TOMORROW starts here.
Practical PKI for VPN
BRKSEC-2053

Jeff Fanelli
Technical Solutions Architect
Abstract

This intermediate level session will provide a technical overview and best practices for deploying X.509 certificates for two-factor authentication to support AnyConnect client.

A number of different SSLVPN use cases including bring your own device will be introduced and explained. The recommended solutions will focus on ease of use and manageability with detailed configuration examples. Technologies used include Cisco ASA and Cisco AnyConnect Secure Mobility using both Cisco and Microsoft public key solutions.

By the end of the session participants should grasp the major steps in X.509 certificate deployment and be able to make informed decisions about using certificate authentication with Cisco solutions.
A little bit about me…

Jeff Fanelli

Technical Solutions Architect – U.S. Enterprise

jefanell@cisco.com
Agenda

- Making the case for Certificates
- Best practices Deployment of Certificates for VPN
- Best Practices Case Study – Cisco AnyConnect with certificates
- Case Study Demo
- Q&A
Certificate Authority (CA)

The source of truth for any PKI

Certificate Authority Hierarchy of Trust

Certificate
Chain of Trust
The source of truth for any PKI
Types of Client Digital Certificates

1. User (identity) Certificates

2. Device / Computer (identity) Certificates

1. Hybrid Certificates
   - Multiple fields for different identity characteristics
   - (i.e. username + device serial number)
Certificate File Formats Demystified

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

- **PEM – Privacy Enhanced Mail**
  - (.pem .cer .crt)
  - Base64 encoded text
  - Can copy / paste

- **PKCS #7 (.p7b .p7c)**
  - Like PEM with root cert chain

- **PKCS #12 (.pfx .p12)**
  - Like PKCS #7 w/ Private Key!
How Identity Certificates Work
VPN Use Case – Exchange 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

- **Certificate Revocation List (CRL)**
  - Flat text file containing serial numbers of revoked certificates
  - May be retrieved via HTTP / LDAP

- **Delta CRL**
  - CRL “update” containing only “new” revoked serial numbers since last update
  - Limited Device / client support!

  - Protocol to request revocation status of an individual certificate serial number
  - Usually a dedicated server separate from Certificate Authorities
  - Requests can be digital signed *(must not require signing*, per RFC 2560)
Certificate Revocation Explained

- Certificate Revocation List
- Online Certificate Status Protocol

1) ASA Identity Certificate

CRL / OCSP Check

Private CA

Internet

2) Client Identity Certificate

CRL / OCSP Check

Public CA

Cisco ASA

VPN Client

Cisco ASA Internet VPN Client
How Identity Certificates Work
VPN Use Case – Parsing of Certificate Attributes

Subject (CN) & Subject Alternative Name (SAN) fields

Configure a certificate matching rule criterion

Rule Priority: 10
Mapped to Connection Profile: DefaultWEBVPNGroup

<table>
<thead>
<tr>
<th>Field</th>
<th>Component</th>
<th>Operator</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alternative Subject SAN</td>
<td>-- Whole Field --</td>
<td>Contains</td>
<td>sfd–dc–lab.cisc</td>
</tr>
</tbody>
</table>
How Identity Certificates Work
Forcing per user cert authentication

Username Mapping from Certificate
- Pre-fill Username from Certificate
- Hide username from end user
- Specify the certificate fields to be used as the username
  - Primary Field: CN (Common Name)
  - Secondary Field: OU (Organization Unit)
- Use the entire DN as the username
- Use script to select username

Screen shot of AnyConnect Secure Mobility Client showing a login prompt with a username of "ned" entered.

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public
BYOD Certificate Deployment

- SCEP Proxy “hides” CA Server from Client
- Client creates public / private key pair **locally** before sending Certificate Signing Request (CSR) inside of SCEP session
Certificate Use Cases

VPN is just one use case!

