



Cisco *live!*

July 10-14, 2016 • Las Vegas, NV

Your Time Is Now

Advanced AnyConnect Deployment and Troubleshooting with ASA5500

Håkan Nohre, Consulting Systems Engineer, CISSP#76731, GIAC GPEN #9666

hnohre@cisco.com

BRKSEC-3033

What We Won't Cover

but may be covered in other Cisco Live sessions

- Clientless SSL VPN via Web Portal
- AnyConnect with IOS and IPSEC/IKEv2 : see BRKSEC-2881,BRKSEC-3054
- AnyConnect Web Security : see BRKSEC-2909
- AnyConnect NAM
- AnyConnect NVM: see BRKSEC-3014
- Roadmaps
- Licensing see BRKSEC-90666: Deploying Cisco Licensing (CCIE Licensing) ☺

The Scenario : Labrats

- Pharmaceutical Research **Conglomerate** *
run by Rats and Cats

* **Conglomerate**

two or more corporations engaged in entirely different businesses that fall under one corporate group

Wikipedia definition

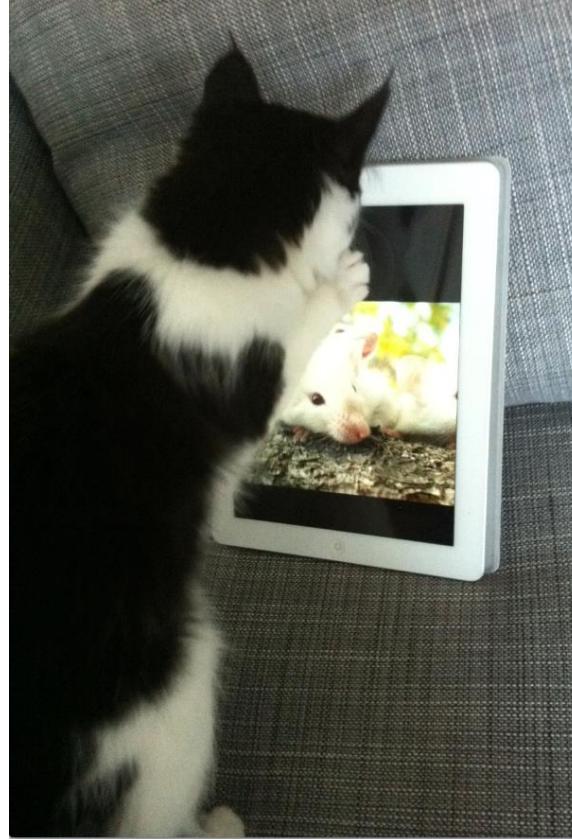
Legal Disclaimer

Any similarities between Labrats and any other organization is (most likely) a coincidence



The Scenario : Labrats

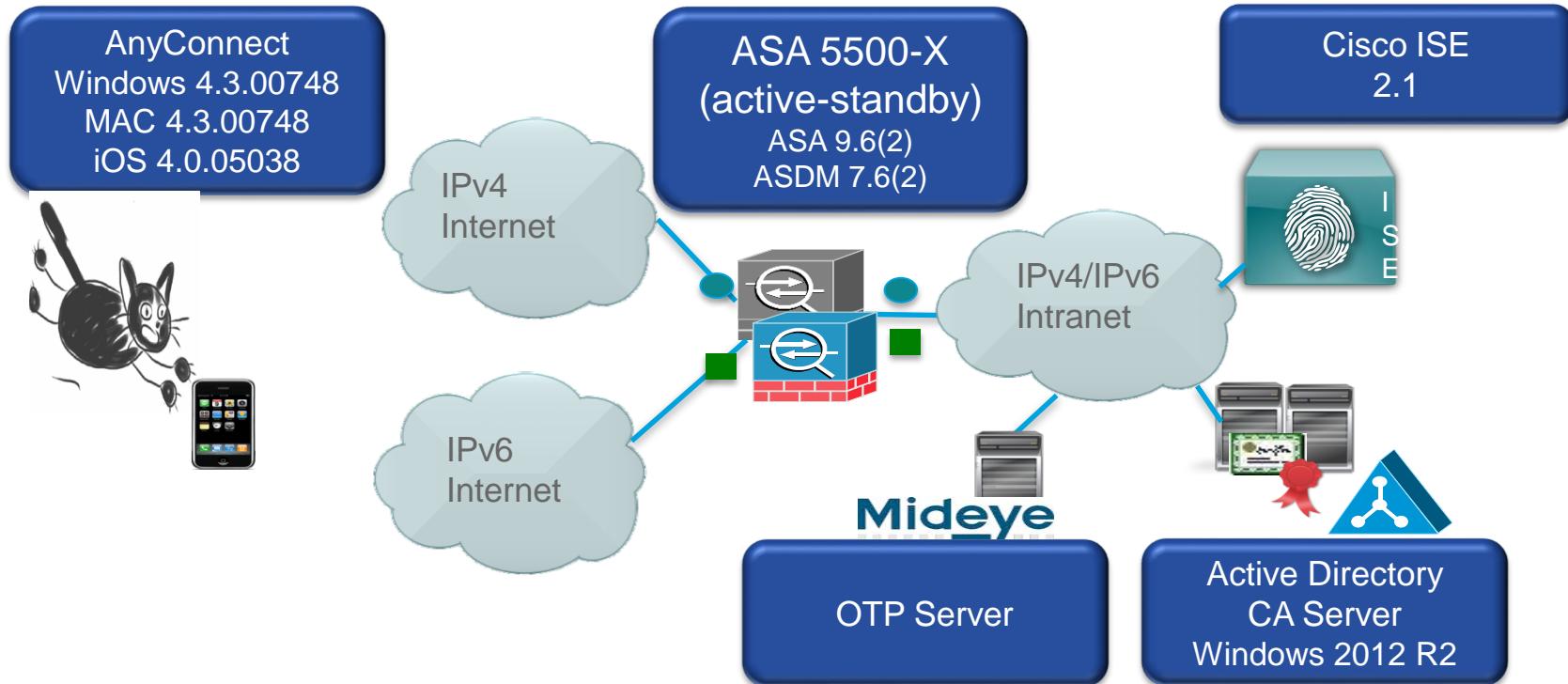
- Using Corporate Devices
 - Windows, MACs, iPADS
- Embracing BYOD
- **Key Requirements :**
 - Security
 - Easy to Use
 - IPv6



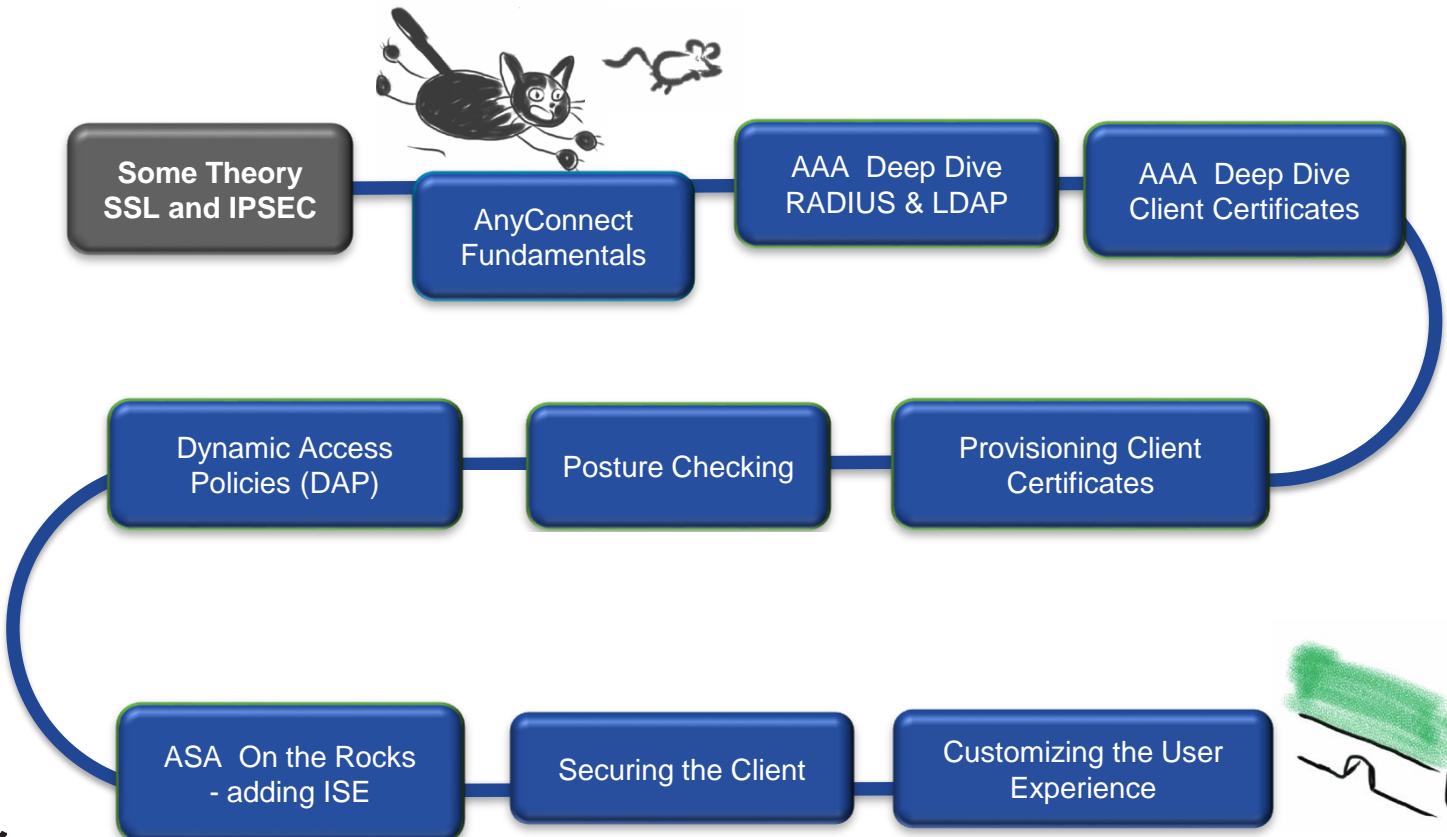


The Scenario : Labrats

- Network Design and Versions Used



Agenda



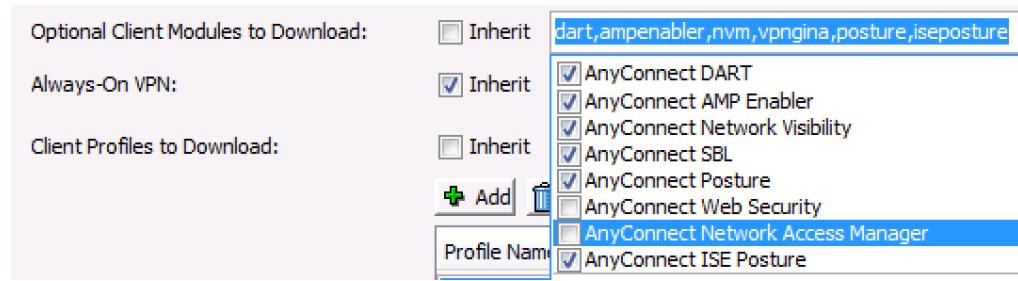


AnyConnect Windows Version Reminder!

- Versions older than 3.1MR13 or 4.2MR1 will no longer run on Windows from 2/14/2017
- Due to Microsoft code signing enforcement
 - <http://social.technet.microsoft.com/wiki/contents/articles/32288.windows-enforcement-of-authenticode-code-signing-and-timestamping.aspx>
 - http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect43/release/notes/b_Release_Notes_AnyConnect_4_3.html#reference_AA75AD8674C4409DBA57F2EBD9CAE3BB

AnyConnect - Installation

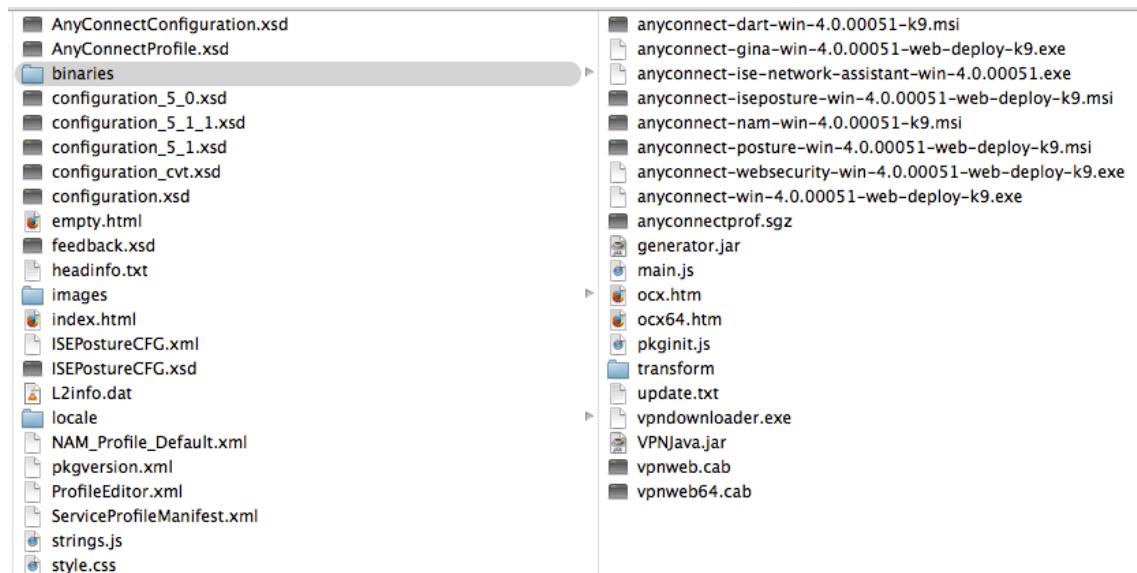
- Installation Options
 - download from ASA or ISE (requires admin privileges)
 - **use Desktop Management System**
 - **Appstore, Google Play ... (mobile devices)**
- Optional modules to install
 - **DART**
 - **Posture**
 - **ISE Posture**
 - **Start-Before-Login**
 - AMP Enabler
 - Web security, Network Access Manager
 - Feedback Module
 - Network Visibility



At least one pkg file needed

- At least one pkg file must be uploaded to ASA, even if AnyConnect pre-deployed on clients (MSI, Appstore...)
- pkg file contains binaries... and more
- To check out, rename pkg file to zip and decompress

Anyconnectxxx.pkg





On the Client: AnyConnect Configuration Files

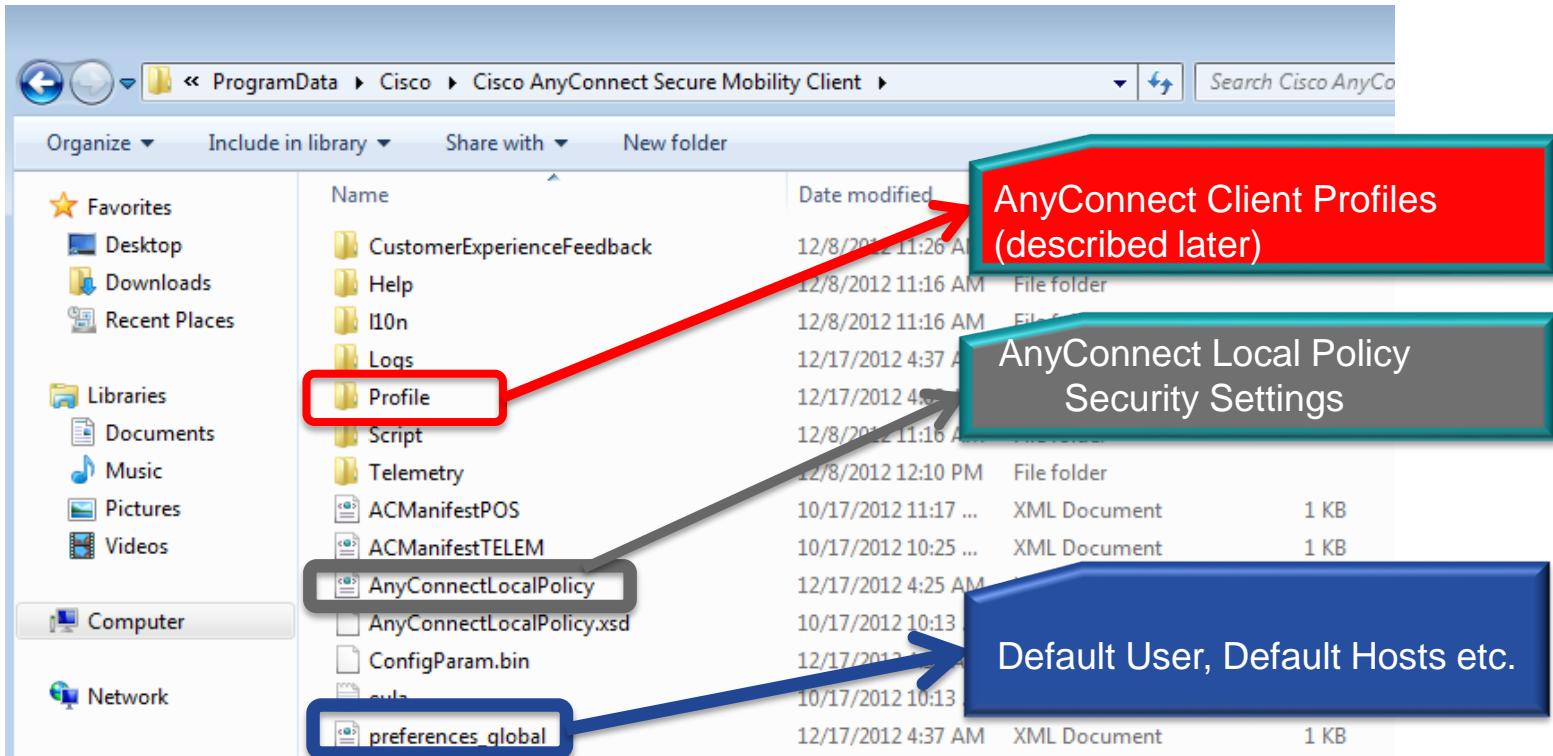
- AnyConnect Configuration Files are stored on the client in the following directories:

Windows 7 and Windows VISTA	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client
Windows XP	C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client
MAC OS X and Linux	/opt/cisco/anyconnect/

Windows 7 and Windows VISTA	C:\Users\username\AppData\Local\Cisco\Cisco AnyConnect VPN Client\preferences.xml
Windows XP	C:\Documents and Settings\username\Local Settings\ApplicationData\Cisco\Cisco AnyConnect VPN Client\preferences.xml
MAC OS X and Linux	/Users/username/.anyconnect

On the Client: AnyConnect Configuration Files

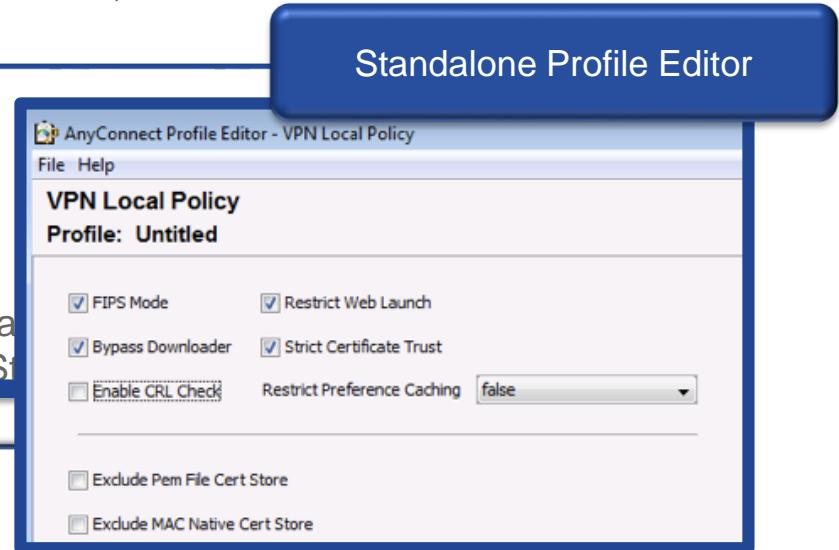
- Apply to all Users logged onto the machine



AnyConnect Local Policy File

- Not downloaded from ASA (use your favorite desktop management system)
- XML file defining important aspects of AnyConnect behavior
 - allowing user to accept untrusted ASA certificates
 - allowing client software updates from ASA (and from which ASAs)
 - allowing client profile updates from ASA (and from which ASAs)
 - certificate stores, credentials caching etc.

```
<FipsMode>true</FipsMode>
<BypassDownloader>true</BypassDownloader>
<RestrictWebLaunch>true</RestrictWebLaunch>
<StrictCertificateTrust>true</StrictCertificateTrust>
<EnableCRLCheck>false</EnableCRLCheck>
<RestrictPreferenceCaching>false</RestrictPreferenceCaching>
<ExcludePemFileCertStore>false</ExcludePemFileCertStore>
```



Local Policy File Example :

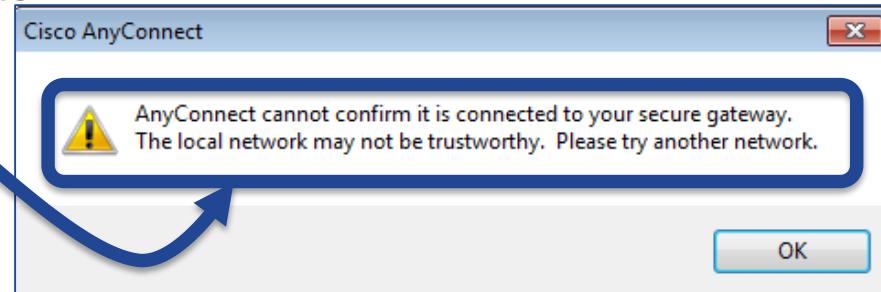
- If the server certificate is not trusted, do you want the user to be able to accept the certificate?

```
<StrictCertificateTrust>  
false  
</StrictCertificateTrust>
```

- or do you want AnyConnect to refuse to connect?

```
<StrictCertificateTrust>  
true  
</StrictCertificateTrust>
```

AnyConnect Local Policy



AnyConnect Troubleshooting Toolbox (Windows)



The screenshot shows the MMC console window with the title bar "MMC - [Console Root\Event Viewer (Local)\Applications and Services Logs\Cisco AnyConnect Secure Mobility Client]". The menu bar includes File, Action, View, Favorites, Window, and Help. The toolbar has icons for Back, Forward, Home, Favorites, and Help. The left pane displays a tree view of logs: Console Root, Certificates (Local Computer), Certificates - Current User, Event Viewer (Local), Custom Views, Windows Logs, Applications and Services Logs (expanded to show Cisco AnyConnect Diagnostics and Reporting Tool, Cisco AnyConnect Posture Module, Cisco AnyConnect Secure Mobility Client, Cisco AnyConnect Telemetry Module, Hardware Events, Internet Explorer). A blue rounded rectangle highlights the Applications and Services Logs section. The right pane shows a table of events:

Level	Date and Time	Source	Event ID	Task Categ...
Error	12/17/2012 4:51:00 AM	acvpnui	2	Engineering...
Information	12/17/2012 4:50:57 AM	acvpnagent	1	Engineering...
Information	12/17/2012 4:50:57 AM	acvpnui	1	Engineering...

Below the table, a details pane for "Event 2, acvpnui" is shown with tabs for General (selected) and Details, and options for Friendly View (radioed) and XML View. A "System" link is visible at the bottom.

MMC console with snap-ins:
Event Viewer
Certificate (Current User)
Certificate (Local Computer)

Function: ConnectMgr::run File:
.\\ConnectMgr.cpp Line: 683 Invoked
Function: ConnectMgr::initiateConnect Return
Code: -29622263 (0xFE3C0009) Description:
CONNECTMGR_ERROR_UNEXPECTED

AnyConnect Troubleshooting Toolbox (MAC)



Keychain Access

Click to lock the login keychain.

Keychains

- login
- Mac...ertificates
- System
- System Roots

Name

Category

- All Items
- Passwords
- Secure Notes
- My Certificates
- Keys
- Certificates

String Matching

Filter

Message

Function: getHostInitSettings File: ProfileMgr.cpp Line: 876 Profile () not found. Using default settings.

Function: processIfcData File: ConnectMgr.cpp Line: 2927 Certificate authentication requested from gateway, no valid certs found in users cert store.

Message type warning sent to the user: No valid certificates available for authentication.

Function: getUsername File: CTransportCurlStatic.cpp Line: 1905 PasswordEntry Username is blank.

Name	Date & Time	Sender[PID]	Message
DATABASE SEARCHES	2011-11-27 11.19.57	acvpnui [32880]	Function: getHostInitSettings File: ProfileMgr.cpp Line: 876 Profile () not found. Using default settings.
All Messages	2011-11-27 11.19.57	acvpnui [32880]	Function: processIfcData File: ConnectMgr.cpp Line: 2927 Certificate authentication requested from gateway, no valid certs found in users cert store.
Console Messages			Message type warning sent to the user: No valid certificates available for authentication.
DIAGNOSTIC AND USAGE IN...			Function: getUsername File: CTransportCurlStatic.cpp Line: 1905 PasswordEntry Username is blank.
Diagnostic and Usage Me...			
User Diagnostic Reports			
System Diagnostic Reports			
FILES			
system.log			
~/Library/Logs			
Adobe			
Cisco			
CrashReporter			
DavMail			
Mac...			

