.66.72</td>
<td>Default Network Access</td>
<td>MSCHAPv2</td>
<td>vpn-sf-ld</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apr 10,12 3:51:31.980 PM</td>
<td>Apr 10,12 3:51:31.883 PM</td>
<td>✗</td>
<td></td>
<td>jianeli</td>
<td>10.117.66.72</td>
<td>Default Network Access</td>
<td>MSCHAPv2</td>
<td>vpn-sf-ld</td>
<td>24407 User authentication against Active Directory failed since user is required to change his password</td>
<td></td>
</tr>
<tr>
<td>Apr 10,12 12:21:48.003 PM</td>
<td>Apr 10,12 12:21:47.930 PM</td>
<td>✗</td>
<td></td>
<td>navegunt</td>
<td>10.20.219.217</td>
<td>Default Network Access</td>
<td>MSCHAPv2</td>
<td>vpn-sf-ld</td>
<td>24408 User authentication against Active Directory failed since user has entered the wrong password</td>
<td></td>
</tr>
<tr>
<td>Apr 10,12 12:21:38.546 PM</td>
<td>Apr 10,12 12:21:38.470 PM</td>
<td>✗</td>
<td></td>
<td>navegunt</td>
<td>10.20.219.217</td>
<td>Default Network Access</td>
<td>MSCHAPv2</td>
<td>vpn-sf-ld</td>
<td>24408 User authentication against Active Directory failed since user has entered the wrong password</td>
<td></td>
</tr>
</tbody>
</table>
Agenda

✓ Making the case for Identity-based Digital Certificates

✓ Using best practices to Simplify the Deployment of Certificates for VPN

✦ Best Practices Case Study – Cisco Anyconnect SSLVPN with certificates

✦ Case Study Demo

✦ Q&A
Case Study

Certificate Authentication for AnyConnect
Assumptions

You have setup an AnyConnect SSLVPN either manually or through the ASDM SSLVPN Wizard

And you understand the basics of:
- Connection Profiles/Tunnel Group
- Group Policy
- Dynamic Access Policy
- Cisco Secure Desktop/Host scan
Case Study Architecture

Internet

Cisco ASA
ASA 8.4.2+

Internal Network

ACS/ISE

AD / Certificate Authority
Windows 2008 R2

VPN User
Configuration Steps Overview

ASA AnyConnect SSLVPN
Modify your Connection Profiles
Create Client Profiles
Modify Group Policy
Create Dynamic Access Policy (DAP) rules

MSFT CA
- Create Certificate Template(s)
- Enable GPO to roll certificates to domain users/devices
- Enable NDES/SCEP Services on Windows Server
Best Practice Essentials

- Delivery – How do I put a certificate on Computers & Mobile Devices?

- AAA – Security of Device/User, Has Certificate been moved?

- Validation – What is required to check the Certificate?

- Management – Certificate, Dynamic Access Policies, and LDAP
Recommended Delivery Methods

**SCEP**
- Controlled via Client
- Needs to use Pull Down List
- Direct communication with CA
- Needs Multiple Conn. Profiles

**SCEP Proxy**
- Controlled via Headend
- Does not need Pull Down List
- ASA communicates with CA
- Can use Single Connection Profile

**Caveats**
- Today not on Mobile Platforms
- Can include DeviceID in Request
- Requires Premium AC License
- Requires ASA 8.4(1)+

**GPO**
- Supported for Domain joined devices only
- ***Easiest way to roll out certificates***
ASA SCEP Proxy Connection Flow

AnyConnect handles with and without Certificate
SCEP Delivery

Connection Profiles

<table>
<thead>
<tr>
<th>Aliases</th>
<th>Authentication Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>secmob</td>
<td>Certificate</td>
</tr>
<tr>
<td>GetCert</td>
<td>AAA(securemobility)</td>
</tr>
<tr>
<td>scep_proxy</td>
<td>AAA(securemobility)</td>
</tr>
</tbody>
</table>

SCEP – iOS and Android

Two Connection Profiles
- **GetCert** – Leverage AAA for enrollment
- **Secmob** – Certificate Authentication for tunnel

SCEP Proxy - Windows/Mac/Linux

One Connection profile
- **Scep_proxy** - profile handles enrollment and authentication