- Certificates are the gift that keeps giving
- Quickly increase corporate security in other areas
- Deploy once, use everywhere*

CLICK HERE TO SUBSCRIBE TO OUR BEER OF THE MONTH CLUB
AnyConnect Secure Mobility

- SSL and IPSec VPN Client
  - Certificate and / or two factor authentication support
- 802.1x network supplicant
  - EAP-TLS support
- Broad client device support
  - Windows, Mac, Apple iOS, Android, Linux
- Built-in SCEP support
  - Easy deployment of certificates
Wired and Wireless 802.1x Security Policy Example

Employee Rule

if

RegisteredDevices AND (Network Access: EapAuthentication EQUALS EAP-TLS AND CERTIFICATE: Subject Alternative Name EQUALS Radius: Calling-Station-ID AND AD1: ExternalGroups EQUALS cts.local/Users/Employees )

then

Employee
Many Other Use Cases for Identity Certs!
Common x.509 Certificate Myths!

- 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

- 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
Common Myths Busted!

- **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
  - Can be paired with local device lock / login requirement

- **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
Agenda

✓ Making the case for Identity-based Digital Certificates

○ Using best practices to Simplify the Deployment of Certificates

○ Best Practices Case Study – Cisco AnyConnect with certificates

○ Case Study Demo

○ Q&A
Our Two Deployment Goals

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>CA</td>
</tr>
<tr>
<td>Serial Number</td>
<td>4e0e8c39</td>
</tr>
<tr>
<td>Status</td>
<td>Available</td>
</tr>
<tr>
<td>Usage</td>
<td>General Purpose</td>
</tr>
<tr>
<td>Public Key Type</td>
<td>RSA (2048 bits)</td>
</tr>
<tr>
<td>Valid From</td>
<td>10:40:40 EST Nov 11 ...</td>
</tr>
<tr>
<td>Valid To</td>
<td>21:51:17 EST Nov 11 ...</td>
</tr>
<tr>
<td>Associated Trustpoints</td>
<td>Entrust 2012 CA Chain</td>
</tr>
<tr>
<td>Signature</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Identity General</td>
</tr>
<tr>
<td>Serial Number</td>
<td>4c1dbbf7</td>
</tr>
<tr>
<td>Status</td>
<td>Available</td>
</tr>
<tr>
<td>Usage</td>
<td>General Purpose</td>
</tr>
<tr>
<td>Public Key Type</td>
<td>RSA (2048 bits)</td>
</tr>
<tr>
<td>Valid From</td>
<td>17:33:22 EDT Sep 4 2012</td>
</tr>
<tr>
<td>Valid To</td>
<td>08:29:52 EDT Sep 5 2014</td>
</tr>
<tr>
<td>Associated Trustpoints</td>
<td>Entrust_Cert_2014</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>SHA1 with RSA Encryption</td>
</tr>
</tbody>
</table>
Certificate Deployment Considerations

Easy as 1-2-3 😊

- Choosing a Certificate Authority Solution
- Best Practice Configuration of CA Server
- Best practices for deploying device and user certificates on various device types
Certificate Authorities

Cisco Adaptive Security Appliance

Cisco Integrated Services Router

Microsoft Server Certificate Services
Cisco ASA Certificate Authority

Summary

- Free with ASA, no extra licensing
- Simple functions, limited scaling
- No support for High Availability (no clustering or failover of CA)
- Cannot be subordinate CA, only standalone Root
Cisco ASA Certificate Authority

Configuration Best Practices

- Small deployments only <50
- Manual Backup/Restore Regularly (all certificates and private keys stored in flash)
- Would not recommend Manual SCEP
- ASA Root CA can be manually exported for use in multiple ASA’s (see backup slides!)
Minimum configuration steps:

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

<table>
<thead>
<tr>
<th>Username</th>
<th>Email</th>
<th>Subject Name</th>
<th>Enrollment Status</th>
<th>Certificate Holder</th>
</tr>
</thead>
<tbody>
<tr>
<td>jfanelli</td>
<td>jefanell...</td>
<td>CN=cisco\jefanell...</td>
<td>allowed</td>
<td>no</td>
</tr>
</tbody>
</table>

Add User:

- Username: jfanelli
- Email: jefanell@cisco.com
- DN String: CN=cisco\jefanell,OU=Borderless Security Team,O=Cisc
ASA CA User Enrollment experience