Earlier Later

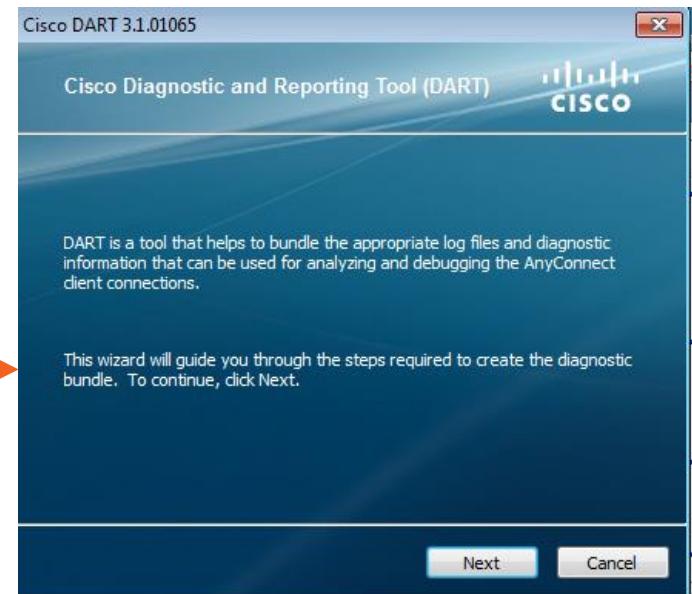
Utilities/Console
Utilities/Keychain Access





DART Tool (Windows and MAC)

- DART Tool can be installed with the client
- Similar to “show tech” on client
- Gathering of OS Data and log files in large zip file



AnyConnect Troubleshooting Toolbox (iOS, Android)



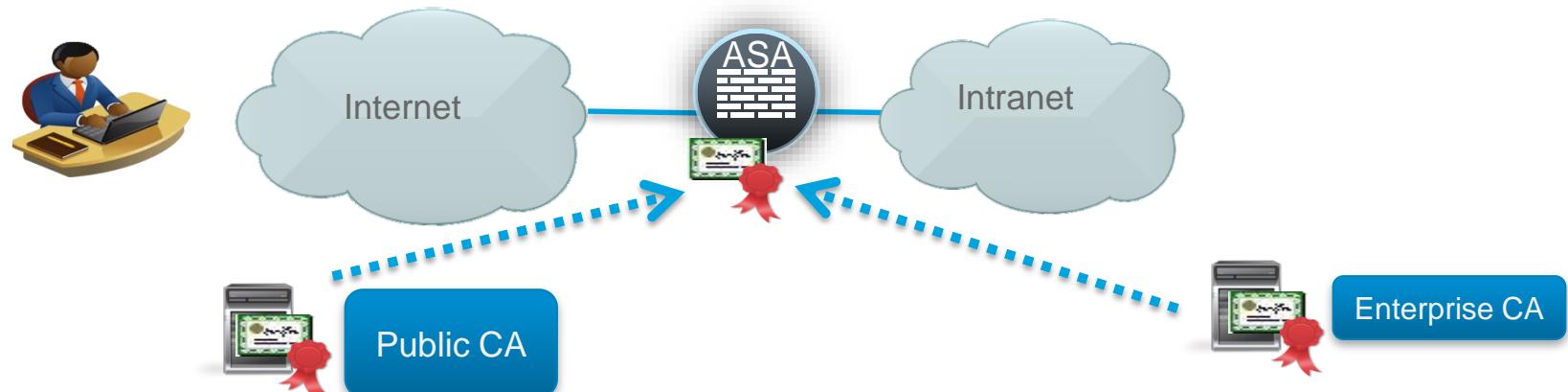
The screenshot shows the Cisco AnyConnect Secure Mobility Client application running on a mobile device. At the top, there is a status bar showing 'iPad' with signal strength, 'VPN' status, the time '7:04 AM', and a battery level of '90%'. The main screen has a dark blue header with the 'cisco' logo and 'AnyConnect Secure Mobility Client' text. Below the header, there is a 'AnyConnect VPN' toggle switch labeled 'ON'. A 'Status' section shows 'Connected'. A 'Choose a connection...' dropdown menu is open, showing two entries: 'rodgy.labrats.se' (selected) and 'rodgy.labrats.se (user)'. Below this is an 'Add VPN Connection...' button. On the right side of the screen, there is a navigation bar with three tabs: 'Graphs', 'Diagnostics' (which is highlighted with a red box), and 'Settings'. Under the 'Diagnostics' tab, there are three sections: 'Management', 'System Information', and 'Debug Logs'. The 'Management' section has a 'Details' button. The 'System Information' section also has a 'Details' button. The 'Debug Logs' section has a toggle switch labeled 'OFF'. Below the 'Diagnostics' tab, there is a large text area labeled 'Messages' containing a log of system events. At the bottom of the screen are two buttons: 'Clear Logs' and 'Email Logs...', with 'Email Logs...' highlighted by a red box.

Possible to view
Profiles and
Certificates

One click email of logs

AnyConnect Fundamentals : ASA Server Certificate

- ASA certificate should be trusted by clients
 - Public (well-known) Certificate Authority (e.g. Verisign, Thawte)
 - Enterprise Certificate Authority, e.g. Microsoft Active Directory
 - Self-Signed (need to import certificate to all clients)
 - AnyConnect 4.1: check of CRL is configurable (Local Policy File)
- FQDN in Subject



Ensure Clients Trust the ASA Certificate

- AnyConnect uses OS to validate certificate
 - Microsoft Windows: MS CAPI
 - MAC OS: Keychain
 - Linux: Varies with distribution
- Tip: Examine warnings with browser
 - Untrusted CA chain
 - Mismatch domain name
 - Validity time (GOT NTP?)

 **This Connection is Untrusted**

You have asked Firefox to connect securely to `roddy.labrats.se`, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

Technical Details

roddy.labrats.se uses an invalid security certificate.

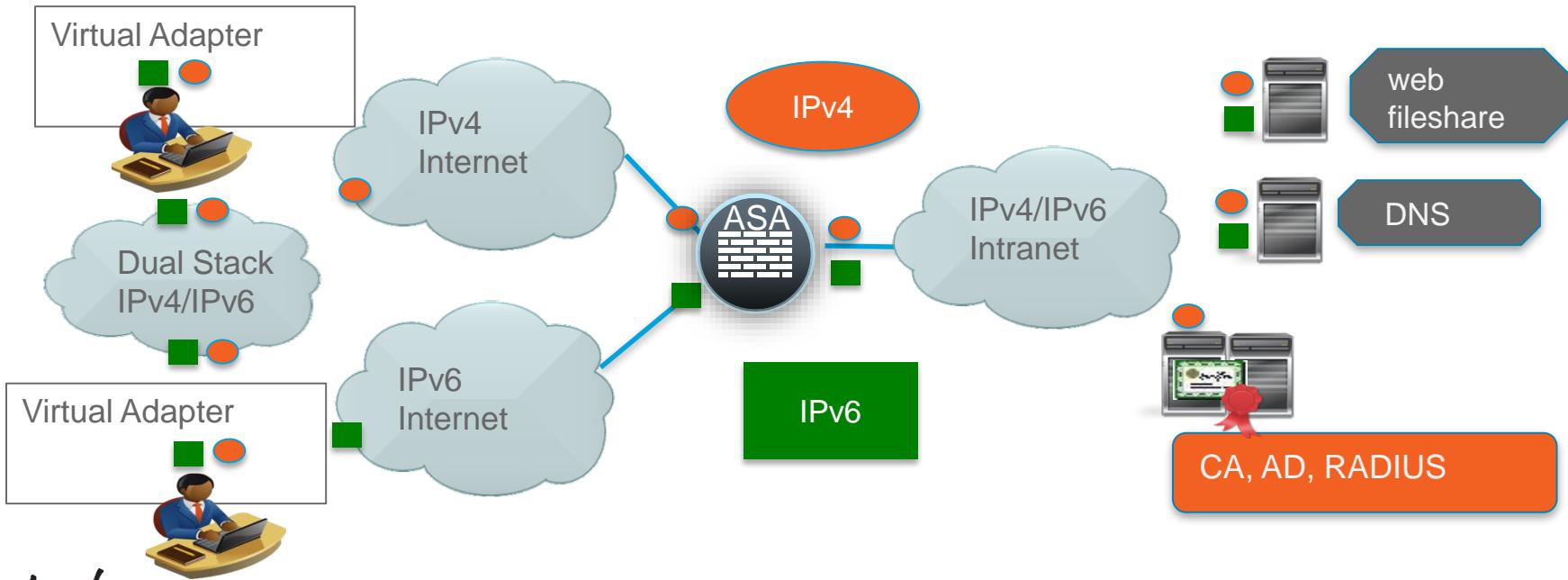
The certificate is not trusted because no issuer chain was provided.

(Error code: sec_error_unknown_issuer)

► [I Understand the Risks](#)

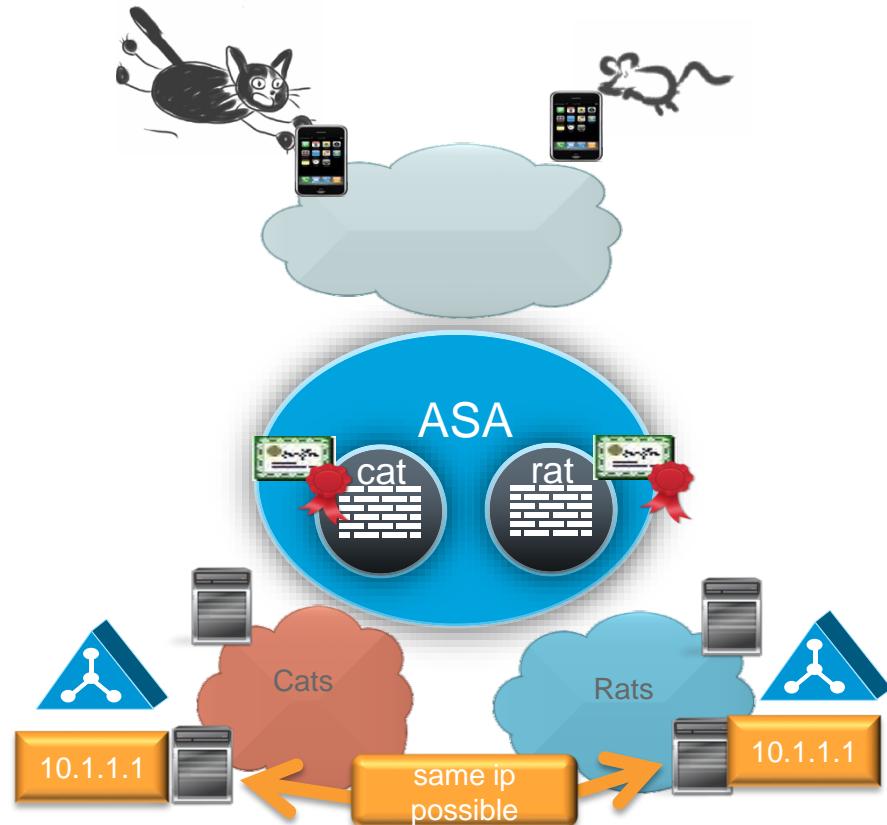
AnyConnect Fundamentals : IPv4 and IPv6

- AnyConnect 3.1 now supports **IPv6** tunneled inside **IPv4** or **IPv6**
 - management/control servers (CA, AD, RADIUS) IPv4 only

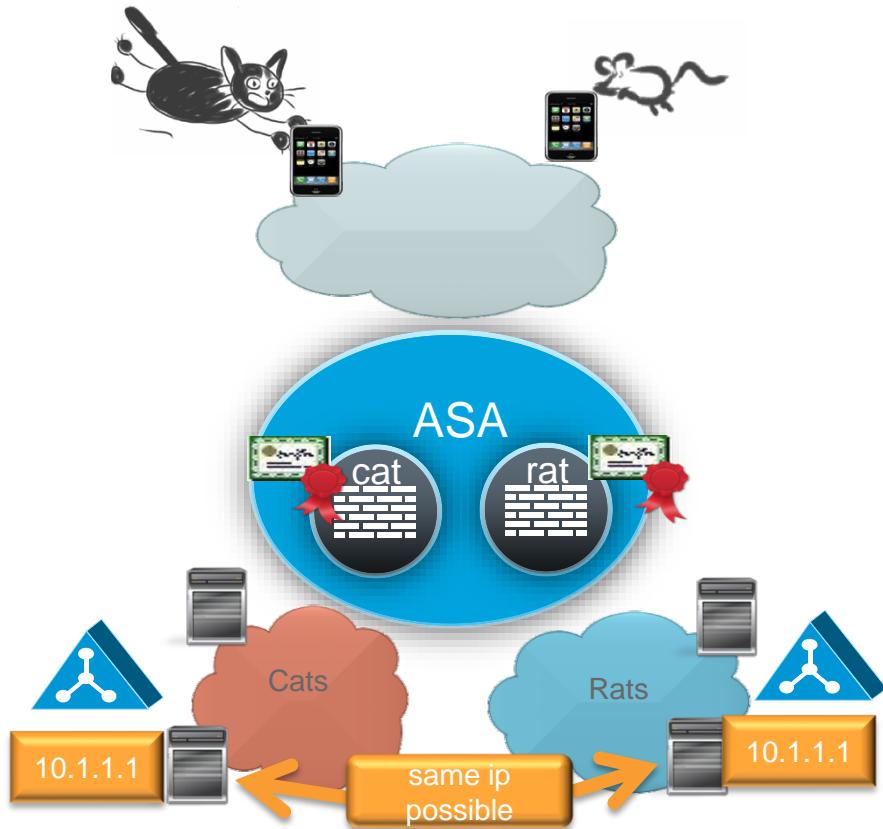


AnyConnect with Multiple Contexts

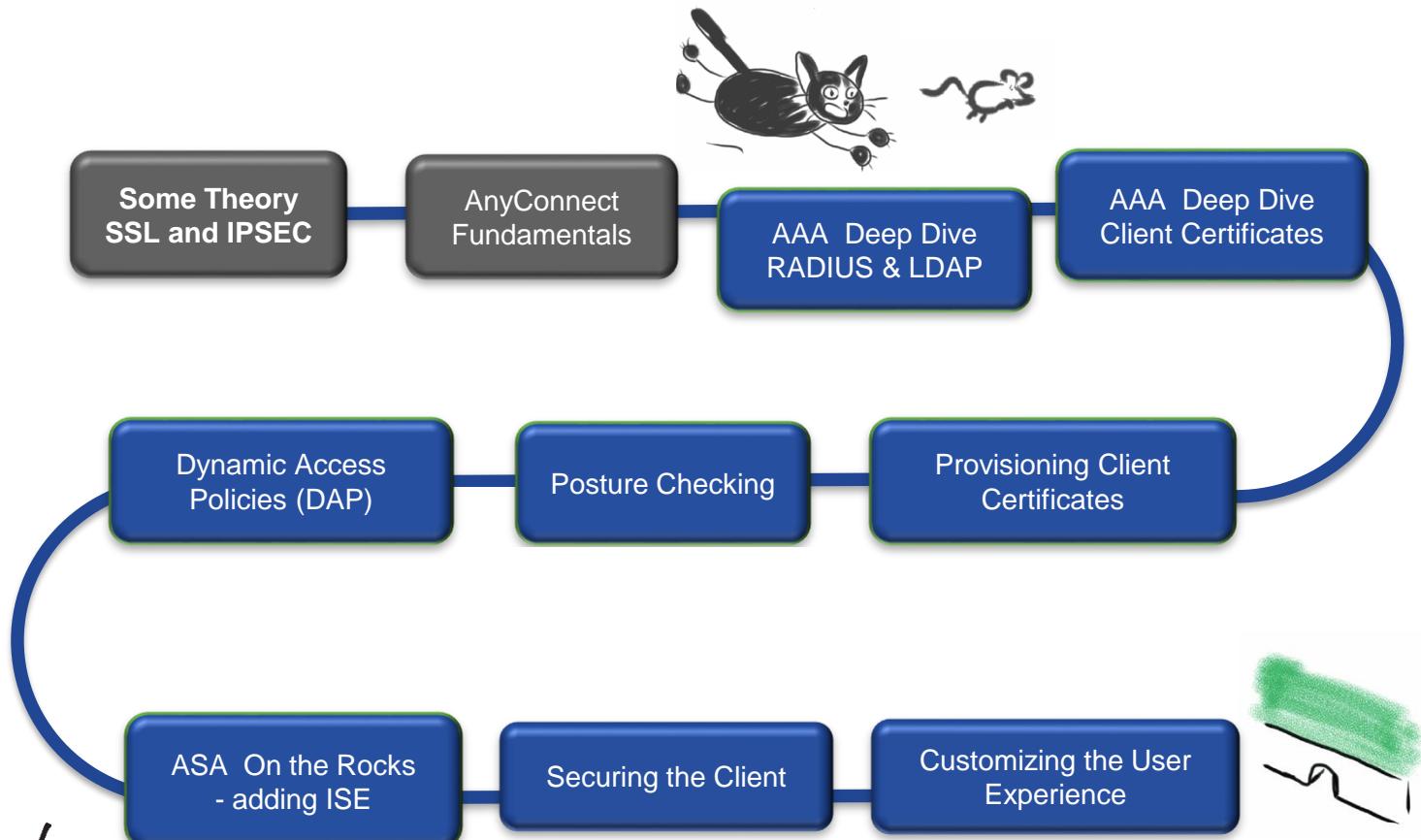
- ASA 9.5(1) and 9.6(2)
- One physical ASA with multiple contexts
- ...with unique configurations
 - Certificates,
 - AnyConnect images
 - Policies
- ...with separate management views
- ...with separate ip address spaces



When Pigs Fly: AnyConnect with Multiple Contexts



Agenda



AAA in ASA : Some Important Concepts

Connection Profile
(tunnel-group)

How to Authenticate
and Authorize

Group Policy

Client
Profile

Authorization

Proving Who you are

Static Passwords (local to ASA, Active Directory, LDAP)
OTP (One-Time-Passwords), typically RADIUS
Certificates



Determining What You are and What You can do

ACL, Split Tunnelling
Proxy settings, Timeouts
etc..

AnyConnect behaviour...

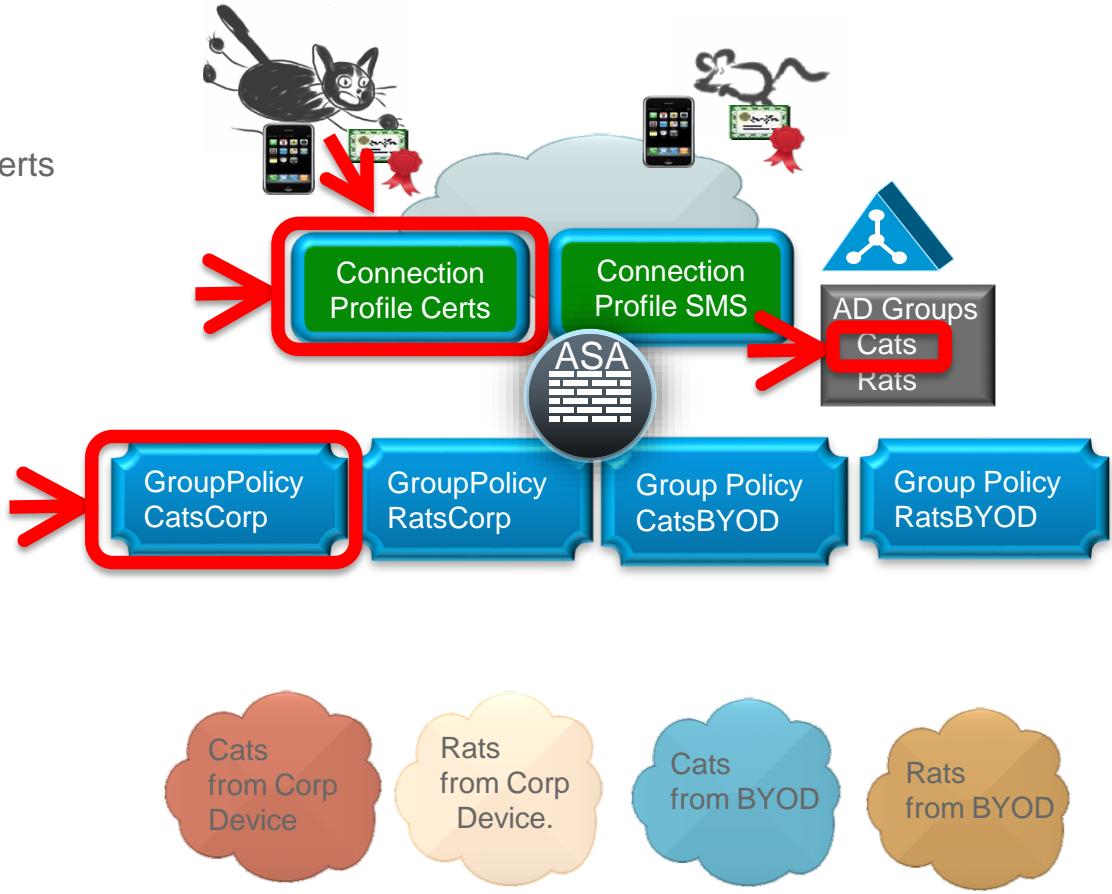
- Which ASA and Connection Profile to connect to
- "Always On"
- which certificate to use, etc...

Labrats Requirements

- Strong Authentication
 - Corporate devices (laptops, iPADs) use certs
 - BYOD use OTP sent as text to mobile
- Granular Authorization
 - Depending on Active Directory group **and** device (corporate vs. BYOD)
 - Access Rights differ with regards to

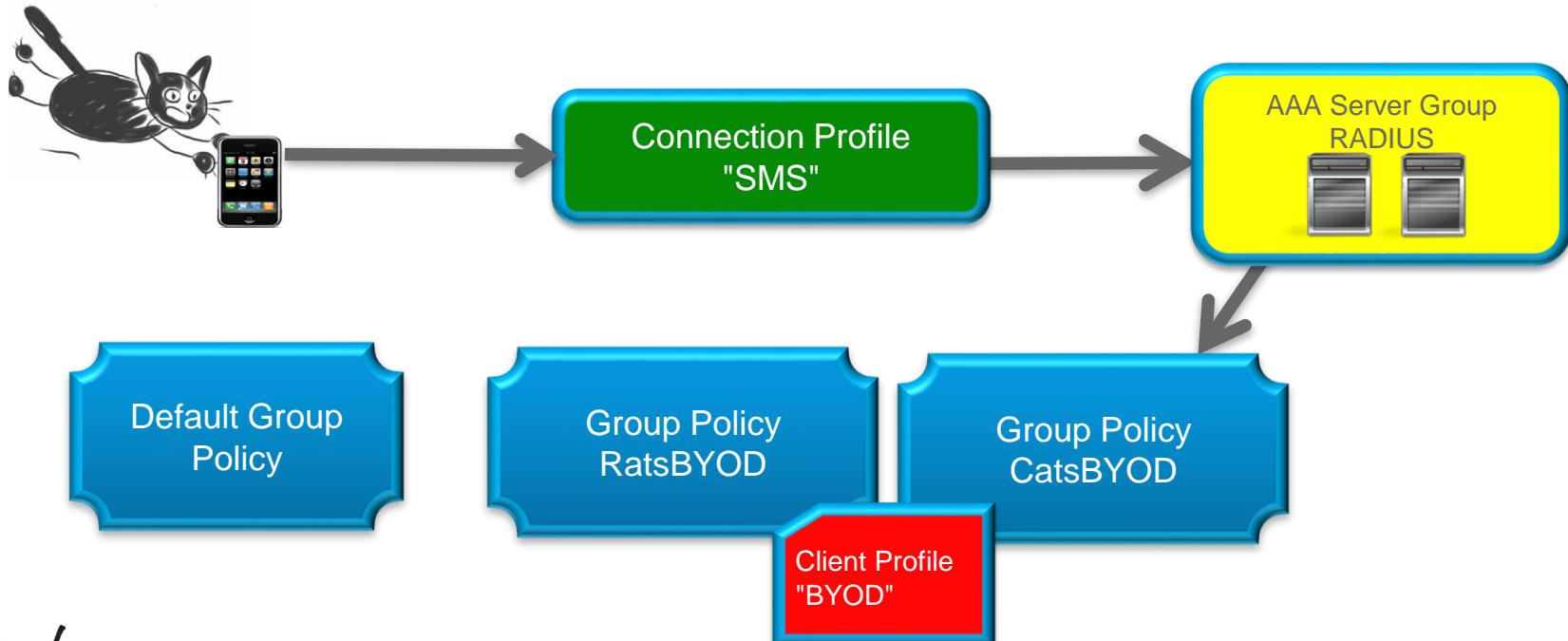
ACL (Filter)
IP address pool
Split Tunneling
Client Profile
Restrict to VLAN

...