*Enable SCEP enrollment for this profile

**Enable Simple Certificate Enrollment Protocol (SCEP) for this Connection Profile**
Delivery
Group Policy Change for SCEP Proxy

Without this feature:
- a device with a certificate will authenticate
- a device without a certificate will not be able enroll
Delivery

AnyConnect SCEP Configuration

Client Profile

- Requires CA URL
- Automatic SCEP Host – Certificate Enrollment Group
- %USER% as CN and/or Email used for User Authorization
Mobile device Specific Configuration

Mobile Settings

Connect on Demand requires Certificate Authentication

Activate on import needed for device to automatically select imported profile.

On Demand Domain list
Delivery
Device Based Certificates

Client Profile

• %MACHINEID% used to input in certificate request [optional]

• Notice %USER% is not in CN to enforce Device/Certificate Pair

• Dynamic Access Policy will be used to verify device/certificate pair
Delivery
Using Microsoft CA with GPO and SCEP/NDES

SCEP configuration for CA

Easiest way to deploy Certificates via Group Policy

[Images of configuration settings and Group Policy Management Editor]

Cisco Public
Delivery

End-user experience

*Activate on import is available on mobile devices. No need to MANUALLY select the profile.
Best Practice Essentials

✓ **Delivery** – How do I put a certificate on Computers & Mobile Devices?

♦ **AAA** – Security of Device/User, Has Certificate been moved?

✉ **Validation** – What is required to check the Certificate?

✉ **Management** – Certificate, Dynamic Access Policies, and LDAP
Authentication Authorization Accounting (AAA)

Case Study Security Requirements:

- **Two-Factor** Authentication (cert, username/pwd)
- **Prevent sharing** of certificates by multiple users
- Check **user exists in AD** before allowing VPN
- Use AD **group membership** as criteria for allowing SSLVPN
- Check if the PC is **joined to the AD domain**
- Severely limit net access during certificate SCEP enrollment
- Verify Device certificate is on correct device
AAA – Two Factor Authentication

Two factor – Best practice for Non-Mobile. Notice both AAA and Certificate is selected.

Pre-Fill Username – Used to verify certificate to User
AAA

Check if user is authorized for connection

Scenario: Need to deny a user access when using Certificate only Auth IT process: 1) IT revokes cert, validity period is 24hrs.
2) IT disables user’s AD account, takes effect immediately.

User valid? - Verifies User is in AAA database

Pre-fill username from certificate for authorization
AAA

Optional Common Authorization checks

DAP for checking User AD group membership

DAP for checking Machine is Domain joined
AAA
Restrict Devices during SCEP Certificate Enrollment

Scep.required is a new field that is populated true when you fail certificate authentication and the connection profile is set for SCEP Proxy

Leverage this field in a DAP rule to further control security of enrollment
AAA

Security during SCEP Certificate Enrollment

- Apply Network ACL to limit access to SCEP/CA Server during enrollment
- ACL “Required” for SCEP but not SCEP Proxy
### Device ID Awareness in ASA

<table>
<thead>
<tr>
<th>Device</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>BIOS Serial Number</td>
</tr>
<tr>
<td>Mac</td>
<td>Device Serial Number</td>
</tr>
<tr>
<td>Linux</td>
<td>Device Serial Number</td>
</tr>
<tr>
<td>Apple iOS</td>
<td>UDID</td>
</tr>
<tr>
<td>Android</td>
<td>IMEI (GSM), ESN (CDMA)</td>
</tr>
</tbody>
</table>

With Android and iOS devices other attributes are available
AAA

Device Certificate is on correct Device

- Endpoint.certificate.user["0"]).subject_cn
- Endpoint.device.id is copied from anyconnect
- If NE, then certificate has been moved.
Best Practice Essentials

✓ Delivery – How do I put a certificate on Computers & Mobile Devices?

✓ AAA – Security of Device/User, Has Certificate been moved?

♦ Validation – What is required to check the Certificate?