From: asa-ca@cisco.com
Subject: Reminder: Certificate Enrollment Invitation
Date: April 3, 2012 9:05:30 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: 7036DE559ABE6CF6
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.sfd-dc-lab.cisco.com/+CSCOCA+/enroll.html

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

MD5: 5D1334D5 561B1179 EF2FF8B3 2C67A5D7
SHA1: DCA06E7A FDF448A6 7485ABE6 2A2E9436 214D27D5
Cisco ASA SSLVPN Connection Log

Group <Split_Policy> User <cisco\jefanell> IP <166.147.96.128> WebVPN session started.

DAP: User cisco\jefanell, Addr 166.147.96.128, Connection AnyConnect: The following DAP records were searched:

Group <DfltGrpPolicy> User <cisco\jefanell> IP <166.147.96.128> Authentication: successful, Session Type: Tunnel

Tunnel group search using certificate maps failed for peer certificate: serial number: 02, subject name: cn=

AAA retrieved default group policy (Split_Policy) for user = cisco\jefanell

Tunnel group search using certificate maps failed for peer certificate: serial number: 02, subject name: cn=

Certificate chain was successfully validated with revocation status check.
Certificate was successfully validated. serial number: 02, subject name: cn=cisco\jefanell, ou=Borderless
Microsoft Certificate Authority

- **Active Directory Certificate Services**
  - Windows Server 2008 R2 (Enterprise edition recommended)
  - Server 2012 (all editions)

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

On a AD plus IIS server…

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services.

Role Status

Messages: None
System Services: All Running
Events: None in the last 24 hours
Create Your Certificate Template

1. Open MMC > Certificates Snap-in

2. **Duplication Process:**
   - Select the certificate template you want to duplicate.
   - Click on **Duplicate Template.**

3. **Template Details:**
   - **Template display name:** Choose a name for your new certificate template.
   - **Template name:** Specify the name of the certificate.
   - **Validity period:** Set the validity period for the certificate.
   - **Renewal period:** Set the renewal period for the certificate.
   - **Publish certificate in Active Directory:** Check this option if you want to publish the certificate in the 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

- 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
Enable SCEP for non-AD joined Hosts
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

Go to Remote Access VPN > Certificate Management > Identity Certificates
How to Verify or Revoke a Certificate
See what certs have been issued

*CRL Validity is 1 week + 10% by default
## Solution Matrix: Certificate Authorities

<table>
<thead>
<tr>
<th>Capability / Feature</th>
<th>ASA</th>
<th>ISR</th>
<th>MS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy BYOD certs via VPN?</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Deploy BYOD certs wired or wireless?</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Deploy certs to Active Directory domain computers?</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Highly Scalable?</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Easily Manageable?</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
</tr>
</tbody>
</table>
Agenda

✓ Making the case for Identity-based Digital Certificates

✓ Using best practices to Simplify the Deployment of Certificates

○ Best Practices Case Study – Cisco Anyconnect SSLVPN with certificates

○ Case Study Demo

○ Q&A
Assumptions

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

And you understand the basics of:

- Connection Profiles/Tunnel Group
- Group Policy
- Dynamic Access Policy
- Host scan
Configuration Steps Overview

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

Microsoft Certificate Services:
- 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 ASA
- Does not need Pull Down List
- ASA communicates with CA
- Can use Single Connection Profile
- Requires ASA 8.4(1+)

**GPO**
- Supported for Domain joined devices only
- Easiest way to roll out User or Machine certificates
## Delivery

<table>
<thead>
<tr>
<th>secmob</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetCert</td>
<td>AAA(securemibility) Certificate</td>
</tr>
<tr>
<td>scep_proxy</td>
<td>AAA(securemibility) Certificate</td>
</tr>
</tbody>
</table>

- ✔ Enable Simple Certificate Enrollment Protocol (SCEP) for this Connection Profile
Without this feature:
- a device with a certificate will authenticate
- a device without a certificate will not be able to enroll
Client Profile