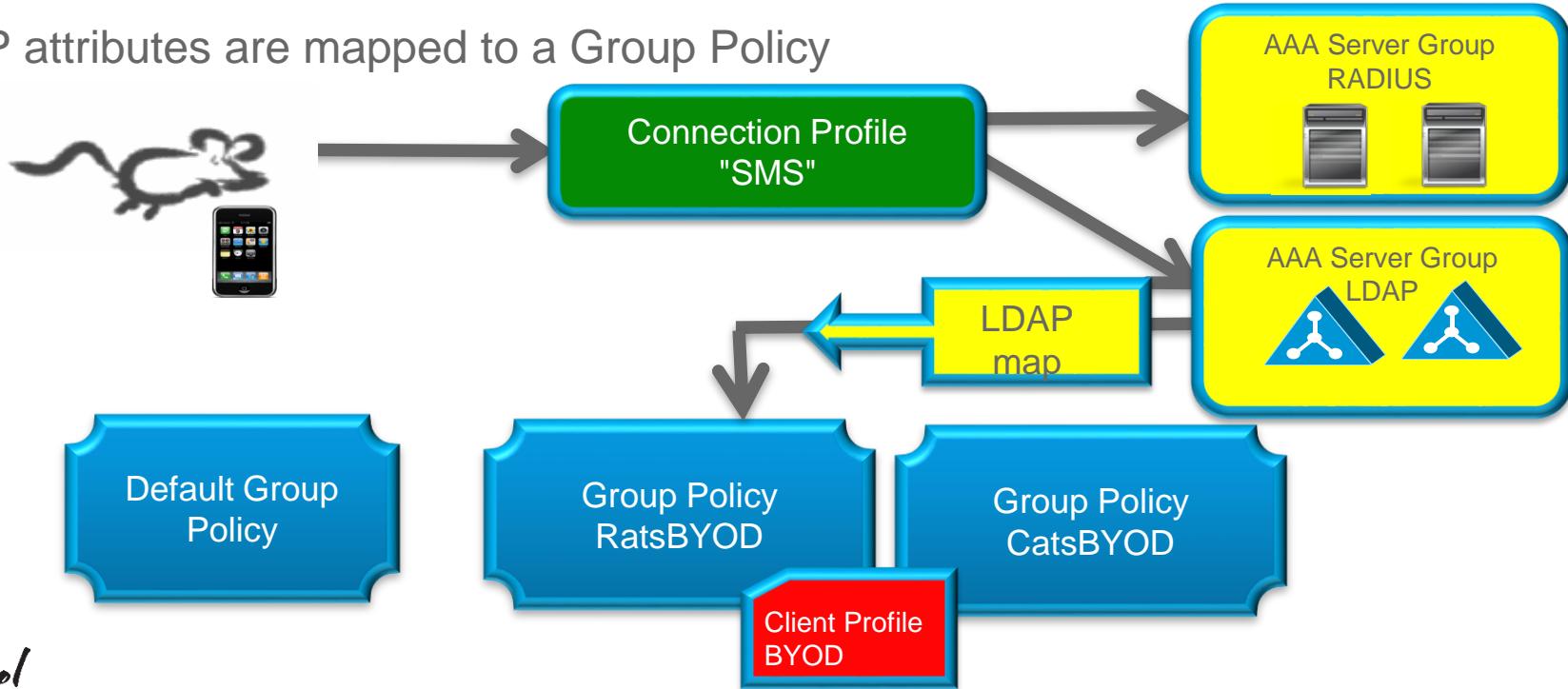
Authentication and Authorization by RADIUS

- User can be authenticated and authorized by RADIUS.
- RADIUS attribute IETF 25 (Class) is used to assign the group policy.



Authentication by RADIUS Authorization by LDAP

- User authenticated by RADIUS (typically strong authentication, OTP)
- Username used for LDAP lookup
- LDAP attributes are mapped to a Group Policy



Connection Profile : How to Authenticate

Edit AnyConnect Connection Profile: SMS-OTP

Basic

Name: SMS-OTP
Aliases: SMS

Authentication

Method: AAA Certificate Both

AAA Server Group: SMS

Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

None DHCP Link DHCP Subnet

Client Address Pools: pool4-Default

Client IPv6 Address Pools: pool6-Default

Default Group Policy

Group Policy: DfltGrpPolicy

AAA, Cert or Both?

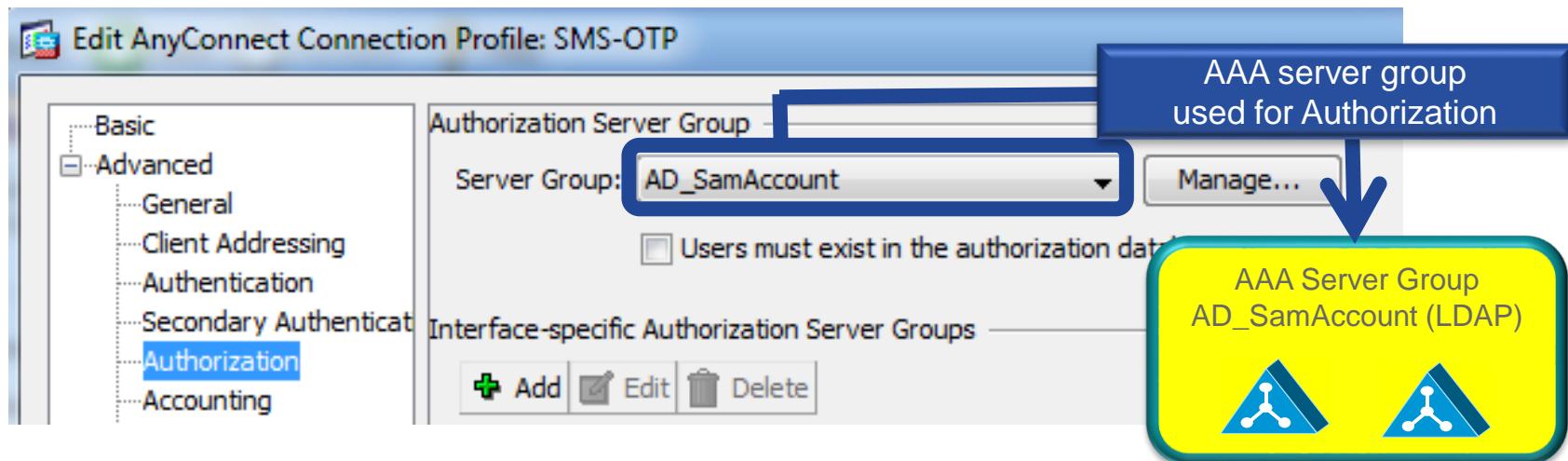
AAA server group

AAA Server Group RADIUS

Group-Policy used unless overwritten by Authorization Server

Connection Profile : How to Authorize

- Possible to define different AAA server group for authorization (if not specified, the same group is used for authentication and authorization).



Connection Profile: Where Send Accounting

- Possible to define AAA Server Group for RADIUS Accounting



In the AnyConnect Client Profile : Server List

- Specify servers in the server list
- Do not specify Host Address
 - May cause cert warnings
- Don't have the user choose connection profile
 - Save mouse clicks

The screenshot shows the AnyConnect Client Profile Editor interface with two main windows:

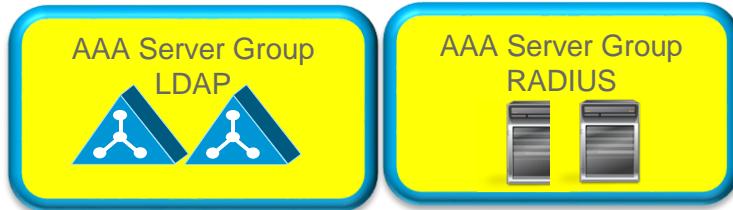
- AnyConnect Client Profile Editor - alwaysOn**: This window displays a "Profile:" sidebar with options like VPN, Preferences (Part 1), Preferences (Part 2), Backup Servers, Certificate Matching, Certificate Enrollment, Mobile Policy, and Server List. The "Server List" option is selected. A blue arrow points from this section to a red box labeled "Client Profile".
- Edit AnyConnect Connection Profile: Certs**: This window shows a "Basic" tab with "Advanced" sub-options: General, Client Addressing, Authentication, Secondary Authentication, Authorization, Accounting, and Group Alias/Group URLs. A green arrow points from the "Group URLs" section to a green box labeled "Connection Profile".

In the "Server List" section of the top window, there is a table with three columns: Hostname, Host Address, and User Group. One row is highlighted with a blue border, showing "Hostname: roddy.labrats.se", "Host Address: Blank", and "User Group: certs".

In the "Group URLs" section of the bottom window, there is a table with a single column labeled "URL". The first row is highlighted with a blue border, showing "https://roddy.labrats.se/certs". Below the table, a note states: "This SSL VPN access method will automatically select the" followed by "Add" and "Delete" buttons, and a note "(The table is in-line editable.)".

AAA Server Groups

- Using the same authentication protocol and characteristics



[Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups](#)

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Logins
AD_SamAccount	LDAP		Depletion	10	3
AD_UPN	LDAP		Depletion	10	2
LOCAL	LOCAL				
SMS	RADIUS	Single			

Add Edit Delete

Find: Match Case

Servers in the Selected Group

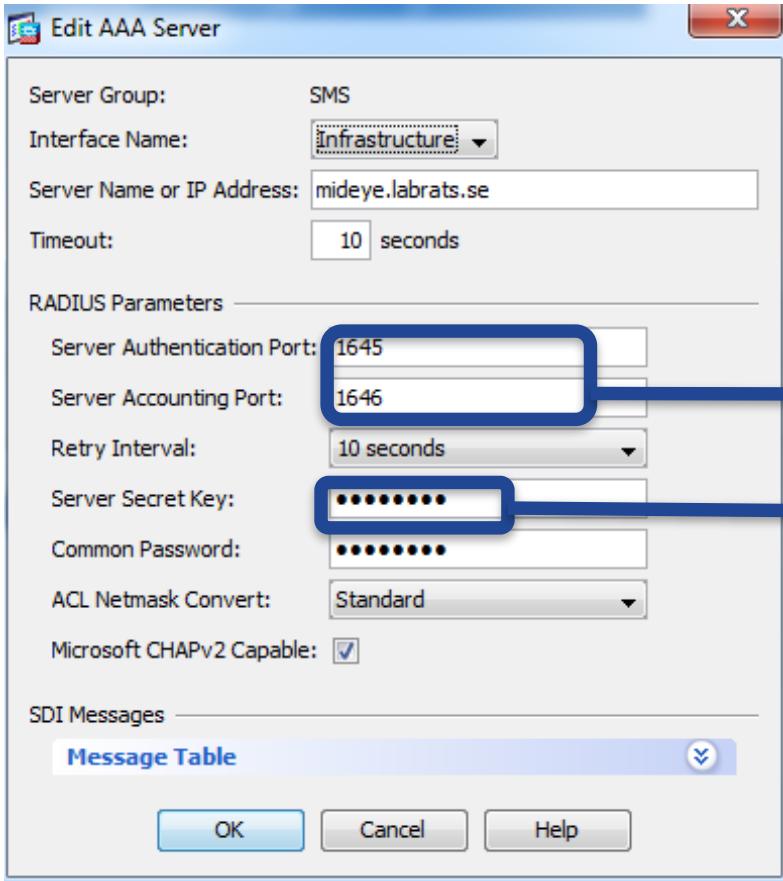
Server Name or IP Address	Interface	Timeout
ratbert.labrats.se	Infrastructure	10
ratatouille.labrats.se	Infrastructure	10

Add Edit

Same Protocol but different Groups if different characteristics

Several Servers in a Group for redundancy

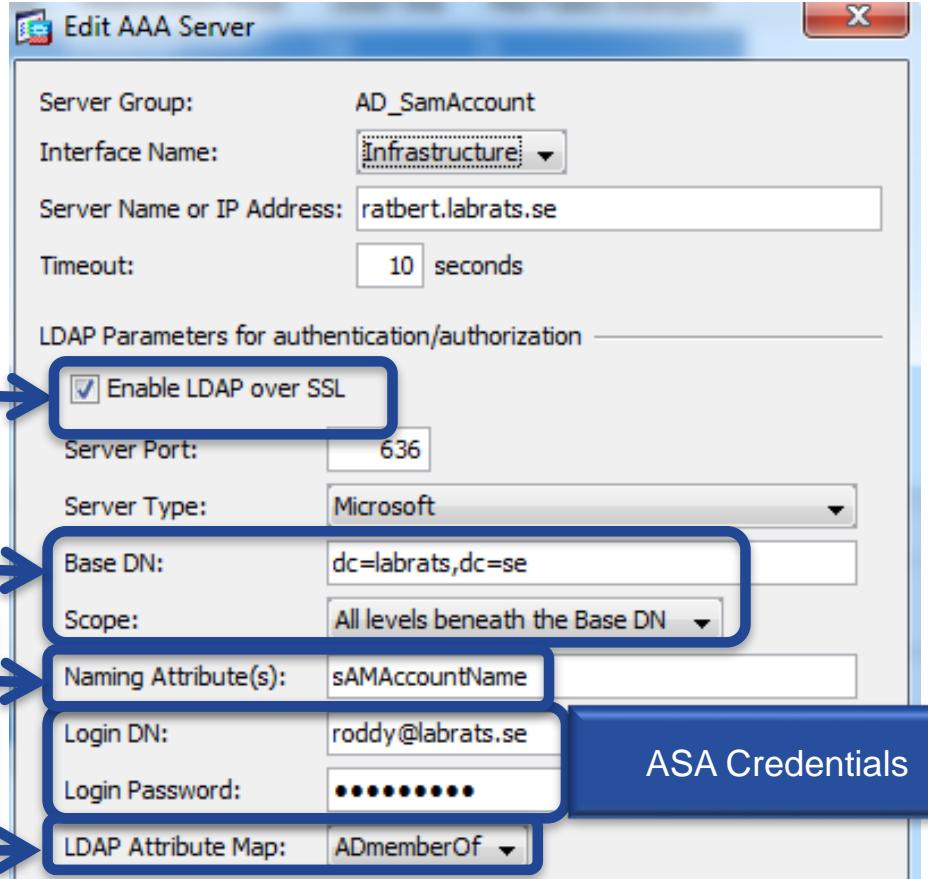
RADIUS Server Definition



Double check port numbers on RADIUS server

Shared Secret must match with RADIUS server

LDAP Server Definition (Active Directory)



LDAP over SSL

Domain is labrats.se

Attribute for user lookup

Map LDAP attributes to ASA attributes (to be covered)

ASA Credentials

A Good LDAP Browser is Useful



- To learn LDAP structure, and for troubleshooting : <http://www.softerra.com>

The screenshot shows an LDAP browser interface with a tree view on the left and a detailed view of user attributes on the right.

Tree View (Left):

- CN=Enterprise Read-only Domain
- CN=FederatedEmail.4c1f4d8b-817f
- CN=Group Policy Creator Owners
- CN=Guest
- CN=Itchy Rat
- CN=krbtgt
- CN=ProjectX
- CN=ProjectY
- CN=ProjectZ
- CN=RAS and IAS Servers
- CN=Rats
- CN=Read-only Domain Controller:
- CN=scep
- CN=Schema Admins
- CN=Scratchy Cat**

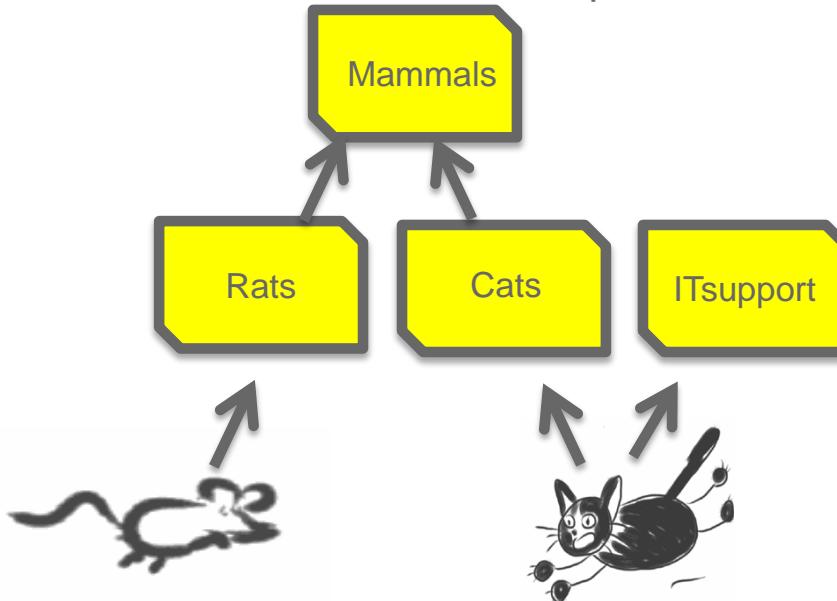
Attribute View (Right):

Name	Value
memberOf	CN=ITsupport,CN=Users,DC=labrats,DC=se
memberOf	CN=Cats,CN=Users,DC=labrats,DC=se
mobile	
modifyTime	
name	
objectCategory	
objectClass	
objectClass	person
objectClass	organizationalPerson
objectClass	user
objectGUID	D1 32 9C 81 EA 62 65 4F 86 B8 AC 6B 52 F2 90 11
objectSid	BA 61
primaryGroup	
pwdLastSet	
sAMAccountName	scratchy

An orange callout box highlights the **memberOf** attribute with its two values: CN=ITsupport,CN=Users,DC=labrats,DC=se and CN=Cats,CN=Users,DC=labrats,DC=se. Another orange callout box highlights the **sAMAccountName** attribute with its value **scratchy**.

Using Active Directory “memberOf”

- A user in Active Directory can be a member of **many** groups
 - But can only belong **one** Group Policy in ASA
- A group may be a member of another group in AD
 - ASA will not do recursive lookup



Cats Properties

General	Members	Member Of	Managed By
---------	---------	------------------	------------

Member of:

Name	Active Directory Domain Services Folder
Mammals	labrats.se/Users

Scratchy Cat Properties

Dial-in	Environment	Sessions	Remote control
Remote Desktop Services Profile	Personal Virtual Desktop	COM+	
General	Address	Account	Profile
		Telephones	Organization
			Member Of

Member of:

Name	Active Directory Domain Services Folder
Cats	labrats.se/Users
Domain Users	labrats.se/Users
IT support	labrats.se/Users

Mapping “memberOf” to Group Policy

- Map “memberOf” to ASA Group Policy with an LDAP attribute map
- **Beware:** First match will apply (many memberOf → one Group Policy)
- **Beware:** No support for lookup of nested groups (“group in group”)
- Using Cisco ISE (covered later) allows for better flexibility in assigning Group Policy
- DAP (covered later) allows for more flexibility in handling "many memberOf"



Edit LDAP Attribute Map

Name: ADmemberOfBYOD

LDAP map

Mapping of Attribute Name Mapping of Attribute Value

LDAP Attribute Name	Mapping of LDAP Attribute Value to Cisco Attribute Value
memberOf	CN=Rats,CN=Users,DC=labrats,DC=se=RatsBYOD CN=Cats,CN=Users,DC=labrats,DC=se=CatsBYOD

Add Edit Delete

CN=Rats,CN=Users,DC=labrats,DC=se : RatsBYOD
CN=Cats,CN=Users,DC=labrats,DC=se : CatsBYOD

The screenshot shows the 'Edit LDAP Attribute Map' interface. The 'Name' field is set to 'ADmemberOfBYOD'. There are two tabs: 'Mapping of Attribute Name' (selected) and 'Mapping of Attribute Value'. Under 'Mapping of Attribute Name', the 'LDAP Attribute Name' is 'memberOf'. Under 'Mapping of Attribute Value', the 'Mapping of LDAP Attribute Value to Cisco Attribute Value' section contains two entries: 'CN=Rats,CN=Users,DC=labrats,DC=se=RatsBYOD' and 'CN=Cats,CN=Users,DC=labrats,DC=se=CatsBYOD'. To the right of the interface, a yellow callout box highlights these two entries with the text 'CN=Rats,CN=Users,DC=labrats,DC=se : RatsBYOD' and 'CN=Cats,CN=Users,DC=labrats,DC=se : CatsBYOD'. A large blue arrow points from the text 'LDAP map' to the 'memberOf' entry in the table.

Troubleshooting AAA server

Servers in the Selected Group

Server Name or IP Address	Interface	Timeout
ratbert.labrats.se	Infrastructure	10
ratatouille.labrats.se	Infrastructure	10

Add Edit Delete Move Up Move Down Test

Test AAA Server - ratbert.labrats.se

To test the following AAA server, enter a username and password.

AAA Server Group: AD_SamAccount (LDAP)

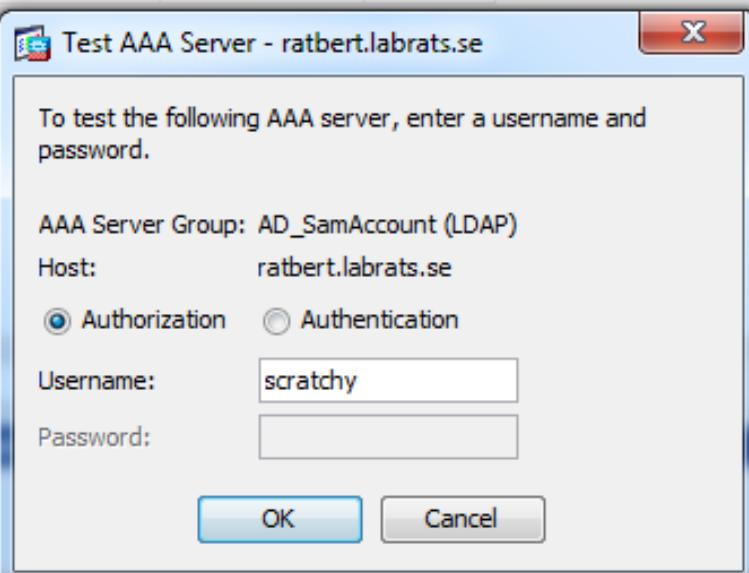
Host: ratbert.labrats.se

Authorization Authentication

Username: scratchy

Password:

OK Cancel



Troubleshooting AAA

- Checking that the right Group Policy has been assigned

[Monitoring > VPN > VPN Statistics > Sessions](#)

Type	Active	Cumulative	Peak Concurrent
AnyConnect Client	1	1	48
SSL/TLS/DTLS			48

Filter By: AnyConnect Client ▾ Username itchy Filter

Username	Group Policy Connection Profile	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
itchy	RatsBYOD SMS-OTP	10.99.110.1, 2001:470:1d.. 192.168.254.4	AnyConnect-Parent SSL-Tunnel DTLS- AnyConnect-Parent: (1)none SSL-Tu..	10:07:03 UTC Sun... 0h:09m:03s	11092 36080

Troubleshooting RADIUS : debug radius (1)

```
roddy(config)# sh debug  
debug radius session  
debug radius decode  
roddy(config)# radius mkreq: 0xa1.....  
got user 'scratchy'  got password  
add_req 0xade2da48 session 0xa1 id 80  
RADIUS_REQUEST  
radius.c: rad_mkpkt  
rad_mkpkt: ip:source-ip=192.168.254.4
```

RADIUS packet decode (authentication request)

Raw packet data (length = 172).....

01 50 00 ac 10 09 0e 2f 3c c5 1a 4b 28 41 e6 27	.P..../<..K(A.'
d4 7d 72 c3 01 0a 73 63 72 61 74 63 68 79 02 12	.}r...scratchy..
67 58 f2 72 53 db 00 ee 29 1a 49 b4 f1 c7 1a c7	gX.rS...).I.....
05 06 00 04 b0 00 1e 0f 31 39 32 2e 31 36 38 2e192.168.
31 31 30 2e 31 1f 0f 31 39 32 2e 31 36 38 2e 32	110.1..192.168.2
35 34 2e 34 3d 06 00 00 00 05 42 0f 31 39 32 2e	54.4=....B.192.
31 36 38 2e 32 35 34 2e 34 04 06 0a 01 29 6e 1a	168.254.4....)n.
22 00 00 00 09 01 1c 69 70 3a 73 6f 75 72 63 65	".....ip:source
2d 69 70 3d 31 39 32 2e 31 36 38 2e 32 35 34 2e	-ip=192.168.254.
34 1a 0f 00 00 0c 04 92 09 53 4d 53 2d 4f 54 50	4..... SMS-OTP
1a 0c 00 00 0c 04 96 06 00 00 00 02

Access-Request
from ASA to RADIUS
Server

Troubleshooting RADIUS : debug radius (2)

Parsed packet data.....

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 15 (0x0F)

Radius: Vendor ID = 3076 (0x00000C04)

Radius: Type = 146 (0x92) Tunnel-Group-Name

Radius: Length = 9 (0x09)

Radius: Value (String) =

53 4d 53 2d 4f 54 50

| **SMS-OTP**

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 12 (0x0C)

Radius: Vendor ID = 3076 (0x00000C04)

Radius: Type = 150 (0x96) Client-Type

Radius: Length = 6 (0x06)

Radius: Value (Integer) = **2** (0x0002)

send pkt 10.1.41.51/1645

ASA also sends Connection Profile
(Tunnel-Group) and Client-Type
(AnyConnect) to RADIUS Server in
ACCESS-REQUEST

Troubleshooting RADIUS : debug radius (3)

RADIUS packet decode (response)

Raw packet data (length = 142).....