روف Management – Certificate, Dynamic Access Policies, and LDAP
Validation
Online Certificate Status Protocol (OCSP) / Certificate Revocation List (CRL)

- OCSP is a best practice for large deployments or immediate revocation
- CRL as a backup or for smaller deployments
Best Practice Essentials

✓ Delivery – How do I put a certificate on Computers & Mobile Devices?

✓ AAA – Security of Device/User, Has Certificate been moved?

✓ Validation – What is required to check the Certificate?

✧ Management – Certificate, Dynamic Access Policies, and LDAP
CA Server – Windows 2008

ASDM Syslog Tool

- debug dap
- debug ldap
Management
CA Server MMC snap-in

- Verify/Revoke/Pending Requests

- To find a Certificate use Filter on CN
Certification validation
  - Fields in the certificate can be used for comparison to CA

Certificate chain was successfully validated with revocation status check.
Certificate was successfully validated. serial number: 1B8C47AD00000001F, subject name: ea=ned@securemobility.net, cn=ned, ou=Mobility, o=Cisco Systems, l=Houston, st=TX, dc=securemobility.net.
Certificate was successfully validated. Certificate is resident and trusted, serial number: 581D32BB283BE68F498E89AA6EDBB3, subject name: cn=securemobility-ca, dc=securemobility, dc=net.
Management
ASA Certificate Debugging

CLI Debug Commands:
- logging class ca console debug
- debug crypto ca 3
- debug crypto ca transaction 3
- debug crypto ca message 3
- debug crypto ca scep-proxy 1
Management

Debug DAP

- CLI: debug dap [trace | error]
- Define logging filter for DAP debugging to show up in ASDM syslog tool

Example output of DAP in ASDM
Management

Debug LDAP

- Since DAP included LDAP lookup, all the LDAP attributes are displayed
- Especially useful when configuring authorization rules against LDAP database

```
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.Idap.memberOf.4 = Enterprise Admins
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.Idap.memberOf.3 = Domain Admins
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.Idap.memberOf.2 = SecureMobilityGroup
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.Idap.memberOf.1 = IronPort-Operator
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.Idap.uSNCreated = 89829
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.Idap.displayName = Ned Zaldivar
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.Idap.whenChanged = 20120403191759.0Z
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.Idap.whenCreated = 20110922152048.0Z
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.Idap.instanceType = 4
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.Idap.distinguishedName = CN=Ned Zaldivar,OU=CSE,DC=securemobility,DC=net
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.Idap.givenName = Ned
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.Idap.description = CSE
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.Idap.sn = Zaldivar
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.Idap.cn = Ned Zaldivar
DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.Idap.objectClass.4 = user
```
Management

Device not authorized

deviceuniqueid NE ldap.extensionAttribute1

DAP: User ned, Addr 97.194.113.0: Session Attribute aaa.cisco.grouppolicy = getcert
DAP: User ned, Addr 97.194.113.0: Session Attribute aaa.ldap.msExchShadowProxyAddresses.2 = SMTP.ned@securemobility.net
DAP: User ned, Addr 97.194.113.0: Session Attribute aaa.ldap.msExchShadowProxyAddresses.1 = smtp.ned@securemobility.org
DAP: User ned, Addr 97.194.113.0: Session Attribute aaa.ldap.msExchRecipientTypeDetails = 1
DAP: User ned, Addr 97.194.113.0: Connection terminated by the following DAP records: Mobile_Device_Authorization
Case Study DEMO/VIDEO
In summary…

- Certificates excel at 2-factor auth or mobile platforms
- Certificates are easy to use
- Certificates can be made easy to deploy
- Certificates are the gift that keeps on giving
Additional Information Sources

Cisco Resources

- www.cisco.com/go/vpn
- www.cisco.com/go/anyconnect
- www.cisco.com/go/asa

Microsoft CA Server

Q & A
Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Passport points for each session evaluation you complete.
- Complete your session evaluation online now (open a browser through our wireless network to access our portal) or visit one of the Internet stations throughout the Convention Center.