- Needed to support Machine Certs
- Not useable until profile is on machine
Delivery
AnyConnect SCEP / BYOD Use Case

Client Profile
- Requires CA URL
- Automatic SCEP Host – Certificate Enrollment Group
- %USER% as CN and/or Email used for User Authorization
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 [OPTION]

### 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

<table>
<thead>
<tr>
<th>Certificate Contents:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name (CN)</td>
</tr>
<tr>
<td>Department (OU)</td>
</tr>
<tr>
<td>Company (O)</td>
</tr>
<tr>
<td>State (ST)</td>
</tr>
<tr>
<td>State (SP)</td>
</tr>
<tr>
<td>Country (C)</td>
</tr>
<tr>
<td>Email (EA)</td>
</tr>
<tr>
<td>Domain (DC)</td>
</tr>
<tr>
<td>SurName (SN)</td>
</tr>
<tr>
<td>GivenName (GN)</td>
</tr>
<tr>
<td>Qualifier (GEN)</td>
</tr>
<tr>
<td>Qualifier (DN)</td>
</tr>
<tr>
<td>City (L)</td>
</tr>
<tr>
<td>Title (T)</td>
</tr>
<tr>
<td>CA Domain</td>
</tr>
<tr>
<td>Key Size</td>
</tr>
</tbody>
</table>
Delivery
Using Microsoft CA with GPO and SCEP/NDES

SCEP configuration for CA

Easiest way to deploy Certificates via Group Policy
Delivery
BYOD 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
Case Study Security Requirements:

- **Two-Factor** Authentication (certificate + password)
- **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

Two factor – Best practice for Non-Mobile.

Pre-Fill Username – Used to verify certificate to User
AAA
Check if user is authorized for connection.

User valid? - Verifies User is in AAA database

Pre-fill username from certificate for authorization
AAA
Common Authorization checks [OPTIONAL]

User AD group membership

Machine is Domain joined
AAA
Restrict while doing 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

## Device ID Awareness in ASA

<table>
<thead>
<tr>
<th>Platform</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>40-byte unique ID at installation + IMEI (GSM), ESN (CDMA) + MAC-Address</td>
</tr>
</tbody>
</table>

With Android and iOS devices other attributes are available.
AAA

Device Certificate is correct on Device

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

Requirements:
- Hostscan
- %MachineID% in certificate
Leverage field in AD like Aaa.ldap.extensionAttribute1
Endpoint. anyconnect.deviceuniqueid
If NE, then device is not authorized

Requirement:
Pre-registration of Device
Best Practice Essentials

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

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

  o Validation – What is required to check the Certificate?

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

- 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?

  o Management – Certificate, Dynamic Access Policies, and LDAP
Troubleshooting options:

- Client certificate verification
- Microsoft Certificate Services
- ASA Certificate Logging / debugging
- ASDM Syslog Tool
- Dynamic Access Policy + LDAP debugging

Monitoring and Reporting options:

- Cisco Security Manager
- Cisco Secure Access Server
- Cisco Identity Services Engine
- Cisco Prime Security Manager
Client Certificate Troubleshooting

- Chain of certificates may be incomplete

![Certificate Chain Diagram]

User Cert

CA Root Cert
MSFT CA Troubleshooting

Server Manager, Event Viewer and Certificate Services are FULL of info
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.
Event Monitoring - ASDM

Real-Time Log Viewer - tx.securemobility.net

<table>
<thead>
<tr>
<th>Syslog ID</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>734003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>734004</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Specify the filtering criteria to apply to syslog messages. Use commas to separate multiple criteria.