02 51 00 8e 13 94 12 5d 9c 56 84 ab bc 99 85 0d	.Q.....].V.....
6a 71 7b 18 01 0a 73 63 72 61 74 63 68 79 18 28	jq{...scratchy.(
52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61	ReauthSession:0a
30 31 32 39 33 33 30 30 30 33 35 31 45 35 30	0129330000351E50
44 42 33 31 35 42 19 0e 52 65 73 65 61 72 63 68	DB315B..Research
42 59 4f 44 19 34 43 41 43 53 3a 30 61 30 31 32	BYOD.4CACS:0a012
39 33 33 30 30 30 33 35 31 45 35 30 44 42 33	9330000351E50DB3
31 35 42 3a 69 73 65 31 2f 31 34 31 35 38 39 31	15B:ise1/1415891
37 31 2f 32 32 34 33 31 1d 06 00 00 00 01	71/22431.....

Parsed packet data.....

Radius: Type = 25 (0x19) Class

Radius: Length = 14 (0x0E)

Radius: Value (String) =

43 61 74 73 42 59 4f 44

| **CatsBYOD**

Radius: Type = 29 (0x1D) Termination-Action

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x1

rad_procpkt: ACCEPT

RADIUS_ACCESS_ACCEPT: normal termination

RADIUS server may assign
Group Policy with the Class
attribute

Troubleshooting RADIUS

Authentication logs from
Cisco ISE

RADIUS Authentication Details	
Showing Page 1 of 1	First Prev Next
Authentication Summary	
Logged At:	January 6,2013 9:58:31.372 AM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	<u>scratchy</u>
MAC/IP Address:	192.168.254.4
Network Device:	roddy : 10.1.41.110 :
Allowed Protocol:	<u>Default Network Access</u>
Identity Store:	SMS_Mideye
Authorization Profiles:	CatsBYOD
SGA Security Group:	
Authentication Protocol :	PAP_ASCII
Authentication Result	
User-Name=scratchy	
State=ReauthSession:0a0129330000366450E94A95	
Class=CatsBYOD	
Class=CACS:0a0129330000366450E94A95:ise1/141589171/24482	
Termination-Action=RADIUS-Request	

Troubleshooting LDAP

- debug ldap

```
roddy(config)# debug ldap 100
debug ldap enabled at level 100
roddy(config)#
[42] Session Start
[42] New request Session, context 0xaddbaacc, reqType = Other
[42] Fiber started
```

[42] Creating LDAP context with uri=ldaps://10.1.41.10:636
[42] Connect to LDAP server: ldaps://10.1.41.10:636, status = Successful

```
[42] supportedLDAPVersion: value = 3
[42] supportedLDAPVersion: value = 2
```

[42] Binding as roddy@labrats.se

[42] Performing Simple authentication for roddy@labrats.se to 10.1.41.10

[42] LDAP Search: Base DN = [dc=labrats,dc=se] Filter =
[sAMAccountName=scratchy] Scope = [SUBTREE]
[42] User DN = [CN=Scratchy Cat,CN=Users,DC=labrats,DC=se]

Connect
(layer 4)

Bind
(authentication)

LDAP search

Troubleshooting LDAP (2)

- debug LDAP (2)

[42] Talking to Active Directory server 10.1.41.10

[42] Reading password policy for scratchy, dn:CN=Scratchy Cat,CN=Users,DC=labrats,DC=se

[42] Read bad password count 0

[42] LDAP Search: Base DN = [dc=labrats,dc=se] Filter = [sAMAccountName=scratchy]
Scope = [SUBTREE]

[42] Retrieved User Attributes:

.....
[42] displayName: value = Scratchy Cat

[42] uSNCreated: value = 386330

[42] memberOf: value = CN=Cats,CN=Users,DC=labrats,DC=se

[42] mapped to Group-Policy: value = CatsBYOD

[42] mapped to LDAP-Class: value = CatsBYOD

[42] uSNChanged: value = 387490

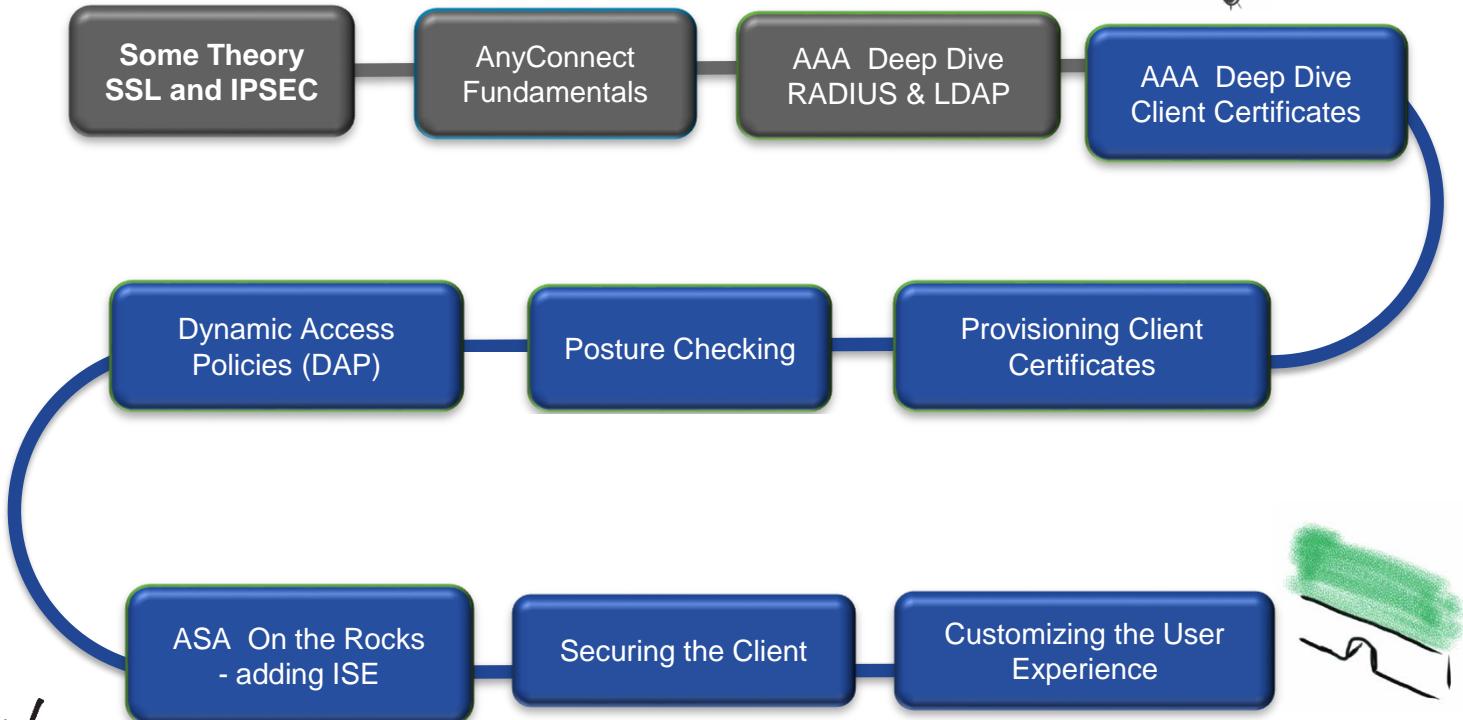
[42] department: value = Cats

[42] name: value = Scratchy Cat

.....

Received Attributes and
Group-Policy mapping

Agenda

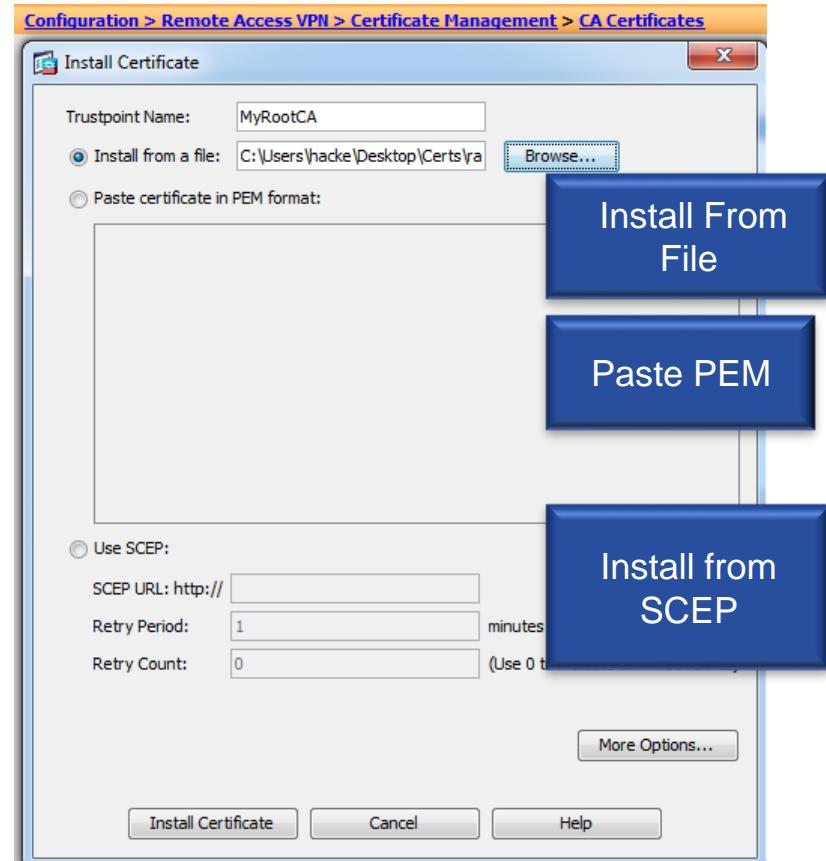


Authentication with Client Certificates

- Considered stronger authentication than passwords
- No need to manage passwords (password complexity, resetting passwords, expiring passwords...)
- Need to manage a PKI (Public Key Infrastructure) to enroll and revoke certificates
- Client Certificates may be tied to machine or user
- User certificates may be soft or hard (smart cards)
- We can make it difficult to move a certificate from one machine to another:
Using client certificates allows us to **distinguish corporate devices from other devices (employee iPADs etc)**

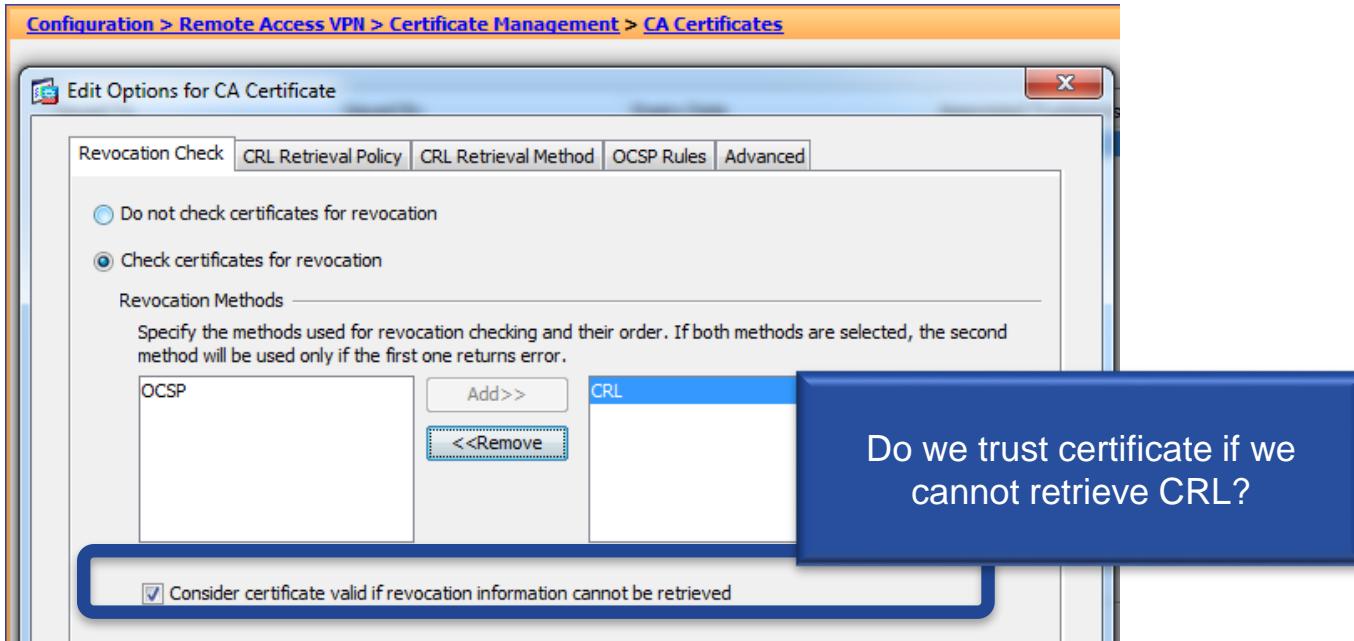
ASA must trust the Issuer of Client Certificates

- Install Issuer CA Certificate
 - from file
 - paste PEM file
 - SCEP
- Issuer of client certificates may be different to the issuer of the ASA certificate



Checking for lost/stolen certificates

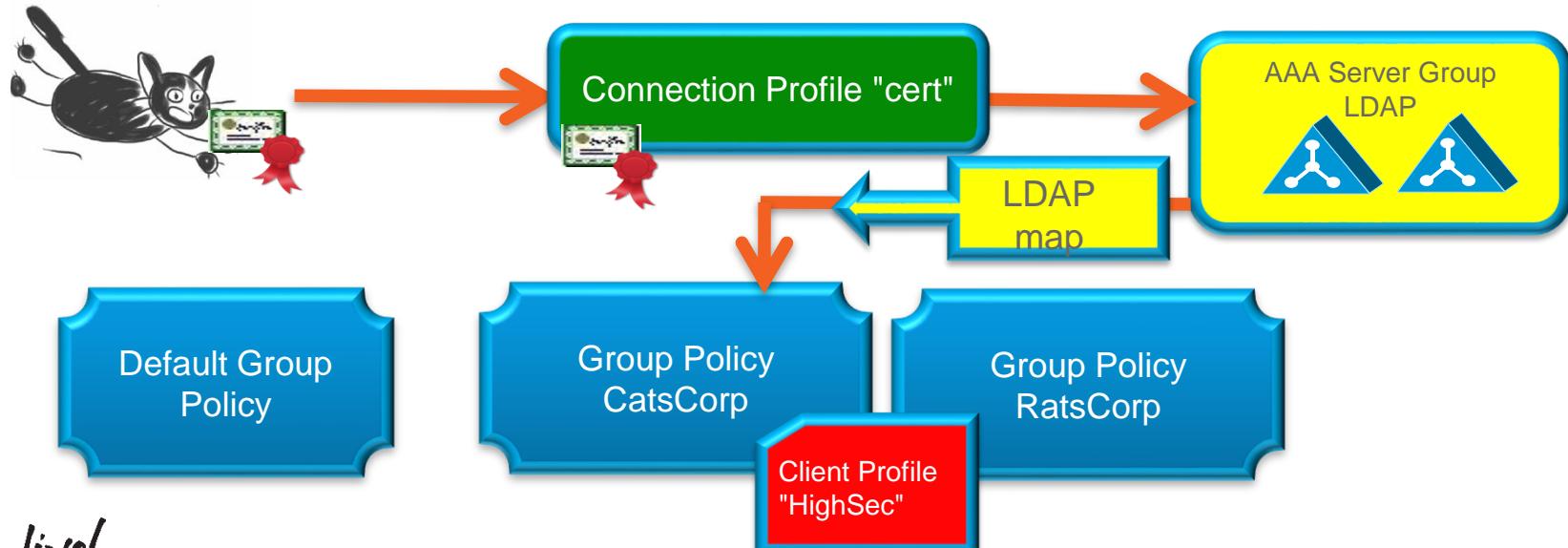
- CRL (Certificate Revocation List) downloads a list of revoked certificates (can be cached)
- OCSP (Online Certificate Status Protocol) checks status of individual certificates



Authentication with Client Certificates

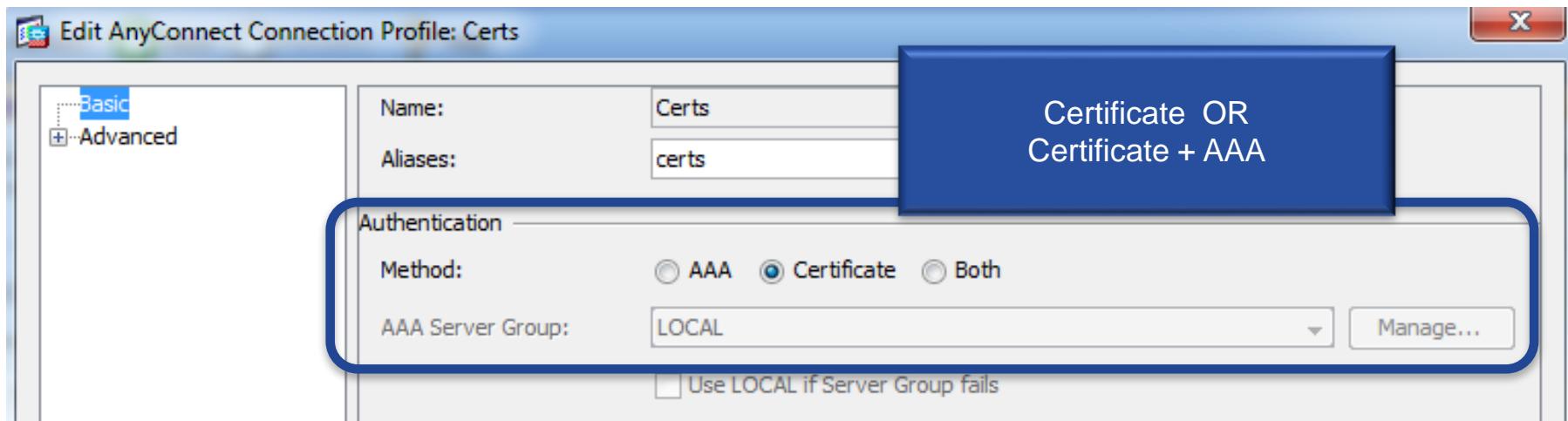
Authorization with LDAP

- User authenticated with client certificate
- Username (some field) of certificate used for LDAP lookup
- LDAP attributes are mapped to a Group Policy



Authentication with Client Certificates

- Defined in Connection Profile
- Choosing "both" means that user first has to authenticate with certificate, then with username/password
 - Use case : Checking that user uses a corporate machine (with a soft certificate)



Authorization with Client Certificates

- Work out which fields in cert to use and how to map to LDAP

Certificate

General Details Certification Path

Show: <All>

Field	Value
SMIME Capabilities	[1]SMIME Capability: Object I...
Subject Key Identifier	82 ac 79 b3 63 d8 f0 50 3c 33 ...
Authority Key Identifier	KeyID=de 9c 27 63 ca 33 69 0...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Alternative Name	Name:Principal Name=s...
Key Usage	Digital Signature, Key Encipher...
Thumbprint algorithm	sha1

Other Name:
Principal Name=scratchy@labrats.se

**Client Certificate : SAN
(Principal Name)**
scratchy@labrats.se

CN=Scratchy Cat,CN=Users,DC=labrats,DC=se

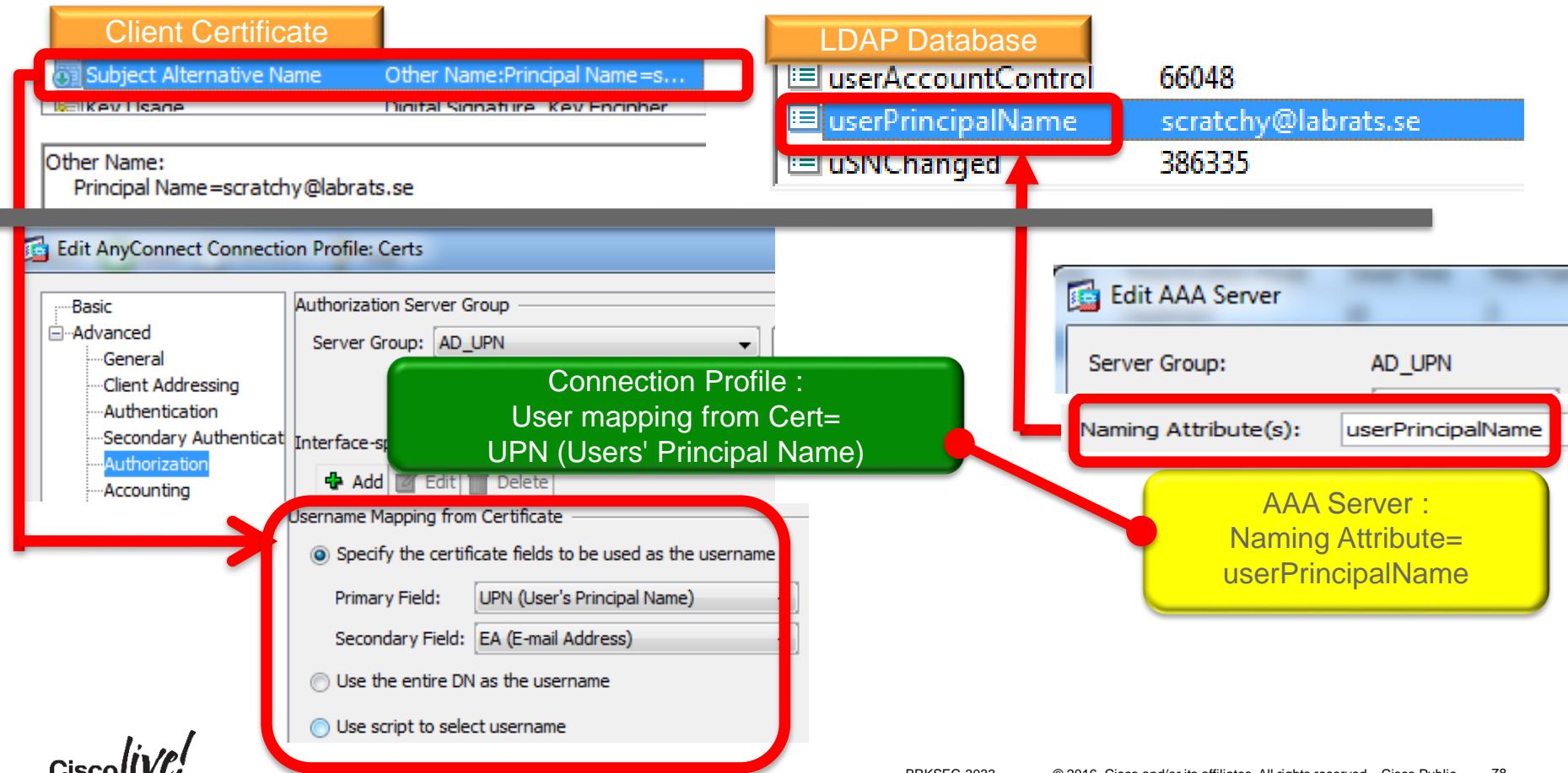
File Edit View Tools Help

LDIF (objectClass=*)

Name	Value
userPrincipalName	scratchy@labrats.se

LDAP : userPrincipalName
scratchy@labrats.se

Authorization with Client Certificates



A smart card is just another client certificate

- Same principles and configuration as for soft client certificates
- ...with the option of having AnyConnect disconnecting VPN when smart card is removed (configured under Group Policy/General)
- ASA/AnyConnect currently do not support “double” cert authentication
 - First with computer certificate, then with user certificate/smart card
 - Workaround : Use Posture checks to verify that it is corporate machine



Edit Internal Group Policy: CatsCorp

General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Client
Login Setting
Client Firewall
Key Decryption

Connection Profile (Tunnel Group) Lock: Inherit

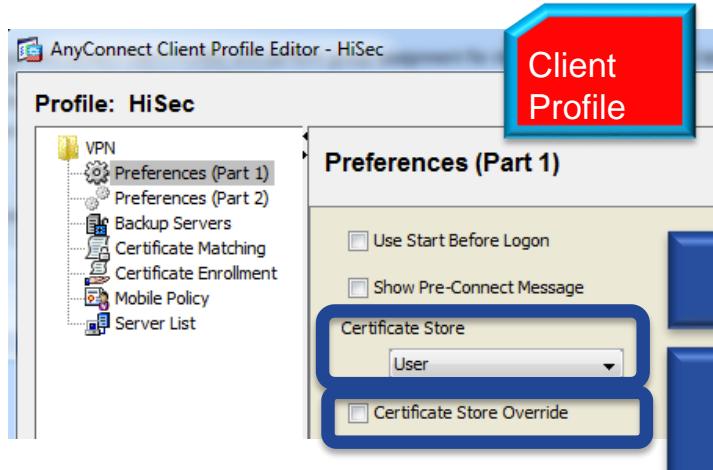
Maximum Connect Time: Inherit Unlimited minutes

Idle Timeout: Inherit None minutes

On smart card removal: Inherit Disconnect Keep the connection

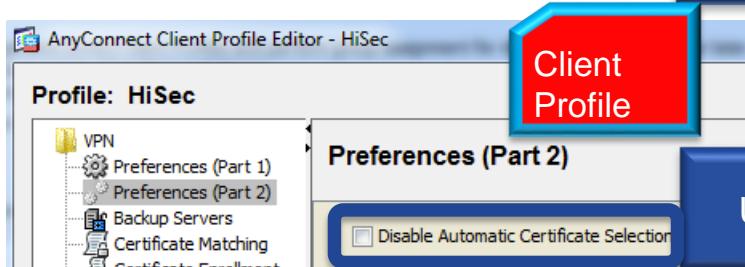
Optionally disconnect if Smartcard is removed

Client Profile Options to select the right certificate



Certificate Store : User, Machine or All

Certificate Store Override :
Check if non administrator needs access to
machine certificate