Don’t forget to activate your Cisco Live Virtual account for access to all session material, communities, and on-demand and live activities throughout the year. Activate your account at the Cisco booth in the World of Solutions or visit www.ciscolive.com.
Final Thoughts

- Get hands-on experience with the Walk-in Labs located in World of Solutions, booth 1042
- Come see demos of many key solutions and products in the main Cisco booth 2924
- Visit www.ciscoLive365.com after the event for updated PDFs, on-demand session videos, networking, and more!
- Follow Cisco Live! using social media:
  - Facebook: https://www.facebook.com/ciscoliveus
  - Twitter: https://twitter.com/#!/CiscoLive
  - LinkedIn Group: http://linkd.in/CiscoLI
Extras
What Is a Certificate?

- Each client sends its public key and Identity information to a third party.
- That third party digitally "signs" the clients public key with its private key, binding it with identity information; this is a certificate.
- The trusted third party is called a certificate authority.
Optional: Device is present in LDAP

- MDM use case
- Aaa.ldap.extensionAttribute1
- Endpoint. anyconnect.deviceuniqueid
- If NE, then device is not authorized
AAA

Optional: Device / AD Authorization for Mobile

- Input Device ID into `extensionAttribute1`
- If multiple devices, leverage `extensionAttribute#`
- Device ID can be retrieved from syslog or require pre-registration of mobile devices.
- **Pre-registration is a best practice** because it lets you set standards for your IT to support.
Signature Verification Steps

- Separate the message from the signature

**Message**
1. Hash the message

**Signature**
1. Decrypt the signature using the public key
2. Decrypted signature should contain the hash of the message

If Hashes Are Equal
Signature Is Verified
Certificate Authorities

Additional Information

Microsoft CA server

IOS CA server

ASA CA server (limited to SSL client certificates only)
How to Export Local ASA CA Cert

Steps:
1. Copy ASA certificate chain (i.e. LOCAL-CA-SERVER.p12) to any PC with OpenSSL
2. "openssl pkcs12 -in LOCAL-CA-SERVER.p12 -out asa-ca.pem -nodes -nokeys"
3. Import asa-ca.pem to ‘other’ ASA’s via ASDM or CLI
4. Manually add CRL URL to ‘other’ ASA

** Note private keys do not need to be moved **
assert(function()
  for k,v in pairs(endpoint.certificate.user) do
    if (EVAL(v.md5_hash, "EQ", aaaldap.physicalDeliveryOfficeName, "string")) and
        (EVAL(endpoint.certificate.user.issuer_cn, "EQ", "Luis Jorge")) and
        (EVAL(EVAL(endpoint.device.id, "EQ", endpoint.certificate.user.subject_e, "string")))
        then
          return true
        end
  end
  return false
end)()
ASA Certificate Troubleshooting

Enable the following debugs when having issues with installing certificates or experiencing problems establishing IPsec/SSL VPN sessions.

- Logging enable
- Logging class ca console debug
- Debug crypto ca 3
- Debug crypto ca transaction 3
- Debug crypto ca message 3

Note: elevating the level to say 5 or 10 may be useful in some cases where more detail is required.
Cisco Jabber Secure Connect

[Diagram of the Cisco Jabber Secure Connect system, showing the integration of remote clients running the Cisco Jabber application with the enterprise network through SSL connections.]

Other applications do not have access to the enterprise network, while only Cisco Jabber applications have access to enterprise services.
Turn on OCSP

1. OCSP template - Add Enroll Permission to CA Computer account

2. Add Revocation Configuration from Online Responder Snap-in
OCSP Success

Online Responder Configuration

Use this snap-in to configure and manage one or more certificate revocation responders.

Overview

The Online Responder Management snap-in helps you configure and manage online certificate revocation authorities.

Use this tool to:
- Manage certificate revocation configurations for an Online Responder Array.
- Monitor the operating status of each member of an Online Responder Array.
- Manage Online Responder Array members.

Revocation Configuration Status

The Status pane identifies Online Responder configurations that are working properly or that require action. Select the Array members.

Note: You may need to click Refresh if recent configuration changes or other administrative actions have occurred.

For more information, see Verifying that a revocation configuration is functioning properly.

- denlab-oscp Working
Public Key Infrastructure (PKI)/CA Enrollment

Step 1: Generate Keys
- User's Keys
- End Host

Step 2: Certificate Request
- Certificate Authority

Step 3: Sign
- CA's Keys

Step 4: End Host's Certificate
- PRIV
- PUB