- **Date and Time**: O Real Time
- **Last**: 
- **Start Time**: Jan 07 2014 00:00:00
- **End Time**: Jan 28 2014 00:00:00

**Severity**: 
**Syslog ID**: 
**Source IP Address**: 
**Source Port**: 
**Destination IP Address**: 
**Destination Port**: 
**Description**: jefarem

**DAP**: User ned, Addr 76.31.26.206: Session Attribute aaa.Idap.givenName = Ned
**DAP**: User ned, Addr 76.31.26.206: Session Attribute aaa.Idap.userCertificate = 0...0........ C6.
**DAP**: User ned, Addr 76.31.26.206: Session Attribute aaa.Idap.description = CSE
**DAP**: User ned, Addr 76.31.26.206: Session Attribute aaa.Idap.sn = Zaldivar
**DAP**: User ned, Addr 76.31.26.206: Session Attribute aaa.Idap.cn = Ned Zaldivar
**DAP**: User ned, Addr 76.31.26.206: Session Attribute aaa.Idap.objectClass.4 = user
**DAP**: User ned, Addr 76.31.26.206: Session Attribute aaa.Idap.objectClass.3 = organizationalPerson
**DAP**: User ned, Addr 76.31.26.206: Session Attribute aaa.Idap.objectClass.2 = person
**DAP**: User ned, Addr 76.31.26.206: Session Attribute aaa.Idap.objectClass.1 = top

AAA transaction status ACCEPT : user = ned
AAA retrieved default group policy (secmob) for user = ned
AAA user authorization Successful : server = 10.20.1.1 : user = ned
Device completed SSL handshake with server inside:10.20.1.1/32961
SSL server inside:10.20.1.1/32961 requesting our device certificate for authentication.
Starting SSL handshake with server inside:10.20.1.1/32961 for TLSv1 session.
Built outbound TCP connection 3817205 for inside:10.20.1.11/636 (10.20.1.11/636) to identity:10.20.1.1/32961 (10.20.1.1/32961)
Device completed SSL handshake with client outside:76.31.26.206/32564
Teardown TCP connection 3817204 for inside:10.20.1.11/389 to identity:10.20.1.11/51187 duration 0:00:00 bytes 266 TCP Reset
Certificate chain was successfully validated with revocation status check.
Certificate was successfully validated. serial number: 3F7A92E90000000000328, subject name: e-ned@securemobility.net.cn=ned, cert valid: 3F7A92E90000000000328.0.
ASDM Troubleshooting

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
ASDM Troubleshooting

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.lap.memberOf=4 = Enterprise Admins |
| DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.lap.memberOf=3 = Domain Admins |
| DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.lap.memberOf=2 = SecureMobilityGroup |
| DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.lap.memberOf=1 = IronPort-Operator |
| DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.lap.sNCRreated = 89829 |
| DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.lap.displayName = Ned Zaldívar |
| DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.lap.whenChanged = 20120403191759.0Z |
| DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.lap.whenCreated = 20110922152048.0Z |
| DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.lap.instanceType = 4 |
| DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.lap.distinguishedName = CN=Ned Zaldívar,OU=CSE,DC=securemobility,DC=net |
| DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.lap.givenName = Ned |
| DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.lap.description = CSE |
| DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.lap.sn = Zaldívar |
| DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.lap.cn = Ned Zaldívar |
| DAP: User ned, Addr 76.31.28.1: Session Attribute aaa.lap.objectClass=4 = user |
Event Monitoring- Cisco CSM 4.2+
Reporting – ACS5.x/ISE 1.x and CSM 4.2+
Logging / Reporting – PRSM for NGFW

Traffic by locations

- Remote access VPN: 22.2 MB
- Local: 62 GB

Top sources

<table>
<thead>
<tr>
<th>Transactions</th>
<th>Data usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>MacOS</td>
<td>11.8 MB</td>
</tr>
<tr>
<td>Android</td>
<td>10.4 MB</td>
</tr>
</tbody>
</table>

User devices

| MacOS | 04/30/2013 9:02:50 AM | HTTP Complete | 172.16.31.1 | 192.168.1.13.5000 | 5000 | HyperText Transfer Protocol |
| MacOS | 04/30/2013 9:02:50 AM | HTTP Complete | 172.16.31.1 | 192.168.1.13.5000 | 5000 | HyperText Transfer Protocol |
| MacOS | 04/30/2013 9:02:50 AM | HTTP Complete | 172.16.31.1 | 192.168.1.13.5000 | 5000 | HyperText Transfer Protocol |
| Android| 04/14/2013 2:47:52 PM| HTTP Complete | 172.16.31.1 | 192.168.1.137    | 80   | HyperText Transfer Protocol |
| Android| 04/14/2013 2:47:49 PM| HTTP Complete | 172.16.31.1 | 192.168.1.137    | 80   | HyperText Transfer Protocol |
Demos!!!
In Summary

✓ 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 with certificates

✓ Case Study Demo
Q & A
Wrap up!
Certificates excel at 2-factor authentication or mobile platform authentication

Certificates are easy to use

Certificates can be made easy to deploy

Certificates are the gift that keeps on giving
Related Cisco Live Breakout Sessions!