Uncheck for Automatic certificate Selection

Certificate Matching (for automatic cert selection)



Client Profile

If client (or smartcard) contains many certificates, we can specify which one should be selected (used with automatic certificate selection)

Profile: HiSec

VPN

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Matching**
- Certificate Enrollment
- Mobile Policy
- Server List

Certificate Matching

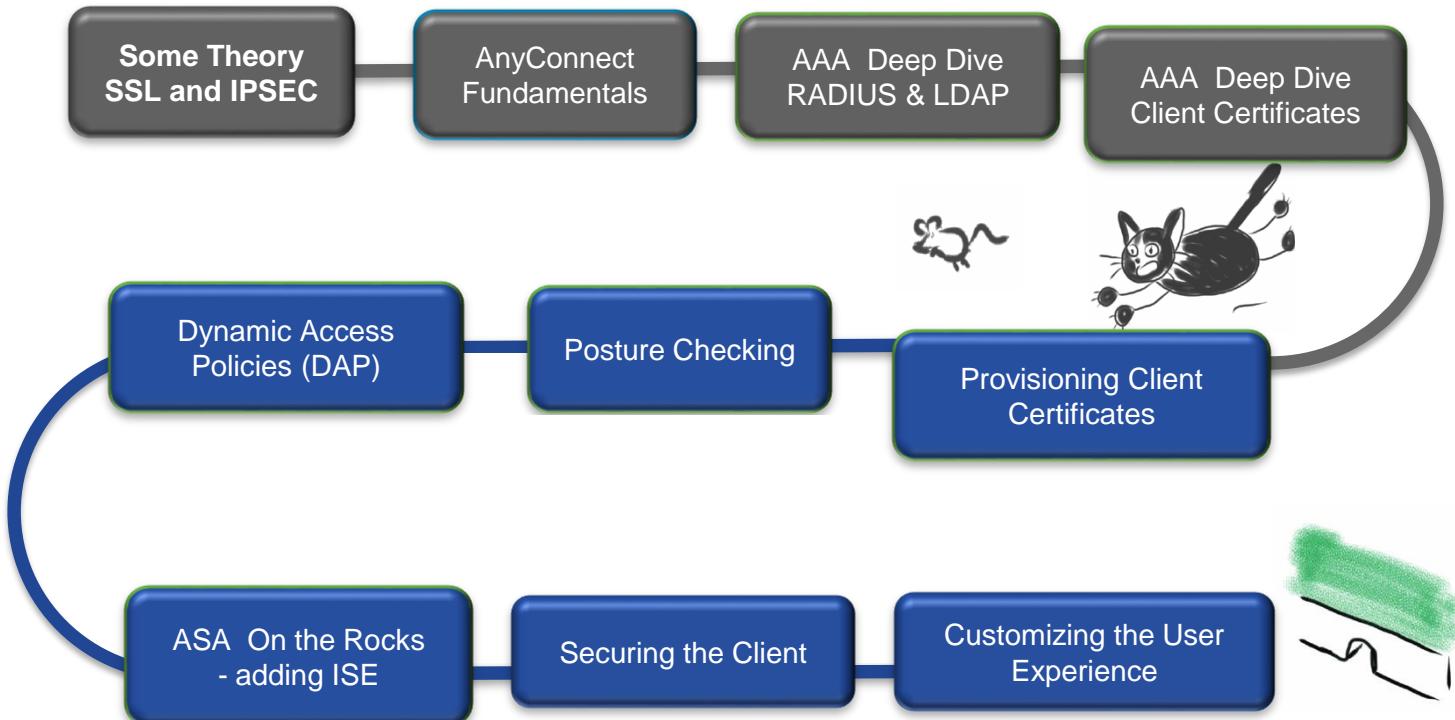
Name	Pattern	Wildcard	Operator	MatchCase
ISSUER-CN	labrats-RATBERT-CA	Disabled	Equal	Enabled

Custom Extended Match Key (Max 10)

Distinguished Name (Max 10)

OK Cancel Help

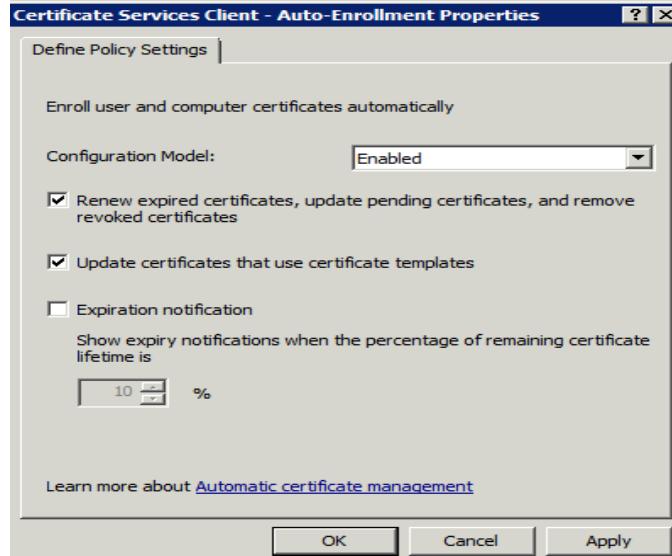
Agenda



Certificate Enrolment : Active Directory

- Microsoft Active Directory supports automatic certificate enrolment for user and machine certificates
- User and machine are members of Active Directory Domain: Their certificates can be pushed by GPOs (Group Policy Objects)

<http://technet.microsoft.com/en-us/library/cc770546.aspx>



Certificate Enrolment : Active Directory (2)

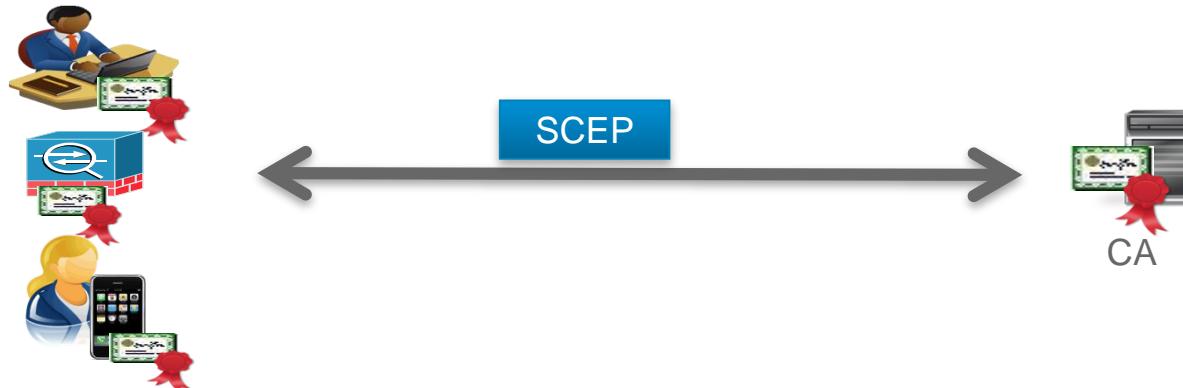
- Microsoft CA also supports web enrolment
- Can be used by non-domain members, e.g. MACs

The screenshot shows a Firefox browser window with the following details:

- Title Bar:** Microsoft Active Directory Certificate Services
- Address Bar:** http://ad/certsrv/
- Toolbar:** Includes standard browser buttons like Back, Forward, Stop, Home, and Refresh.
- Menu Bar:** Most Visited, Getting Started, Latest Headlines, Microsoft Active Directory Certific..., +
- Status Bar:** Do you want Firefox to remember the password for "hnohre" on http://ad?
- Content Area:**
 - Header:** Microsoft Active Directory Certificate Services – CA
 - Welcome Section:** Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
 - Select a task:**
 - [Request a certificate](#)
 - [View the status of a pending certificate request](#)
 - [Download a CA certificate, certificate chain, or CRL](#)

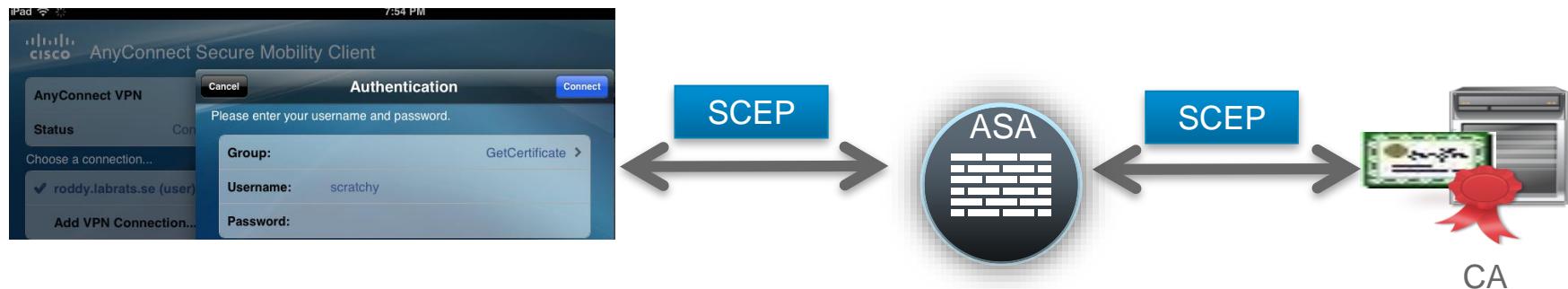
Simple Certificate Enrolment Protocol (SCEP)

- <http://tools.ietf.org/id/draft-nourse-scep-23.txt>
- Protocol for enrolling certificates over HTTP (basically encapsulating PKCS#10, PKCS#7 over HTTP)
- Originally developed by Verisign for Cisco
- **Widely** supported by network devices (including ASA and AnyConnect), clients and most Certificate Authorities (including Microsoft CA and Cisco ISE)



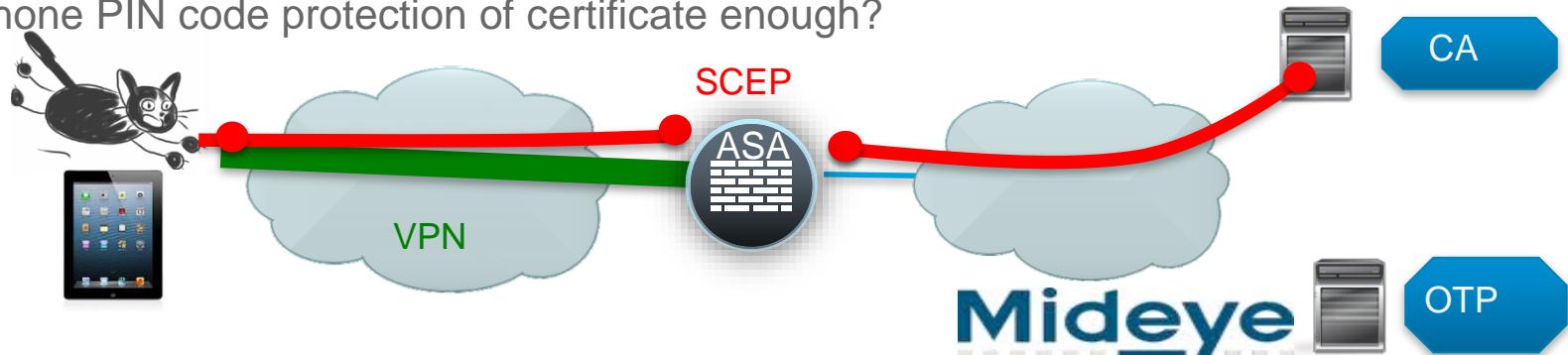
AnyConnect SCEP Proxy Support

- ASA can be an SCEP proxy, enabling AnyConnect on the outside to enroll to a CA on the inside of ASA without poking holes in Firewall
- Not to be confused with Legacy SCEP, where AnyConnect speaks directly to the CA over the VPN tunnel.
- SCEP proxy requires AnyConnect 3.0 or later :

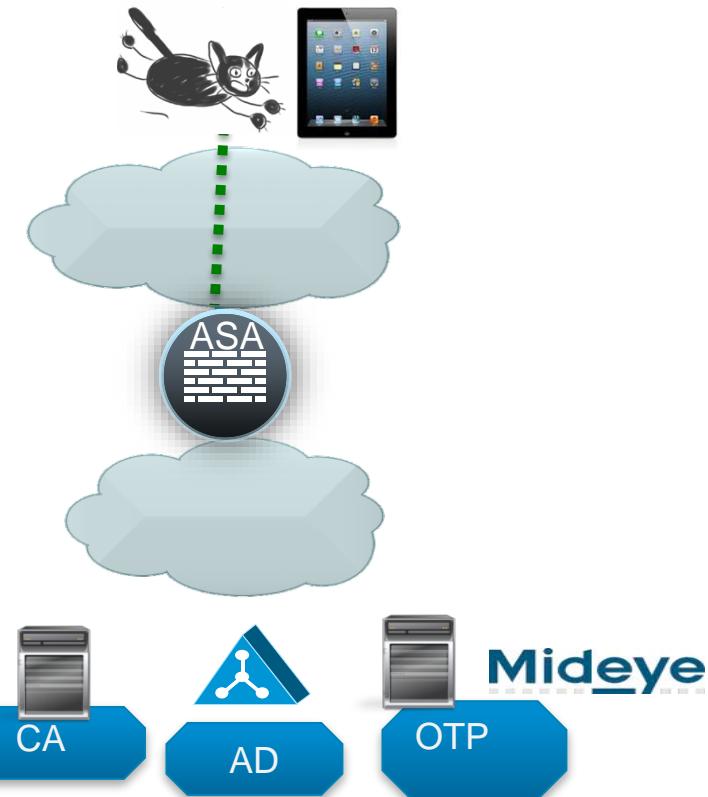
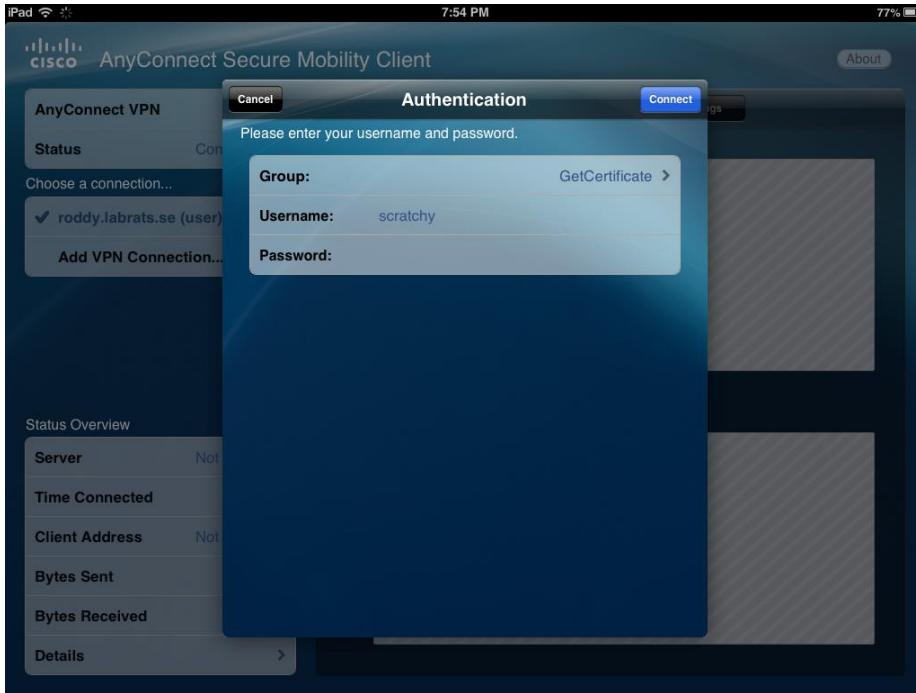


Case Study : Secure Enrolment of Certificates to Mobile Devices

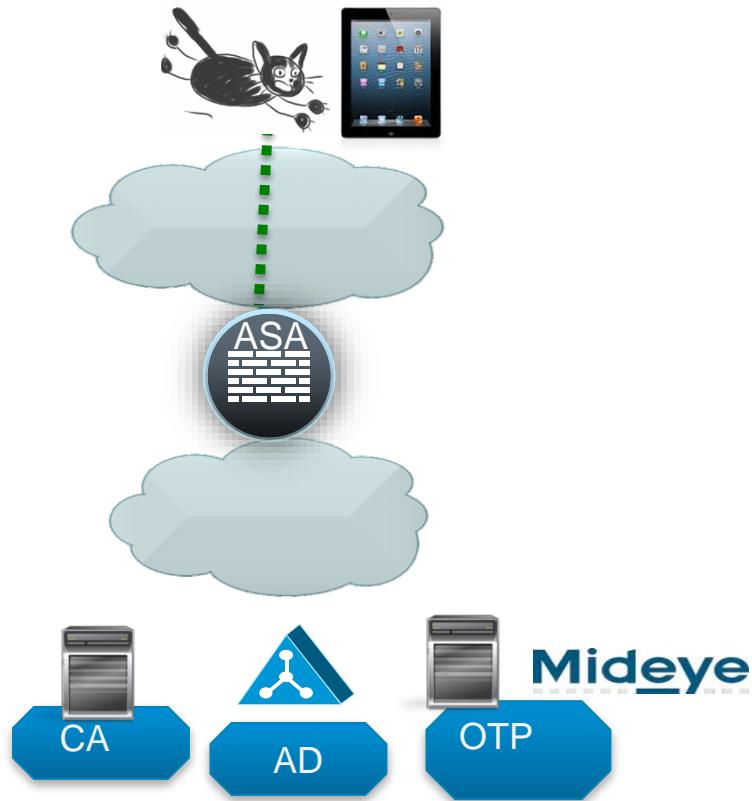
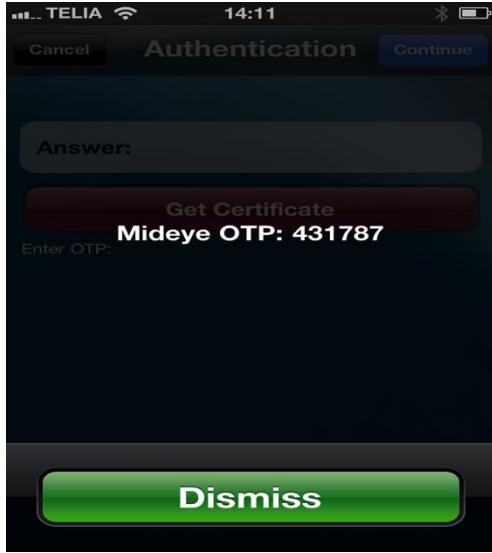
- Mobile users (Windows, MAC, Phone, Android) logon from **anywhere** (over internet) to enroll
- Secure authentication via OTP sent by SMS to mobile
- Certificate automatically enrolled with correct subject name
- Note : to mitigate risk of stolen phones, use certs + AAA for authentication
 - is phone PIN code protection of certificate enough?



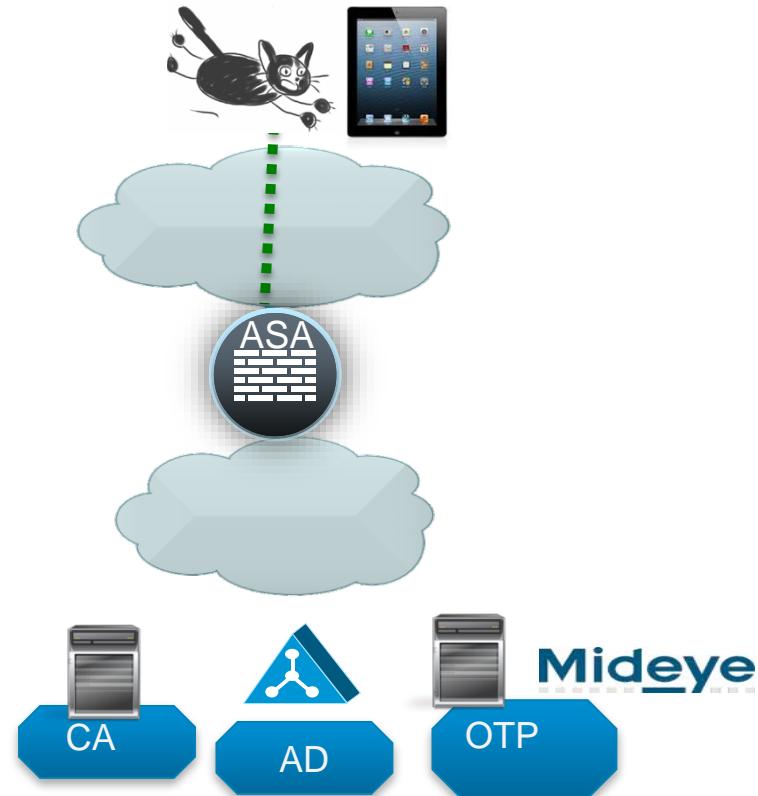
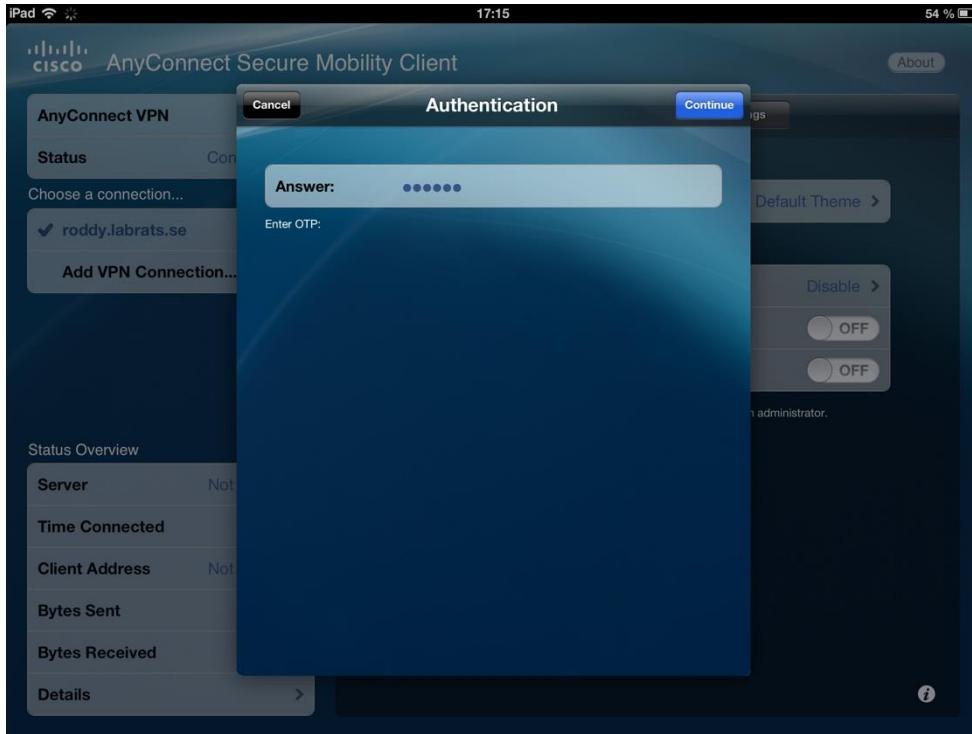
1. User Connects to ASA



2. User Gets SMS with OTP

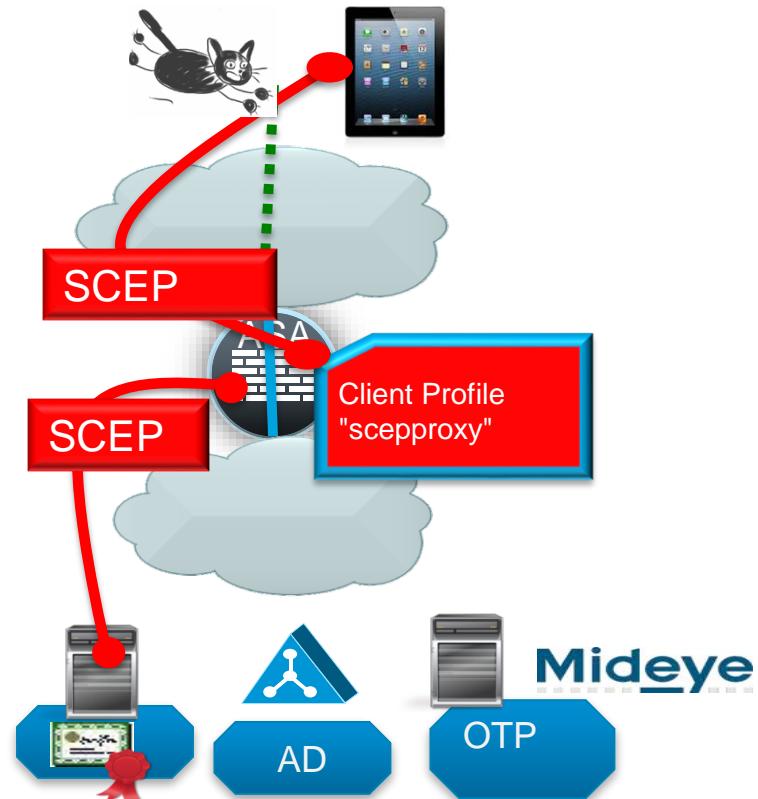
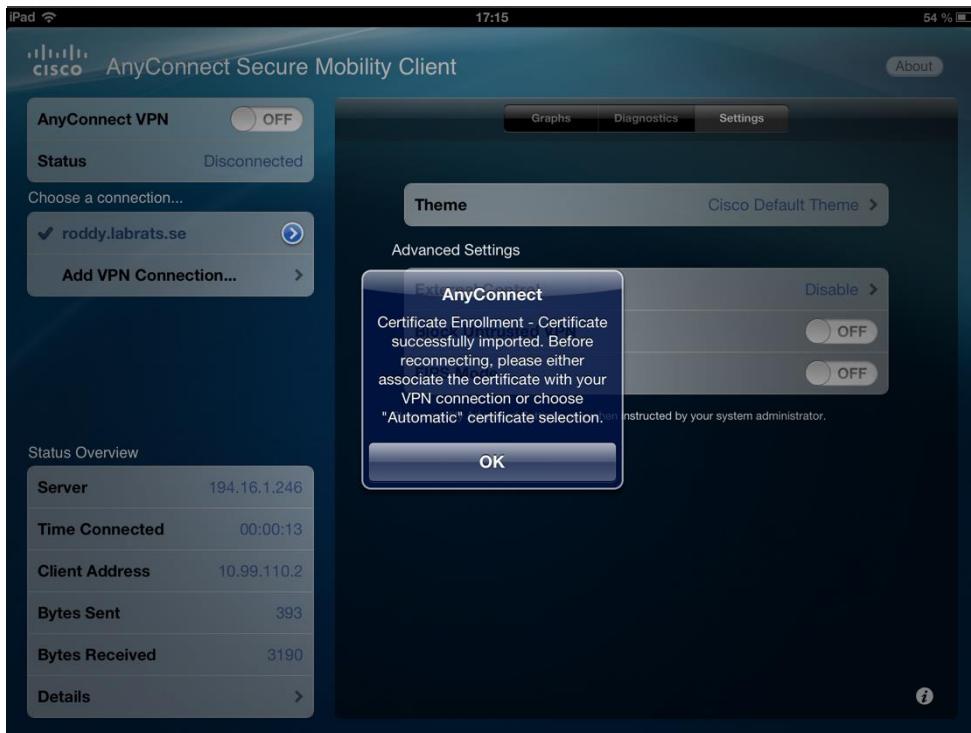


3. User logs on with OTP



4. AnyConnect Gets Certificate from ASA (proxy to CA)

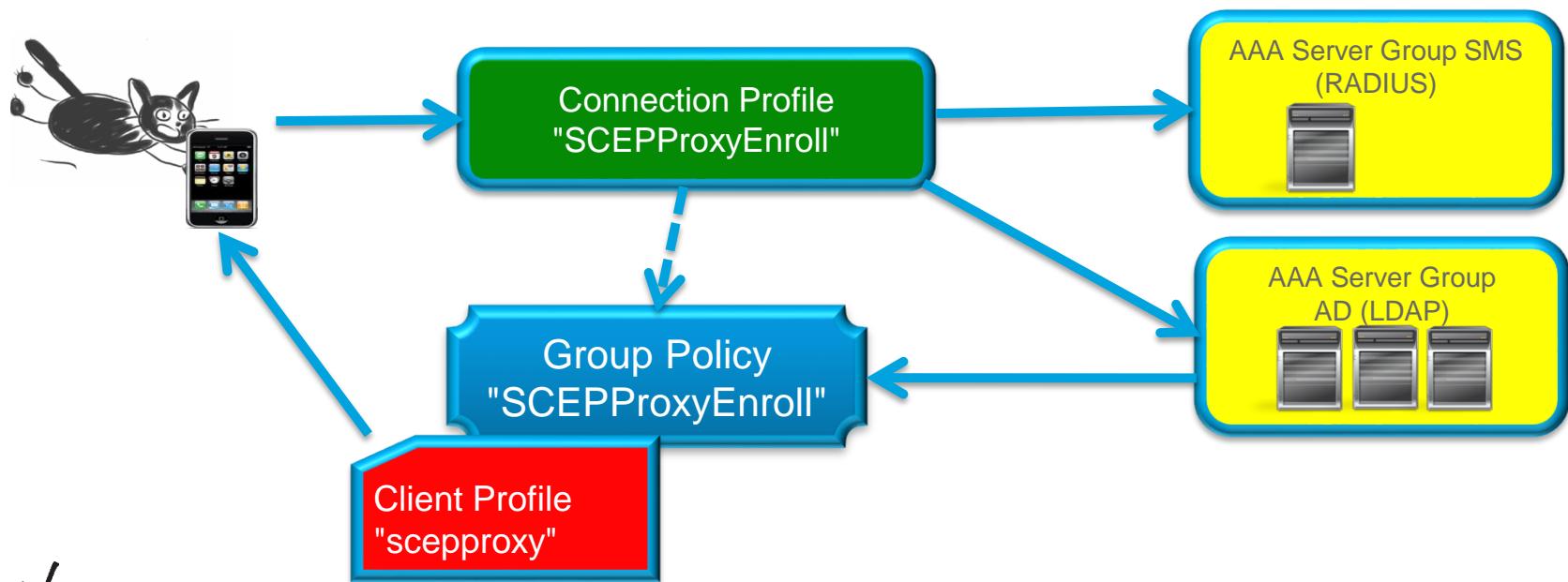
Cert can also be used for 802.1X*



What to Configure on ASA

- Configuration example on

http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect31/administration/guide/ac03vpn.html#wp1591160



Client Profile For Certificate Enrollment

The screenshot shows the 'AnyConnect Client Profile Editor - sceproxy' window. The left sidebar lists 'Profile: sceproxy' and 'VPN' options: Preferences (Part 1), Preferences (Part 2), Backup Servers, Certificate Matching, Certificate Enrollment (selected), Mobile Policy, and Server List. The main 'Certificate Enrollment' tab is selected. It contains the following fields:

- Certificate Enrollment
- Certificate Expiration Threshold (days): []
- Certificate Import Store: All
- Automatic SCEP Host: []
- CA URL: []
- Prompt For Challenge Password
- CA Thumbprint: []
- Certificate Contents: (Example: %USER% for user name, %MACHINEID% for machine ID)

Name (CN)	%USER%	Qualifier (GEN)	[]
Department (OU)	[]	Qualifier (DN)	[]
Company (O)	[]	City (L)	[]
State (ST)	[]	Title (T)	[]
State (SP)	[]	CA Domain	[]
Country (C)	[]	Key Size	2048
Email (EA)	%USER%@labrats.se	<input checked="" type="checkbox"/> Display Get Certificate Button	[]
Domain (DC)	[]		
- Domain (DC): []

Annotations on the slide:

- A red callout box at the top right says "Client Profile 'sceproxy'".
- A blue callout box on the left side of the 'Name (CN)' field says "subject-name can use %USER% %MACHINEID%".
- A blue callout box on the right side of the 'Key Size' field says "Default of 512 will not work with Windows CA default".
- A blue callout box at the bottom left says "EA can be used instead of SAN".

Group Policy for Certificate Enrollment

Edit Internal Group Policy: SCEPProxyEnroll

Group Policy "SCEPProxyEnroll"

Name: SCEPProxyEnroll

Banner: Inherit

SCEP forwarding URL: Inherit <http://ratbert.labrats.se/certsrv/mscep/mscep.dll>

URL for Microsoft CA
<http://ad.labrats.se/certsrv/mscep/mscap.dll>

URL for ISE CA
<http://ise.labrat.se:9090/auth/caservice/pkiclient.exe>

Edit Internal Group Policy: SCEPProxyEnroll

Client Profiles to Download:

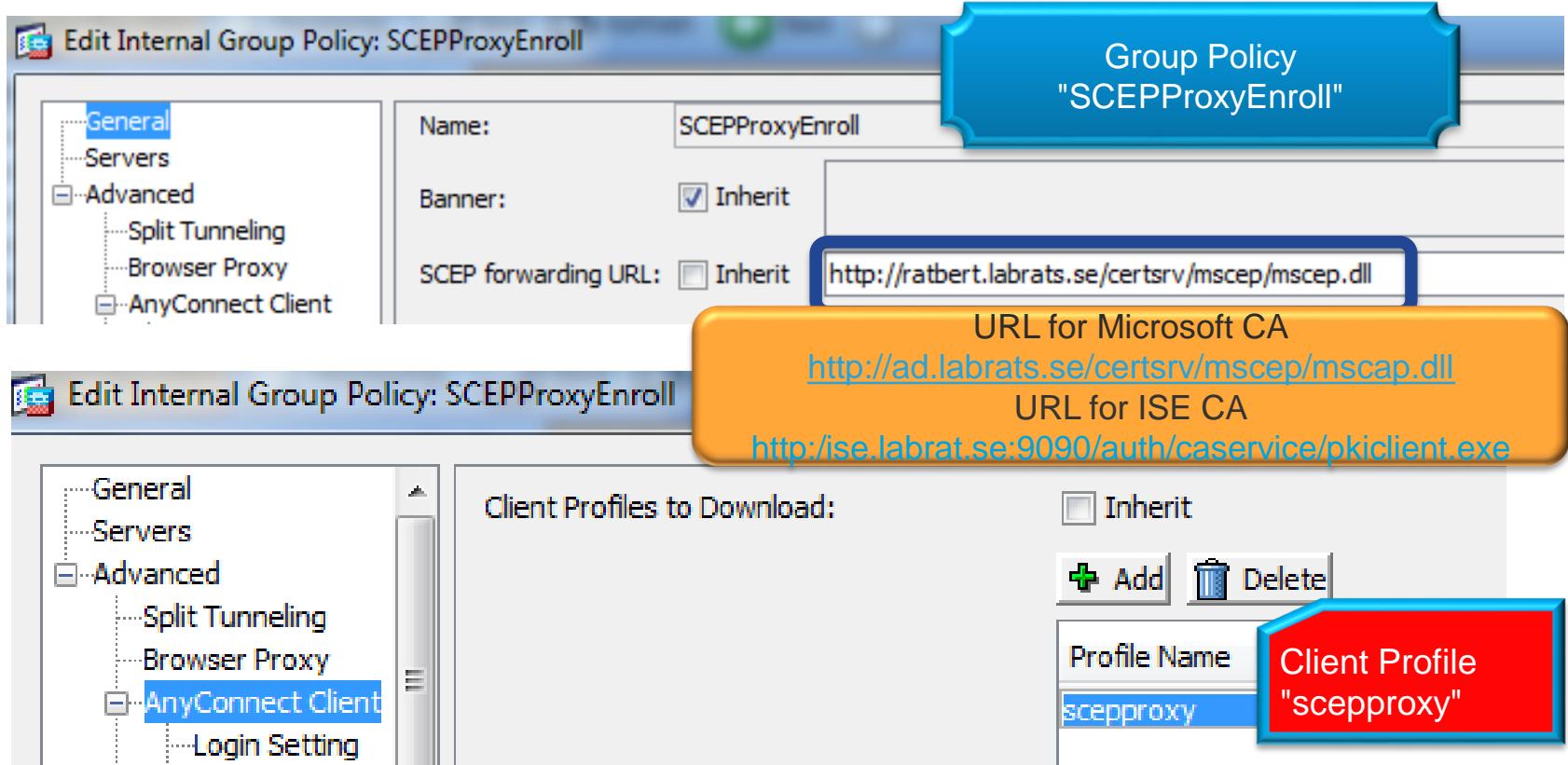
Inherit

Add **Delete**

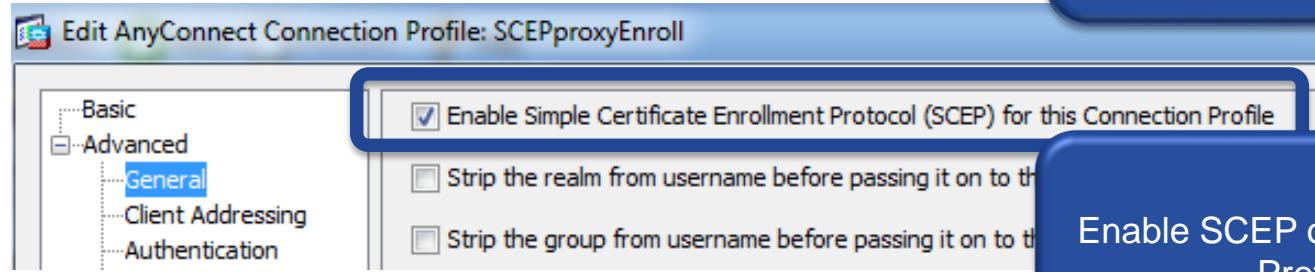
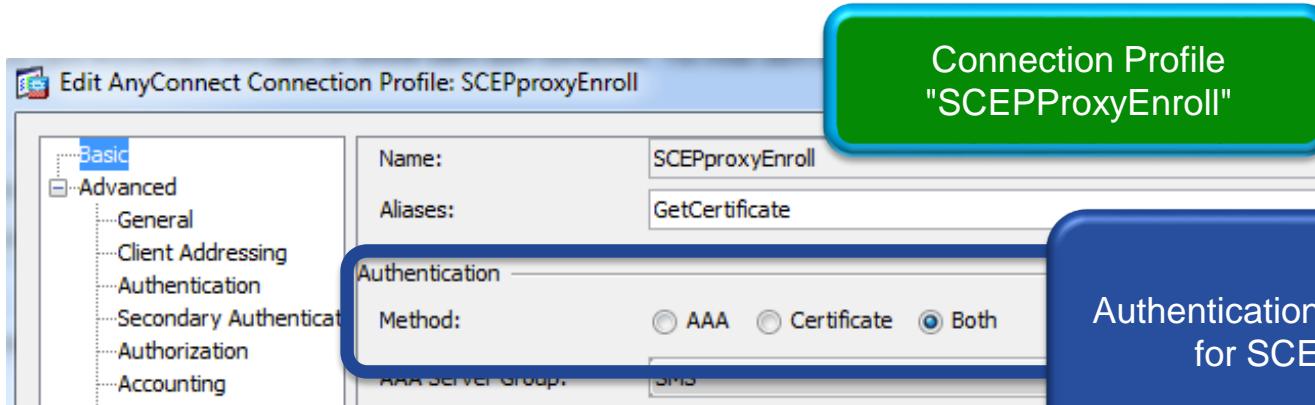
Profile Name

scepproxy

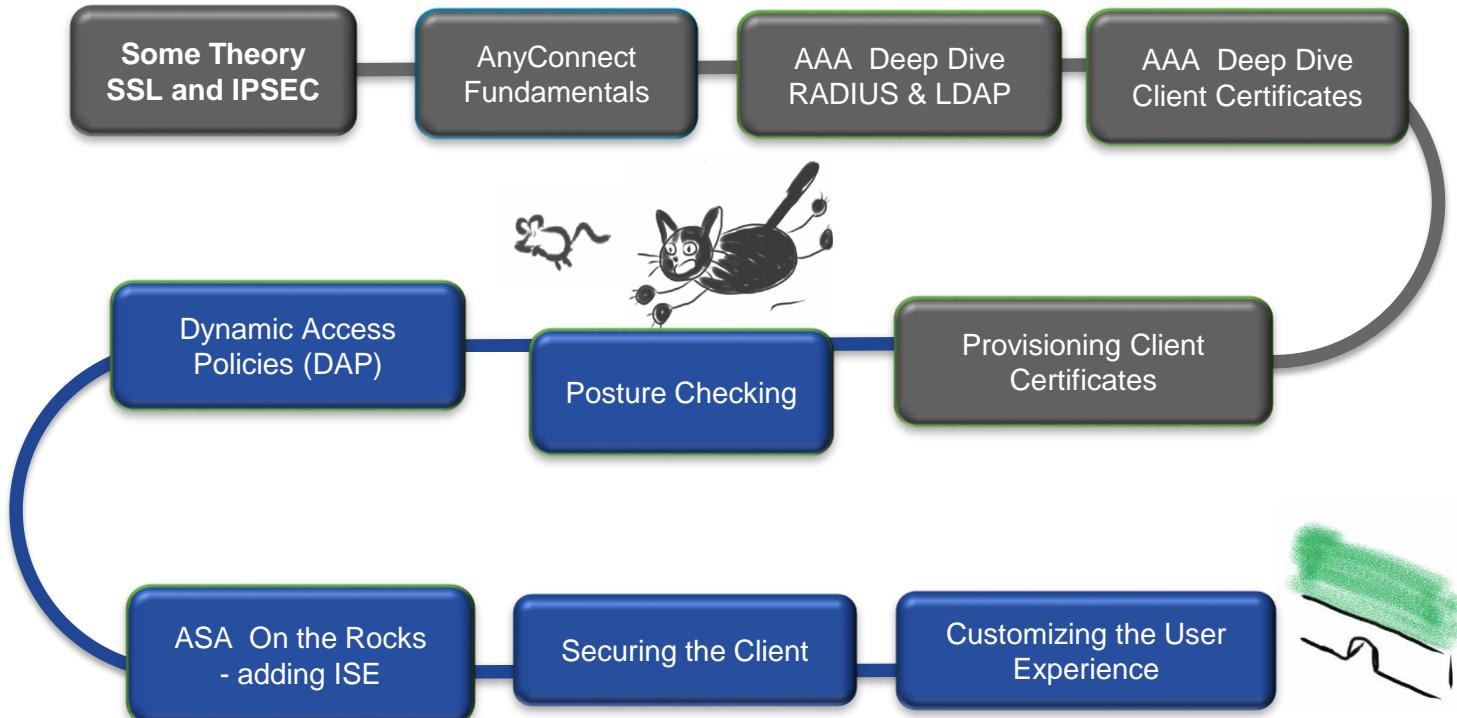
Client Profile "scepproxy"



Connection Profile for Certificate Enrollment



Agenda

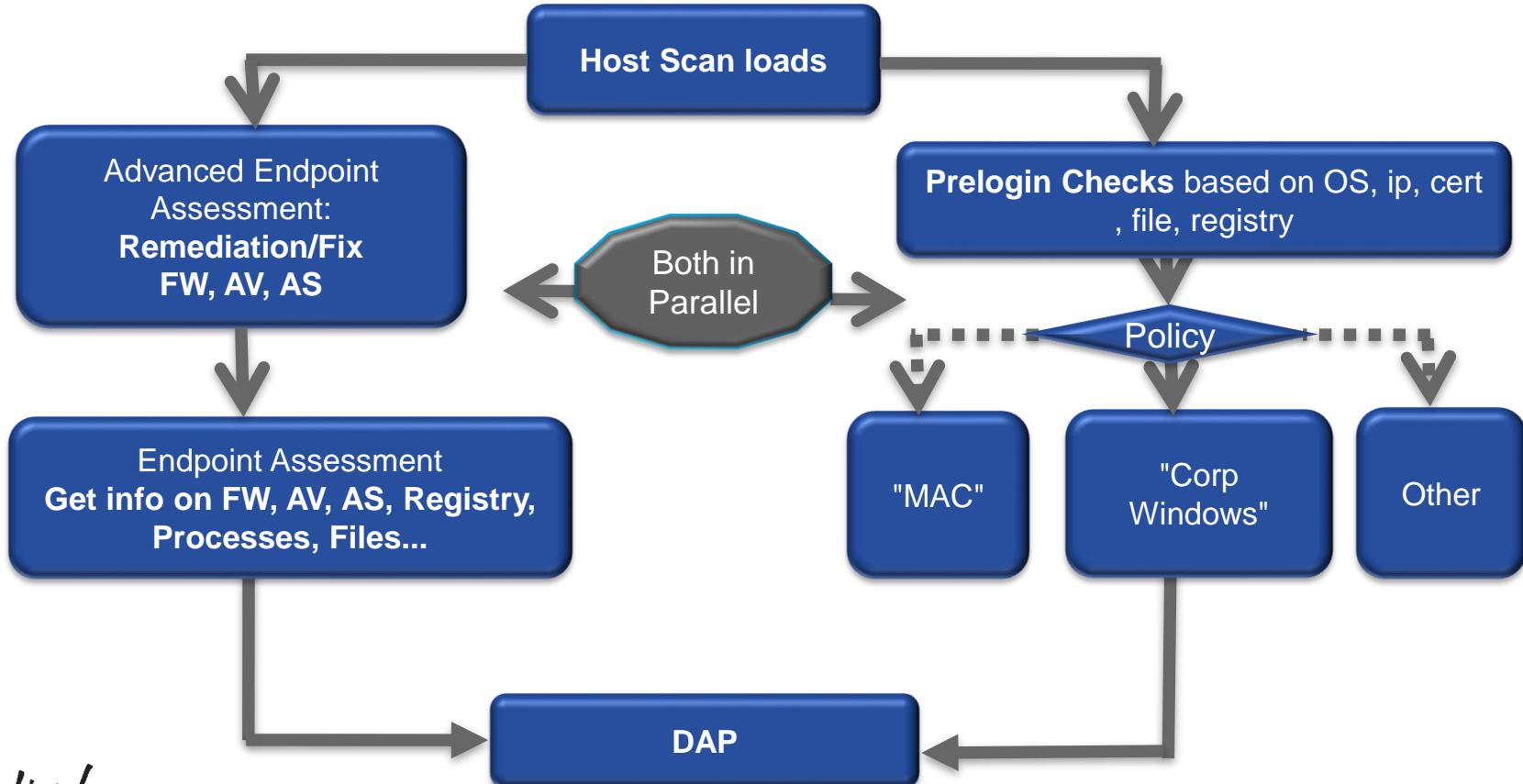


AnyConnect Posture : Do the Clients meet Requirements?

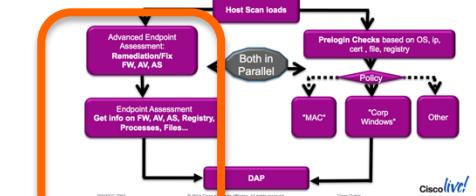
- Possible to check that client meets Posture Requirements : OS, Anti-Virus, Personal Firewall, Registry Keys, Open Ports etc
- Used in combination with Dynamic Access Policies (DAP) to grant access to clients depending on their posture status



The Host Scan Process



Configuring Host Scan



Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan

Host Scan

Create entries to be scanned on the endpoint system. The scanned information can be configured under [Dynamic Access Policies](#).

Basic Host Scan

ID	Info	Type
CorporateFile	C:\corporate.txt	File
CorporateKey	HKEY_CURRENT_USER\CorporateKey	Registry
CorporateProcess	notepad.exe	Process

Add ▾

- Registry Scan...
- File Scan...
- Process Scan...

Host Scan Extensions

Advanced Endpoint Assessment ver 3.6.4140.2

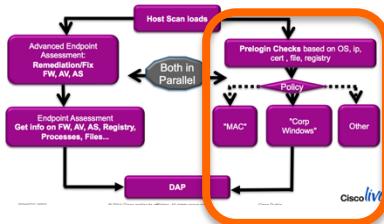
Endpoint Assessment ver 3.6.4140.2

Configure

Possible to create checks for Process, File and Registry keys that can be enforced by DAP

Endpoint Assessment must be checked to retrieve info on AV, AS, Firewall settings that can be enforced by DAP

Prelogin Policy

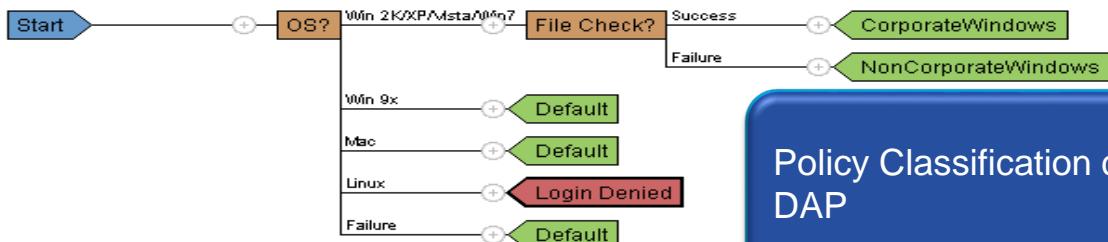


- Typical use case is to differentiate corporate devices
- Check client ip address, OS, that file exists, registry keys/values and certificate
 - client ip is the ip of network adapter (before any NAT...)
 - note : certificate check only checks if certificate exist, it does not cryptographically verify that the private key is there

[Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy](#)

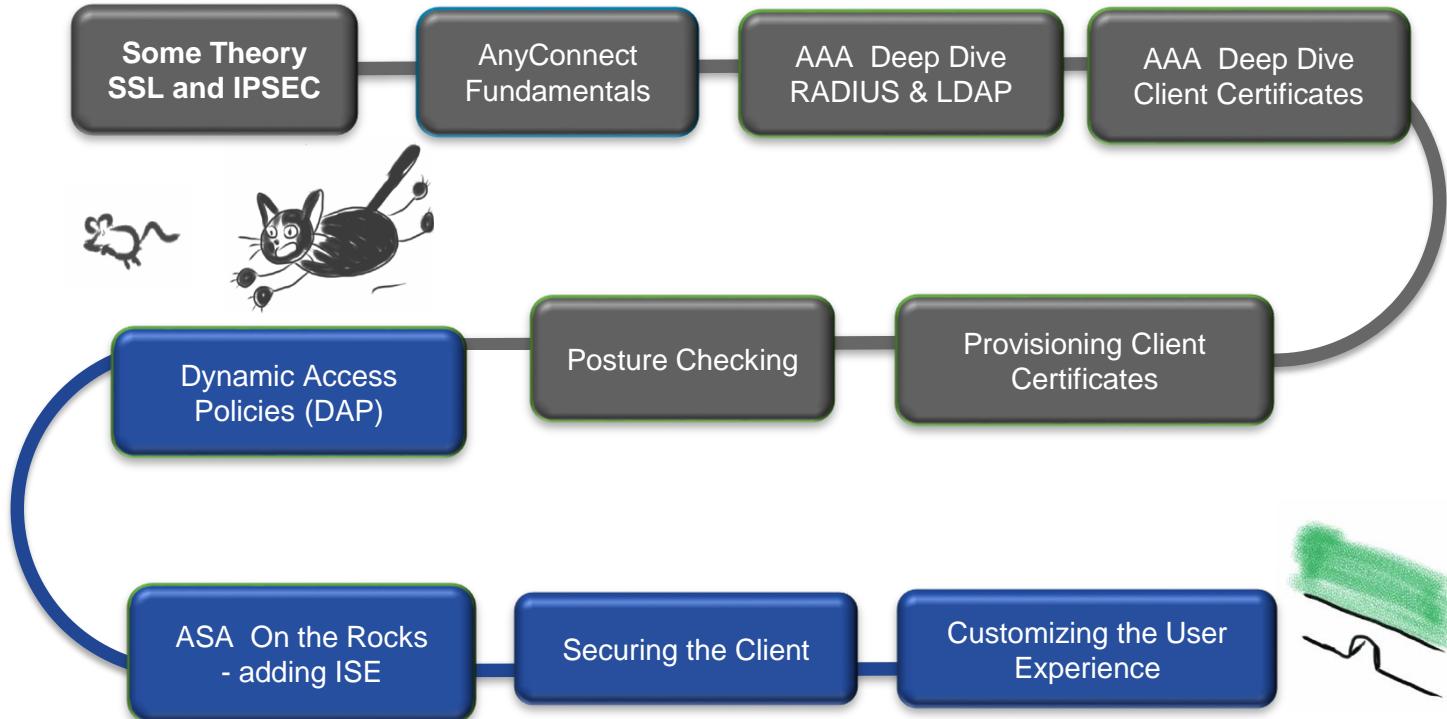
Prelogin Policy

Use the decision tree below to create prelogin policies. Click the + symbol to check for a specific registry key, file, certificate, OS version, or IP address. Click an end node to rename a prelogin policy, change it to a subsequence, or change it to "Login Denied." The policy name can be used as the value for the Policy endpoint selection attribute under [Dynamic Access Policies](#).