- **BRKSEC-2045** – Mobile Devices and BYOD Sec. – Deploy and Best Practices
  - Wednesday 2:30PM

- **BRKSEC-2697** – Remote Access using Clientless VPN
  - Wednesday 4:30PM

- **BRKSEC-2881** – VPN Remote Access with IOS & Introduction to FlexVPN
  - Tuesday 4:45PM

- **BRKSEC-3033** – Advanced AnyConnect Deployment and Troubleshooting with ASA
  - Friday 11:30AM
Call to Action…

Visit the World of Solutions:-

- Cisco Campus
- Walk-in Labs
- Technical Solutions Clinics

- Meet the Engineer

- **Lunch Time Table Topics**, held in the main Catering Hall

- **Recommended Reading**: For reading material and further resources for this session, please visit [www.pearson-books.com/CLMilan2014](http://www.pearson-books.com/CLMilan2014)
Complete Your Online Session Evaluation

- Complete your online session evaluation
- Complete four session evaluations and the overall conference evaluation to receive your Cisco Live T-shirt
Extras
Additional Information Sources

Cisco Resources

- www.cisco.com/go/vpn
- www.cisco.com/go/anyconnect
- www.cisco.com/go/asa
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.
Advantages of Certificates

- **Two-factor Authentication** using Identity Certificate (What you need) plus username/password (What you have)
  - 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
### 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>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<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>
Summary on GPO Certs / Auto Enrollment

Easy but be careful!

5 Steps – Almost too easy!

1) Duplicate/Modify Template (User / Computer)
2) Security - Group (Domain Users/ Domain Computers)
3) Permissions - set Autoenroll to deny
4) Publish
5) Domain Policy Change enabling auto enrollment (Computer and User)
6) Verify and then Go back to Template Permissions -> set Autoenroll to Allow
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 3rd party on premise or cloud service
  - Tightly integrated with Cisco ASA
  - Streamlined enrollment process
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
AAA
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.
ASA SCEP Proxy Connection Flow

AnyConnect handles with and without Certificate
Management
Certificate Validation from Syslog

Certification validation:
- Fields in the certificate can be used for comparison to CA
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.Idap.msExchShadowProxyAddresses.2 = SMTP.ned@securemobility.net
DAP: User ned, Addr 97.194.113.0: Session Attribute aaa.Idap.msExchShadowProxyAddresses.1 = smtp.ned@securemobility.org
DAP: User ned, Addr 97.194.113.0: Session Attribute aaa.Idap.msExchRecipientTypeDetails = 1
DAP: User ned, Addr 97.194.113.0: Connection terminated by the following DAP records: Mobile_Device_Authorization
Signature Verification Steps
Separate the message from the signature.

1. Hash the message

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

Active Directory Certificate Services

IOS CA server

ASA CA server (limited to SSL client certificates only)

Public Key Cryptography Services
http://en.wikipedia.org/wiki/PKCS
Demos

- Untrusted Certificate and Manual SCEP example
  - http://www.youtube.com/watch?v=j6CS2R2x1ZY

- Getting certificate using Scep Proxy
  - http://www.youtube.com/watch?v=l6W7gw3f94A

- Debug of Revoked Certificate Authentication
  - http://www.youtube.com/watch?v=Un_S_uJ4M1Q

- Debug of Good Certificate Authentication
  - http://www.youtube.com/watch?v=i6oFg-VsaG0