Policy Classification can be used by DAP

Agenda

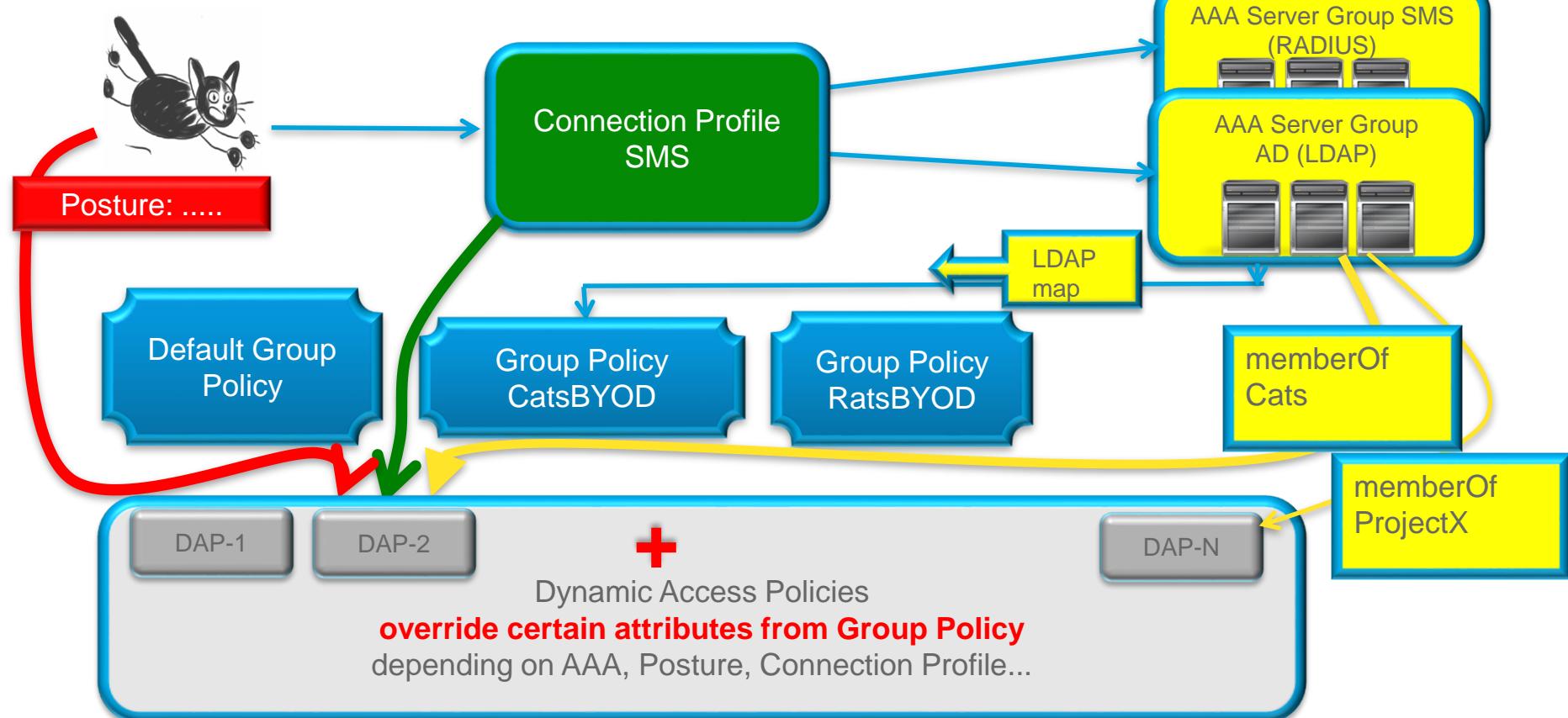


Dynamic Access Policies (DAP)

- DAP allows **granular access control** to resources based on authentication method, AAA parameters and Posture
- Very flexible, allowing policies set by **Data Owners** access to Data :
 - "to access **my data** you must be member of AD groups Cats and ProjectX, you must be logged in with strong authentication and you must have Antivirus on a corporate machine"



How DAP relates to AAA



Configuring DAP

Edit Dynamic Access Policy

Policy Name: Access-ProjectX
Description: Members of Cats AND Projects X logged on with clean corp PC
ACL Priority: 80

Selection Criteria

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ALL of the following AAA Attributes values...

AAA Attribute	Operation/Value
ldap.memberOf	= Cats
cisco.tunnelgroup	= Certs
ldap.memberOf	= ProjectX

If member of Cats and ProjectX logged on with certificate...

and the following endpoint attributes are satisfied.

Endpoint ID	Name/Operation/Value
registry.Corp... av.MicrosoftAV	exists = true type = dword value = S3cret description = Microsoft Forefront Client Security version > 1.5 lastupdate < 172800 activescan = ok

and Policy is Corporate Windows Registry Key is... Antivirus Updated...

Access/Authorization Policies

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Action | Network ACL Filters (client) | Webtype ACL Filters (clientless) | Functions | Port Forwarding Lists | Bookmarks | Access Method | AnyConnect

Network ACL (only all-permit and all-deny entries allowed)

Permit-CatWebserver

Add>> | Manage... | Delete

Network ACLs

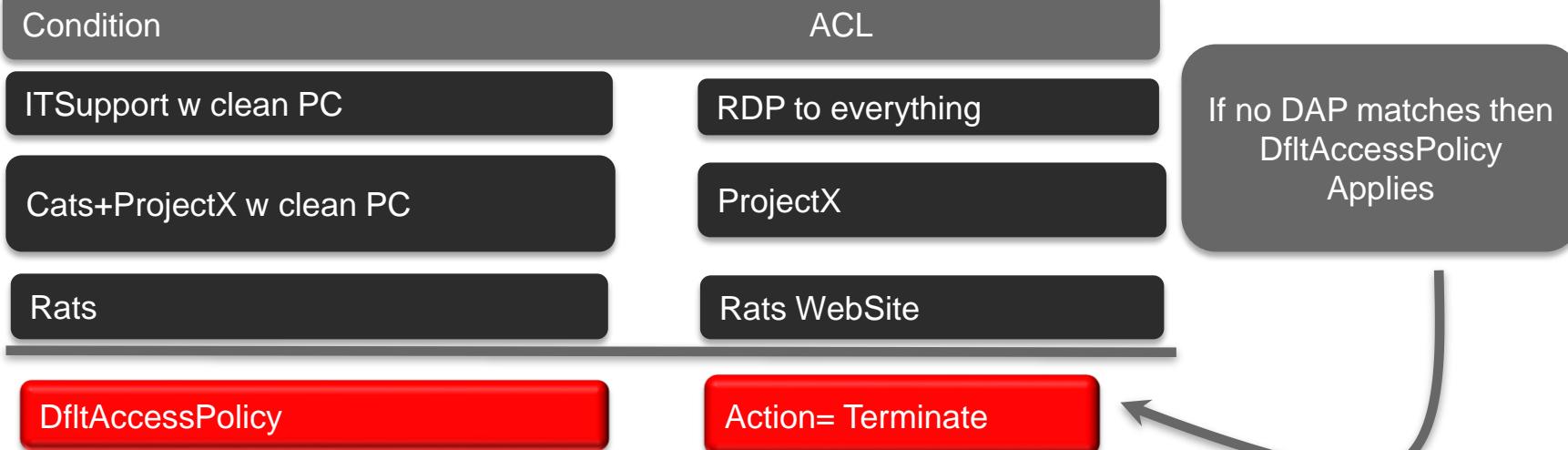
ACLprojectX

Authorization IPv4/IPv6 ACL don't mix permit and deny in ACL

Default DAP (DfltAccessPolicy)

[Configuration > Remote Access VPN > Network \(Client\) Access > Dynamic Access Policies](#)

ACL Priority	Name	Network ACL List	Description
90	ITsupport Access	RDP-to-Everything	IT support Access with RDP
80	Access-ProjectX	ACLprojectX	Members of Cats AND Projects X logged on with d...
70	Access to Rat Webserver	Permit-RatWebserver	Allow access to Rat Webserver to members of Rats...
-	DfltAccessPolicy		



DAP Grows On You! (DAP accumulates)

[Configuration > Remote Access VPN > Network \(Client\) Access > Dynamic Access Policies](#)

ACL Priority	Name	Network ACL List	Description
90	ITsupport Access	RDP-to-Everything	IT support Access with RDP
80	Access-ProjectX	ACLprojectX	Members of Cats AND Projects X logged on with d...
70	Access to Rat Webserver	Permit-RatWebserver	Allow access to Rat Webserver to members of Rats...
-	DfltAccessPolicy		



The Power of DAP

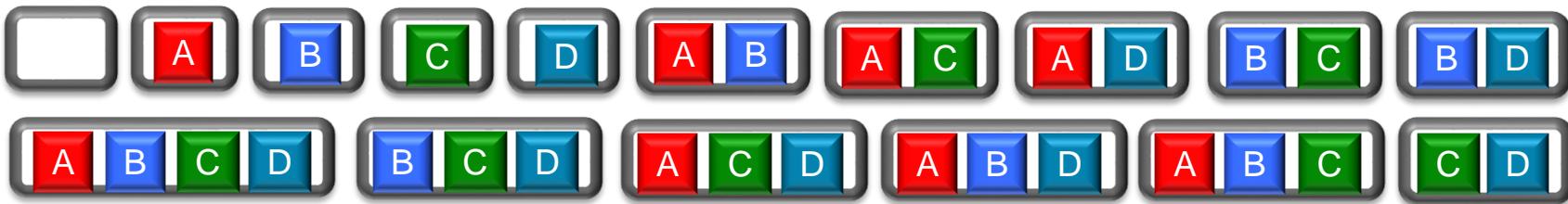
- Very flexible mapping to multiple "memberOf"

- Example : 4 groups in Directory



n

- A user may be a member of 0 to 4 groups : 16 combinations (2^n)



- Quiz** : How many DAP policies do you need to cover the 16 combinations?

Condition (memberOf)

ACL



DAP with LUA

The screenshot shows the 'Add Dynamic Access Policy' dialog box. The policy name is 'Cats BYOD w Any Antivirus' and the description is 'Require that at least one AV is installed'. The ACL Priority is set to 0. Under 'Selection Criteria', it specifies that the user must have all of the following AAA attributes: 'ldap.memberOf = Cats'. Below this, there is a table for endpoint attributes, which is currently empty. A callout bubble highlights the 'Advanced' section where LUA code can be written. The LUA code provided is:

```
assert(function()
    for k,v in pairs(endpoint.av) do
        if (EVAL(v.exists, "EQ", "true", "string")) then
            return true
        end
    end
    return false
end)()
```

LUA (www.lua.org) – scripting language that allows for advanced checks, e.g.

- check for any AV
- check for any AV, AS, Firewall
- regexp matching of hotfixes, DN etc

LUA examples



```
assert(function()
    function check(antix)
        if (type(antix) == "table") then
            for k,v in pairs(antix) do
                if (EVAL(v.exists, "EQ", "true", "string")) then
                    return true
                end
            end
        end
        return false
    end
    return (check(endpoint.av) or check(endpoint.fw) or check(endpoint.as))
end)()
```

Check for Any Antivirus, Firewall or
AntiSpyWare

Troubleshooting DAP : debug dap trace

DAP_TRACE: DAP_open: B09086B0

DAP_TRACE: DAP_add_CSD: csd_token = [2441266B55C307BA5BEB70E5]

.....

DAP_TRACE: Username: scratchy@labrats.se, aaa.Idap.logonCount = 15

DAP_TRACE: Username: scratchy@labrats.se, aaa.Idap.sAMAccountName = scratchy

.....

DAP_TRACE:

dap_install_endpoint_data_to_lua: endpoint.as["MicrosoftAS"].description = "Windows Defender"

DAP_TRACE: name = endpoint.as["MicrosoftAS"].description, value = "Windows Defender"

DAP_TRACE: dap_install_endpoint_data_to_lua: endpoint.as["MicrosoftAS"].version = "6.1.76"

DAP_TRACE: name = endpoint.as["MicrosoftAS"].version, value = "6.1.7600.16385"

.....

DAP_TRACE: name = endpoint.os.hotfix["KB2654428"], value = "true"

DAP_TRACE: dap_install_endpoint_data_to_lua: endpoint.os.hotfix["KB2656373"] = "true"

DAP_TRACE: name = endpoint.os.hotfix["KB2656373"], value = "true"

LDAP info

Posture
(Subset)

Troubleshooting DAP : Monitoring

Session Details

Username	Group Policy Connection Profile	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
scratty@labrats.se	CatsCorp Certs	10.99.110.1 2001:470:dfed:110::1 192.168.254.4	AnyConnect-Parent SSL-Tunnel DTLS-.. 16:13:02 UTC Sun... 11684	AnyConnect-Parent:	

Details **ACL**

The following ACL is being applied to this session:

```
access-list DAP-ip-user-50418800; 1 elements; name hash: 0xe4c6096c
access-list DAP-ip-user-50418800 line 1 extended permit tcp any any
access-list DAP-ip-user-50418800 line 1 extended permit tcp any any
```

The following IPv6 ACL is being applied to this session:

```
access-list DAP-ip-user-50418800; 1 elements; name hash: 0xe4c6096c (dynamic)
access-list DAP-ip-user-50418800 line 1 extended permit tcp any any object-group rdp (hitcnt=0) 0x27408a58
access-list DAP-ip-user-50418800 line 1 extended permit tcp any any eq 3389 (hitcnt=0) 0xdc9892a8
```

Monitoring/
Session Details/ACL

Troubleshooting DAP : Syslog

- Debug DAP trace not always practical in production
 - too much info
 - no filtering on username
- Syslog Message with good DAP info : **username** and **selected DAP records**

%ASA-6-734001: DAP: User **scratchy@labrats.se**, Addr 192.168.254.4, Connection AnyConnect: The following DAP records were selected for this connection: **ITsupport Access**

Troubleshooting Hostscan Component

- Enable Debugging level at ASDM, then rerun test on problematic client

[Configuration > Remote Access VPN > Secure Desktop Manager > Global Settings](#)

Global Settings

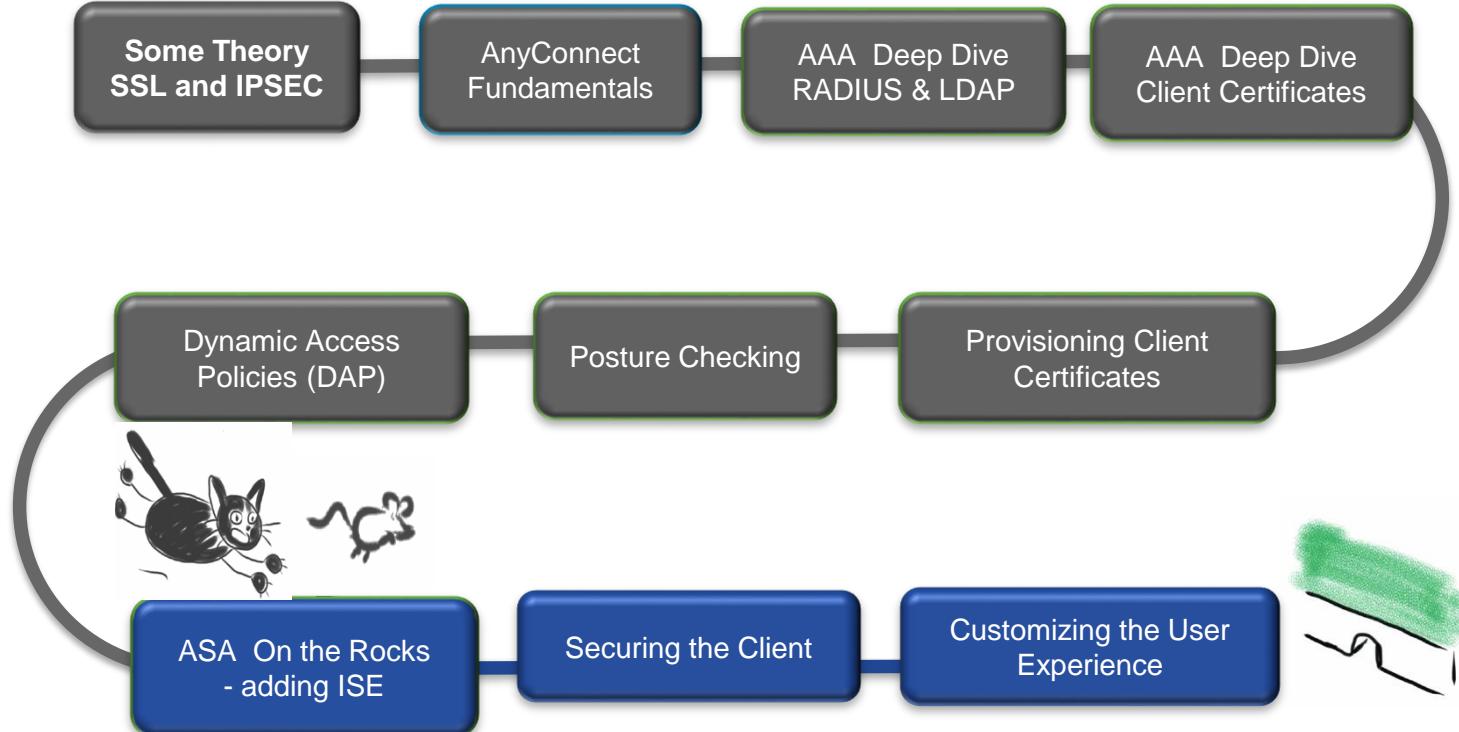
Logging level controls CSD logging on all VPN user endpoints that run CSD. By default, the Logging Level is set to Errors. Each event level is cumulative. For example, the Warnings option enables logging for both errors and warnings.

Logging Level **Debugging** ▾

- Check Host Scan log files on problematic client
 - libcsd.log
 - cscan.log, detailed posture attributes
- These are located at
 - Windows %LOCALAPPDATA%\Cisco\Cisco HostScan\log
 - MAC/Linux : ~/.cisco/hostscan/log
- Examine Windows Event logs

GOT DART?

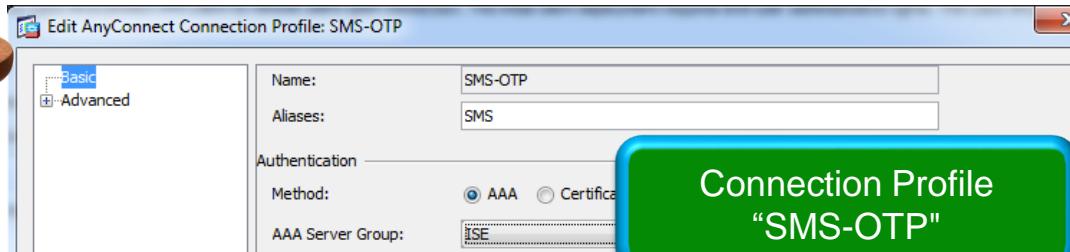
Agenda



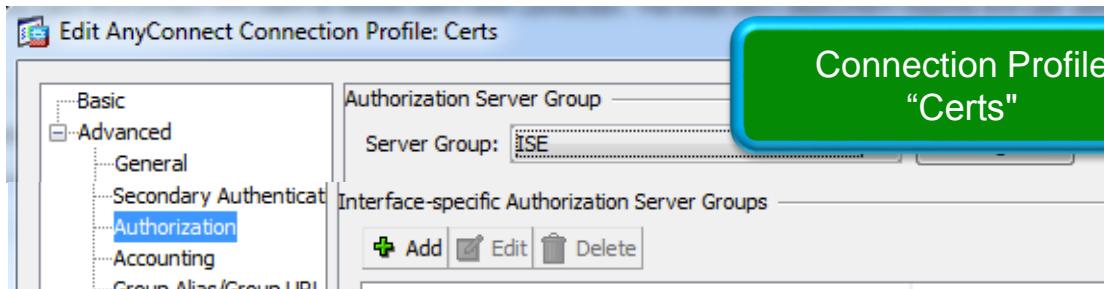
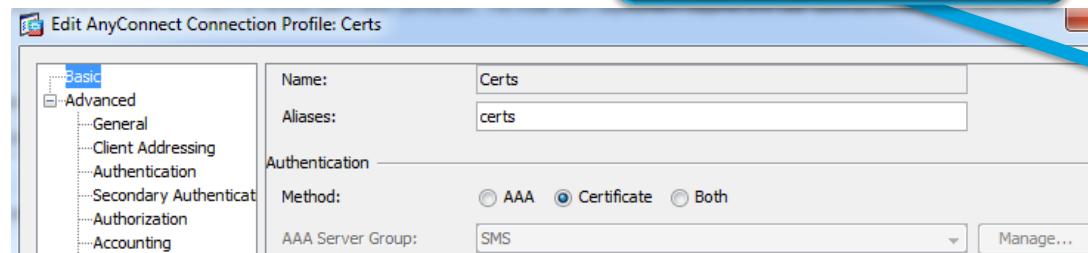
Benefits of Secure Unified Access with ISE



Secure Unified Access : 2 minutes ASA Configuration



We no longer need to care about AD, LDAP or LDAP maps.. or OTP server



ASA configuration of ISE AAA Server Group

Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
ISE	RADIUS	Single	Depletion	10	3

Edit AAA Server Group

AAA Server Group: ISE
Protocol: RADIUS
Accounting Mode: Simultaneous Single
Reactivation Mode: Depletion Timed
Dead Time: 10 minutes

Enable interim accounting update
 Update Interval: 24 Hours
 Enable Active Directory Agent mode

ISE Policy Enforcement

Enable dynamic authorization
Dynamic Authorization Port: 1700
 Use authorization only mode (no common password configuration required)

VPN3K Compatibility Option

OK Cancel Help

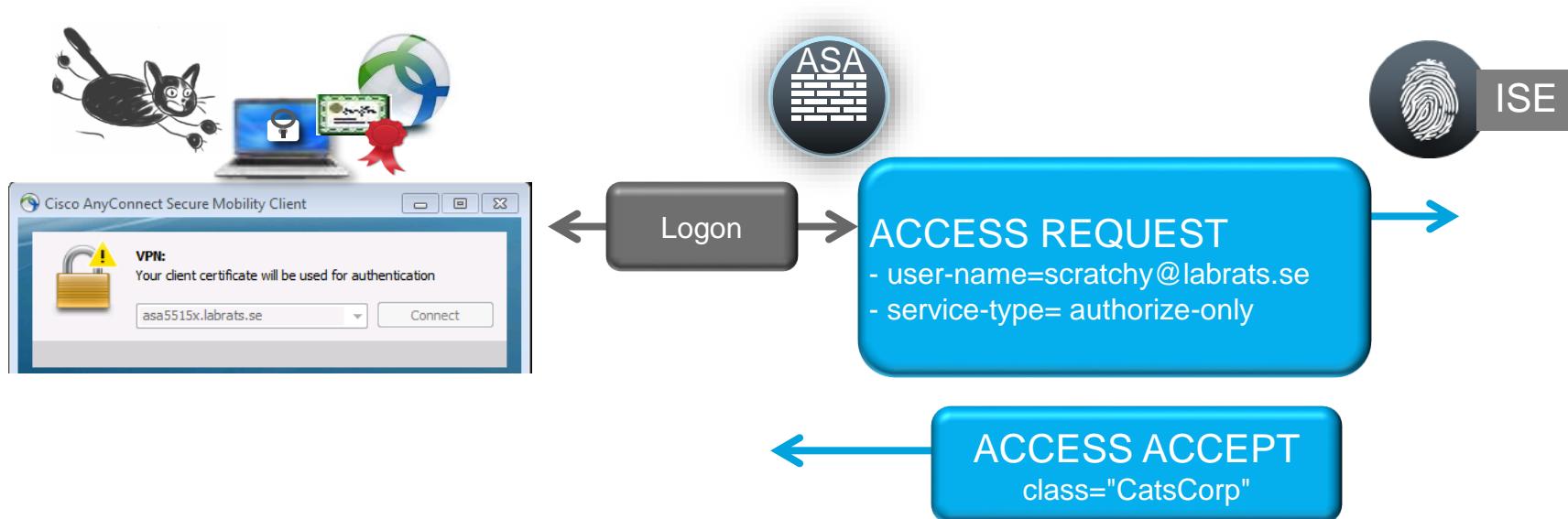
Interim Accounting

Authorization-Only

Dynamic Authorization (CoA, Change of Authorization)