- Certificate Authentication with Prefill End User Experience
  - http://www.youtube.com/watch?v=zyGXCKITxQ8
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", aaa.ldap.physicalDeliveryOfficeName, "string"))
      and (EVAL(endpoint.certificate.user.issuer_cn, "EQ", "Joe Smith"))
      and (EVAL (EVAL(endpoint.device.id, "EQ", endpoint.certificate.user.subject_e, "string")) )
      then
      return true
    end
  end
  return false
end)()
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
GPO Authorization
Just in case

Verify GPO policies allow certificates to be used for authentication
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 attention. 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-ocsp: Working
A Debug of Valid Cert

CRYPTO_PKI: Certificate validation: Successful, status: 0
CRYPTO_PKI: Attempting to retrieve revocation status

CRYPTO_PKI: Starting CRL revocation check.
CRYPTO_PKI: Attempting to find cached CRL for CDP ldap://CN=securemobil
20Services,CN=Services,CN=Configuration,DC=securemobility,DC=net?certifi
stributionPoint
CRYPTO_PKI: Select DER crl(cn=securemobility-ca,dc=securemobility,dc=net
CRYPTO_PKI: Found CRL in cache for CDP: ldap://CN=securemobility-ca,CN=
,CN=Services,CN=Configuration,DC=securemobility,DC=net?certificateRevoca
Point, status 0.

CRYPTO_PKI: Certificate is not revoked!

CRYPTO_PKI:Certificate validated. serial number: 10DC0F90000000000370, s
=ned,ou=Employee,o=SCEPPROXY,l=Houston,st=TX.
A Debug of Revoked Cert

//RYPTO_PKI: Starting CRL revocation check.
//RYPTO_PKI: Attempting to find cached CRL for CDP ldap:////CN=securemobility-ca,CN=Services,CN=Configuration,DC=securemobility,DC=net?certificateRevocationPoint
//RYPTO_PKI: Select DER crl(cn=securemobility-ca,dc=securemobility,dc=net)
//point, status 0.
//RYPTO_PKI: Certificate is revoked!

//ERT-C: I crlstat.c(485) : Error #751h

//ERROR: Certificate validation failed, Certificate is revoked, serial number: 205F,Z=ned@securemobility.net,cn=ned,ou=Mobility,o=SCEP,l=Houston,st=TX,dc=securemobility
Management
Debug Cert

Debug of Valid Cert Chain

CRYPTO_PKI: Sorted chain size is: 2
CRYPTO_PKI: Verifying certificate with serial number: 5B1032B82B6E98F498E09AAA6ED00B3, subject name: cn=securemobility-co,dc=securemobility,dc=net, issuer_name: cn=securemobility-ca,dc=securemobility,dc=net, signature alg: SHA1/RSA.

CRYPTO_PKI: Checking to see if an identical cert is already in the database...

CRYPTO_PKI(Cert Lookup) issuer="cn=securemobility-co,dc=securemobility,dc=net" serial number=5b 1d 32 bb 28 3b e5 8f 49 8e 89 aa d6 ed db b3 | [...]:...:1........

CRYPTO_PKI: looking for cert in handle=0x74373000, digest=-

CRYPTO_PKI: Found cert in database.

CRYPTO_PKI: Certificate is resident.

CRYPTO_PKI: Verify chain of certs, Getting public key from signersCert.

CRYPTO_PKI: Sorted chain size is: 1
CRYPTO_PKI: Found ID cert. serial number: 1000F9000000000570, subject name: e=ned@securemobility.net, cn=ned, ou=Employee, o=SCEPPROXY, l=Houston, st=TX
CRYPTO_PKI: Verifying certificate with serial number: 1000F9000000000570, subject name: e=ned@securemobility.net, cn=ned, ou=Employee, o=SCEPPROXY, l=Houston, st=TX, issuer_name: cn=securemobility-co,dc=securemobility,dc=net, signature alg: SHA1/RSA.

CRYPTO_PKI: Checking to see if an identical cert is already in the database...

CRYPTO_PKI(Cert Lookup) issuer="cn=securemobility-co,dc=securemobility,dc=net" serial number=10 dc 0f 90 00 00 00 00 03 70 | ........p