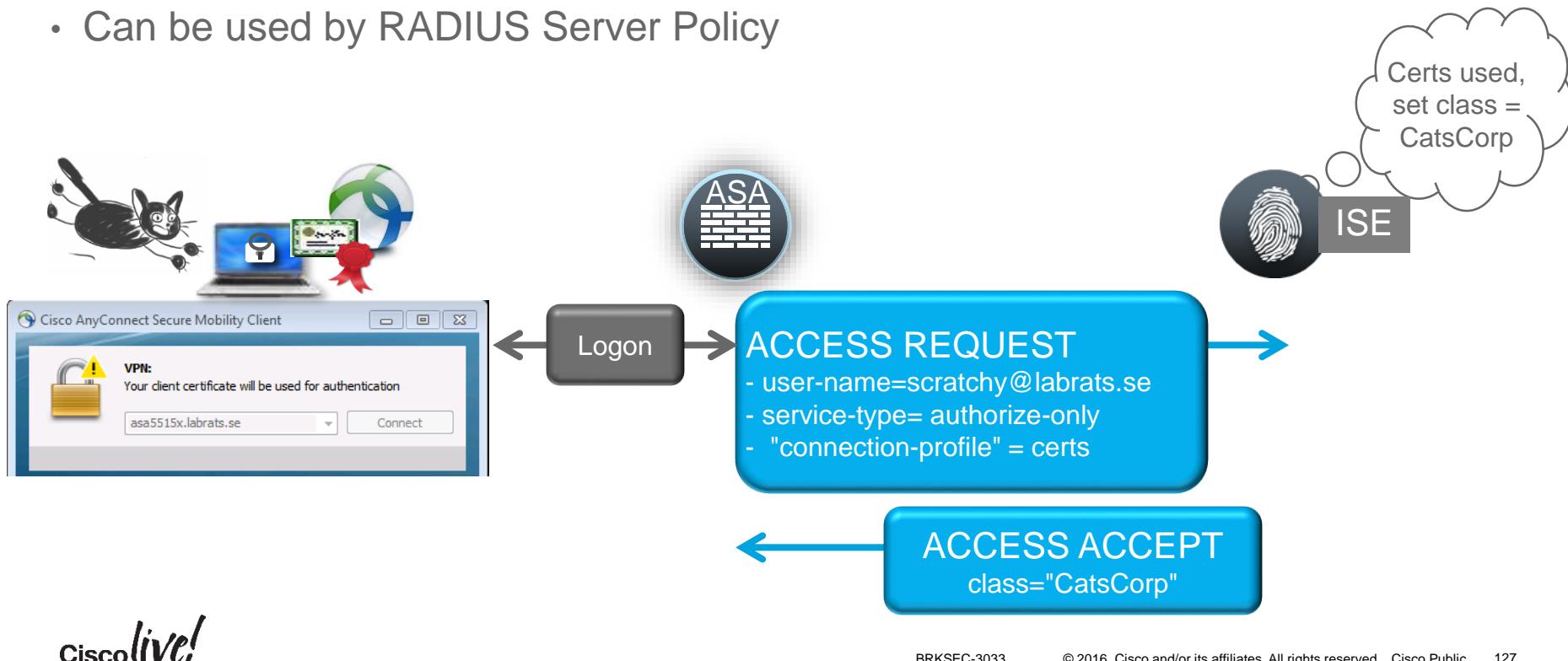
RADIUS Deep Dive: Client Certificate Authentication

- Authentication is between AnyConnect and ASA, ISE never sees or validates cert
- ASA does a authorize-only lookup (RFC 5176) with no password



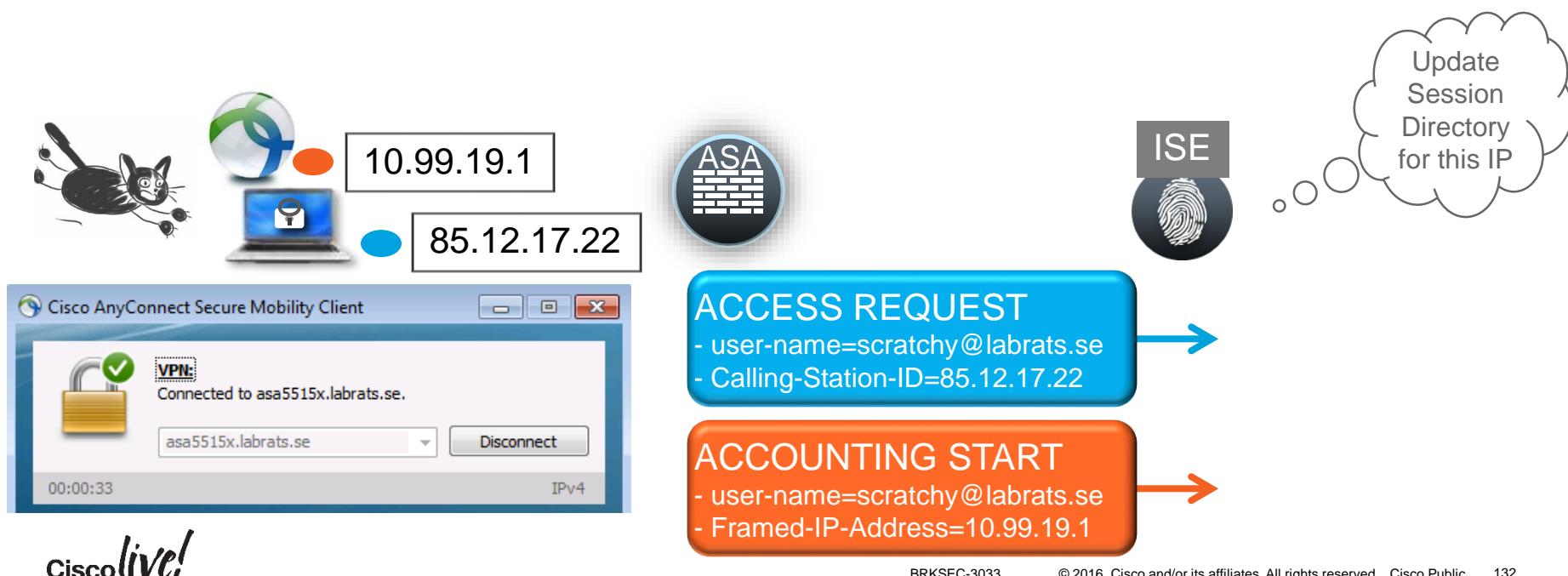
RADIUS Deep Dive: Connection Profile Name to ISE

- ASA sends info about Connection Profile and Client Type to RADIUS server
- Can be used by RADIUS Server Policy



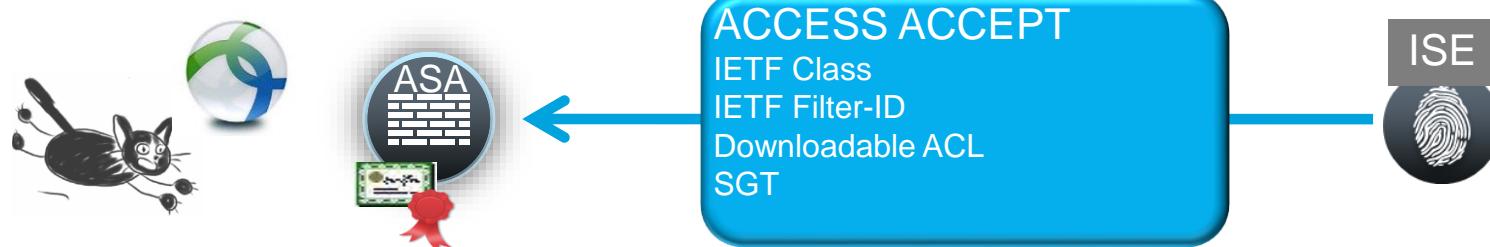
RADIUS: Keeping track of IP addresses

- Client physical ip address in RADIUS Calling-Station-ID
- Client virtual ip address in RADIUS Accounting Framed-IP-Address
 - turn on RADIUS accounting for visibility



ASA Authorization Options

- IETF Class Attribute
 - map to Group Policy where Filter (ACL), VLAN restriction etc. defined
- IETF Filter ID Attribute:
 - map to ACL pre-defined on ASA
- DAP (Dynamic Access Policy) specifying ACL
- Downloadable ACL (dACL)
 - ACL defined on ISE and downloaded with RADIUS to ASA
- Security Group TAG (SGT)



A Note on other (not **The** Firewall Rule table) ACLs

- Other ACL options: Group Policy, DAP, Filter-ID, dACL
 - applied from different places in GUI, separate from main Firewall Ruleset
 - applied from RADIUS (Filter-ID)

The diagram illustrates four methods to apply ACLs:

- Group Policy:** A screenshot of the "Edit Internal Group Policy" window for "catsCorp". It shows a "General" tab with "Servers" and "Advanced" sections like "Split Tunneling" and "AnyConnect Client". A blue callout box labeled "GroupPolicy CatsCorp" highlights the "Name" field set to "catsCorp".
- DAP:** A screenshot of the "Edit Dynamic Access Policy" window for "CatsCorp". It shows a "Network ACLs" section with a list containing "catsCorp". A blue callout box labeled "DAP CatsCorp" highlights this list.
- Filter-ID:** A screenshot of the "Edit Firewall Ruleset" window for "catsCorp". It shows two rules:
 - Rule 1: Action Permit, Source any, Destination Cats-ProjectX (HTTP/HTTPS), Service TCP (smtp), Action Permit.
 - Rule 2: Action Permit, Source any, Destination mail (TCP smtp), Action Permit.A red callout box labeled "Filter-ID" points to the "Action Permit" entry in the second rule's row.
- ISE:** A circular icon with a fingerprint pattern, labeled "ISE".

Consolidated Stateful Access Policy

Unified Control of all Access

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user interaction.

Access Interfaces

Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below!

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMZ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Bypass interface access lists for inbound VPN sessions

Unselect, to let VPN traffic go through Global/interface ACLs

Configuration > Firewall > Access Rules

Add | Edit | Delete | Find | Diagram | Export | Clear Hits | Show Log | Packet Trace

#	Enabled	Source Criteria:			Destination Criteria:			Service	Action
		Source	User	Security Group	Destination	Security Group			
4	<input checked="" type="checkbox"/>	any		testserver		http https	<input checked="" type="checkbox"/>	Permit	
5	<input checked="" type="checkbox"/>	any		mail		http https smtp	<input checked="" type="checkbox"/>	Permit	
6	<input checked="" type="checkbox"/>	any	SG_RatsCorp	Rats-Servers		http https	<input checked="" type="checkbox"/>	Permit	
7	<input checked="" type="checkbox"/>	any	SG_CatsCorp	Cats-ProjectX		http https	<input checked="" type="checkbox"/>	Permit	

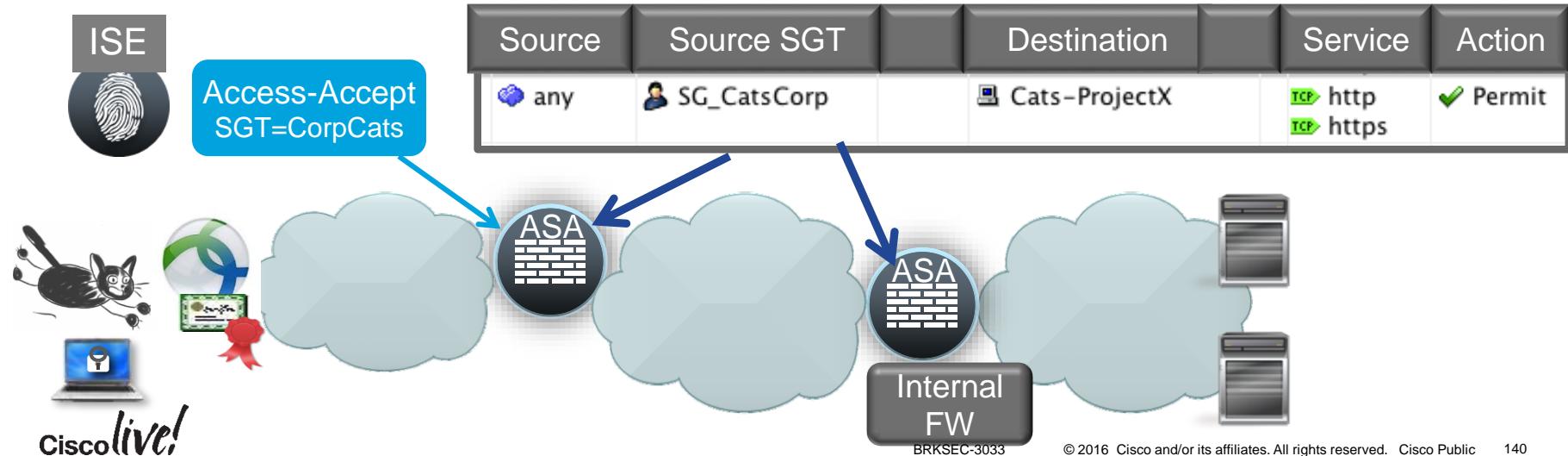
Cisco live!

Mix and Match ACEs with and without SGTs

Authorization with Security Group Tags

Unified Control of all Access

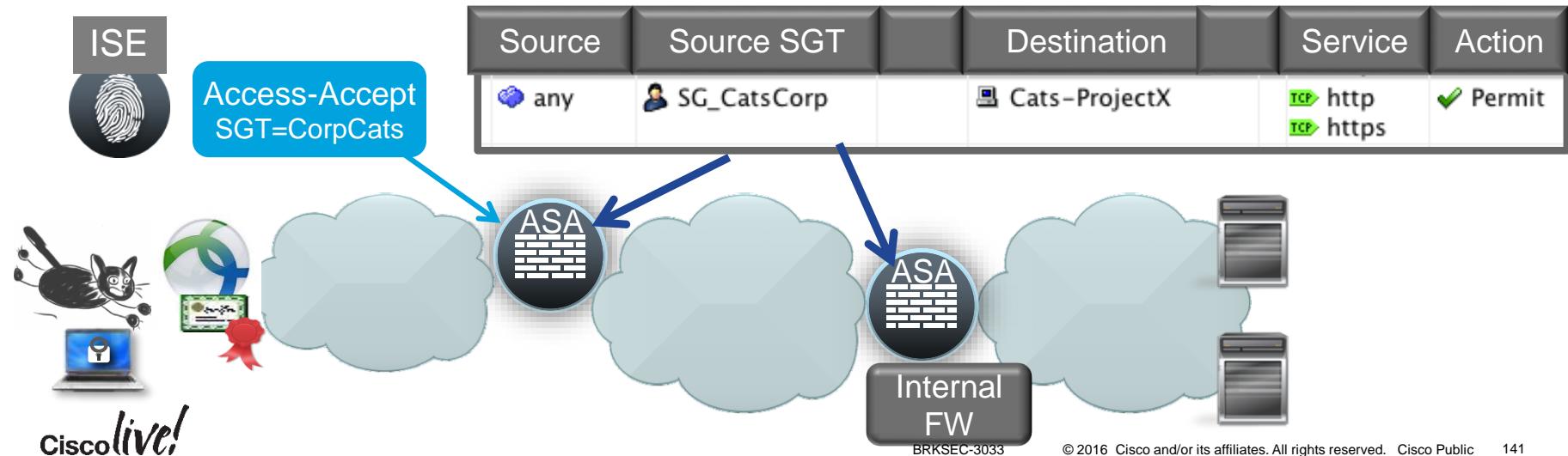
- ISE assigns SGTs to client session
- SGT used by ASA terminating Remote Access for policy enforcement
- ...and/or enforced by **downstream** device (e.g. ASA or Nexus in DC)
 - SGT info propagated by SXP or native SGT tagging (ASA 9.3.2)



This is Obviously **Cool**, but any Benefits?

Unified Control of all Access

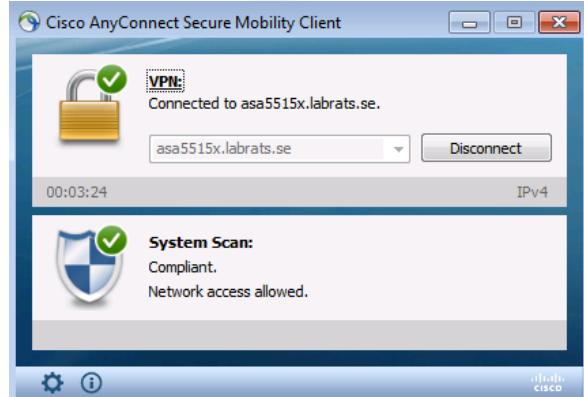
- De-coupling ip addressing from security
- Adding context (corporate device, AD group, posture status) to Firewall Rules
- Easy to configure same policy for VPN, Wired, Wireless
- ASA RA config: Consolidated, Statefull Security Policy.



AnyConnect ISE Posture Module

Desktop Posture
Checking and
Remediation

- Windows and MAC
- Checks and Remediates Posture
 - Works on campus (wired, wireless 802.1X)
 - Works with AnyConnect VPN
- Software and XML config file provisioned from
 - ASA
 - ISE or
 - **via Desktop Management System**
- Requires Compliance Module provisioned from
 - ISE or
 - via Desktop Management System



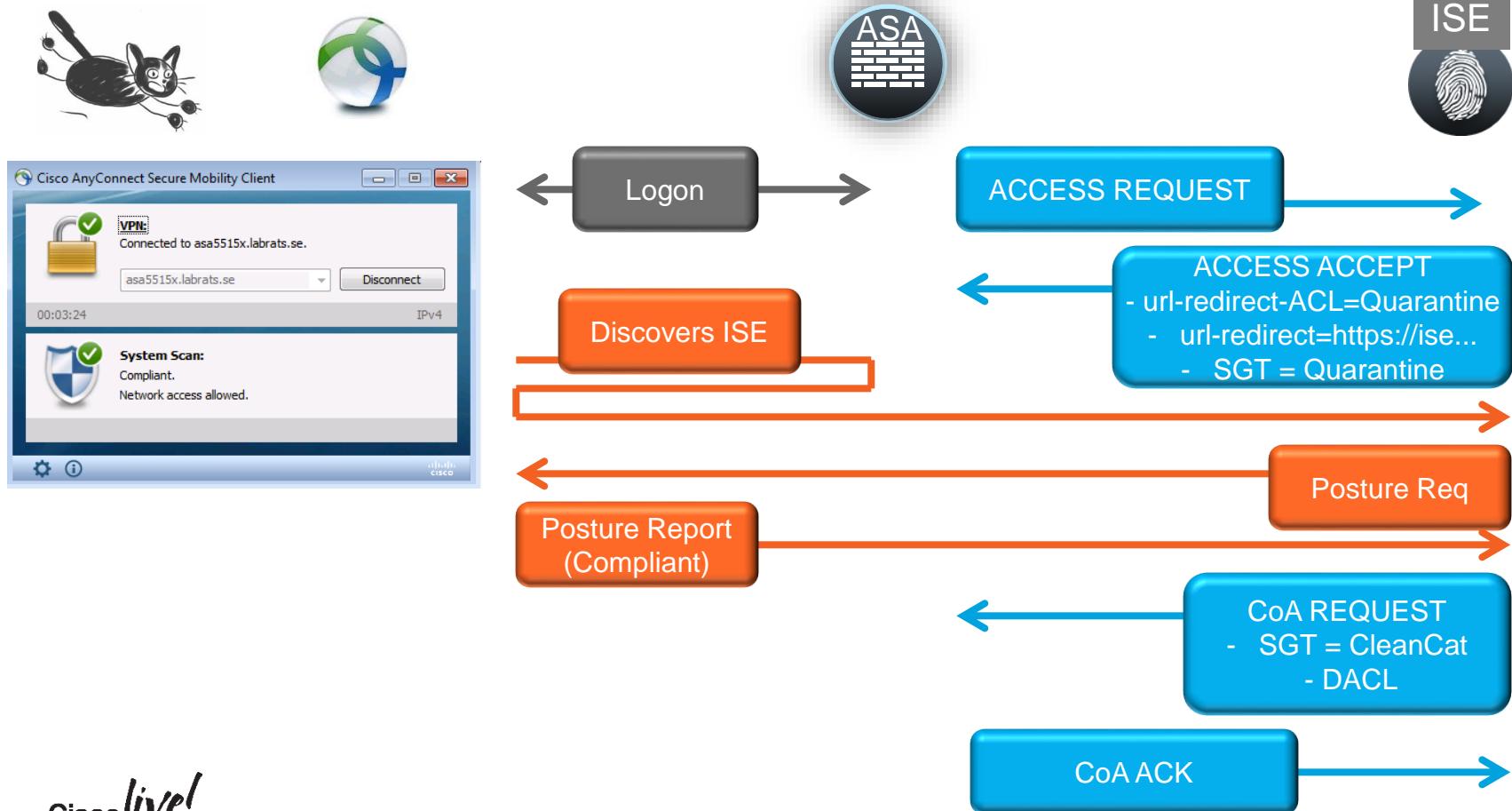
Desktop Posture Assessment



Agent Listing	Windows AnyConnect / NAC Agent	MAC OSX AnyConnect / NAC Agent
Client Provisioned by ISE		
Posture Assessment		
Microsoft Updates		
Service Packs		Not Applicable
Hotfixes		
OS / Browser Versions		
AntiVirus		
Installation / Signatures		
AntiSpyware		
Installation / Signatures		
File Data		Not Available
Services		
Application / Processes		
Registry Keys		
Posture Remediation		
Passive Re-Assessment (PRA)		



AnyConnect ISE Posture Flow



What to Configure on ASA for ISE Posture

- Configure a standalone ACL
 - permit means redirect traffic to ISE (default)
 - deny means do not redirect : this is traffic to ISE itself, traffic to remediation servers...
 - name of ACL must match RADIUS attribute "**"url-redirect-acl"** signaled by ISE

Configuration > Firewall > Advanced > ACL Manager

The screenshot shows the ASA ACL Manager interface. At the top, there are buttons for Add, Edit, Delete, and navigation. Below is a table with columns: Destination, Service, and Action. The first row (entry 1) has 'any' in Destination, 'ISEs' in Service, and 'ip' with a yellow arrow icon in Action, followed by a red 'Deny' button. The second row (entry 2) has 'any' in Destination, 'any' in Service, and 'ip' with a yellow arrow icon in Action, followed by a green 'Permit' button.

	Destination	Service	Action
1	any	ISEs	ip Deny
2	any	any	ip Permit

Deny means
"Do not Redirect"

Permit means "Redirect
to ISE"

Information Sharing

3rd Party Information Sharing

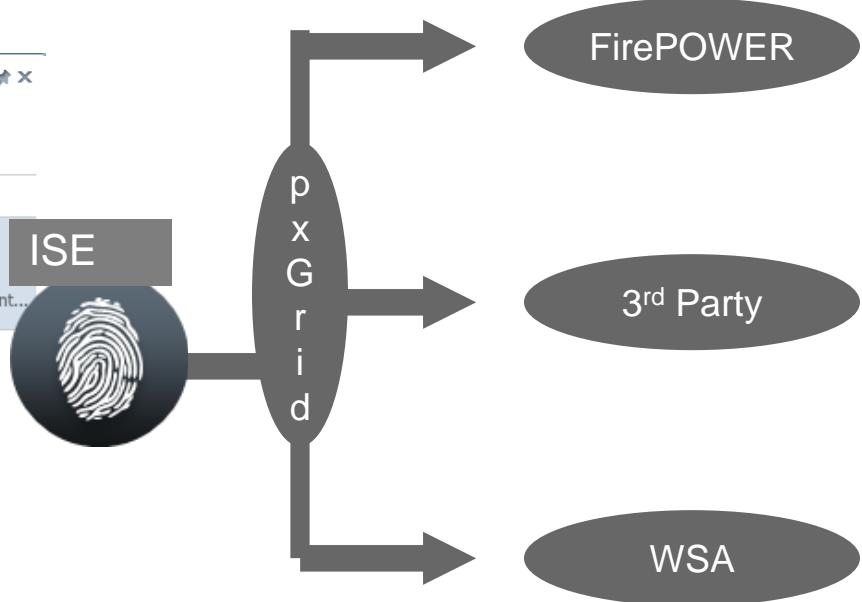
- ISE knows identity, device, posture status, authentication method for everything
- ISE shares info via pxGrid

Search

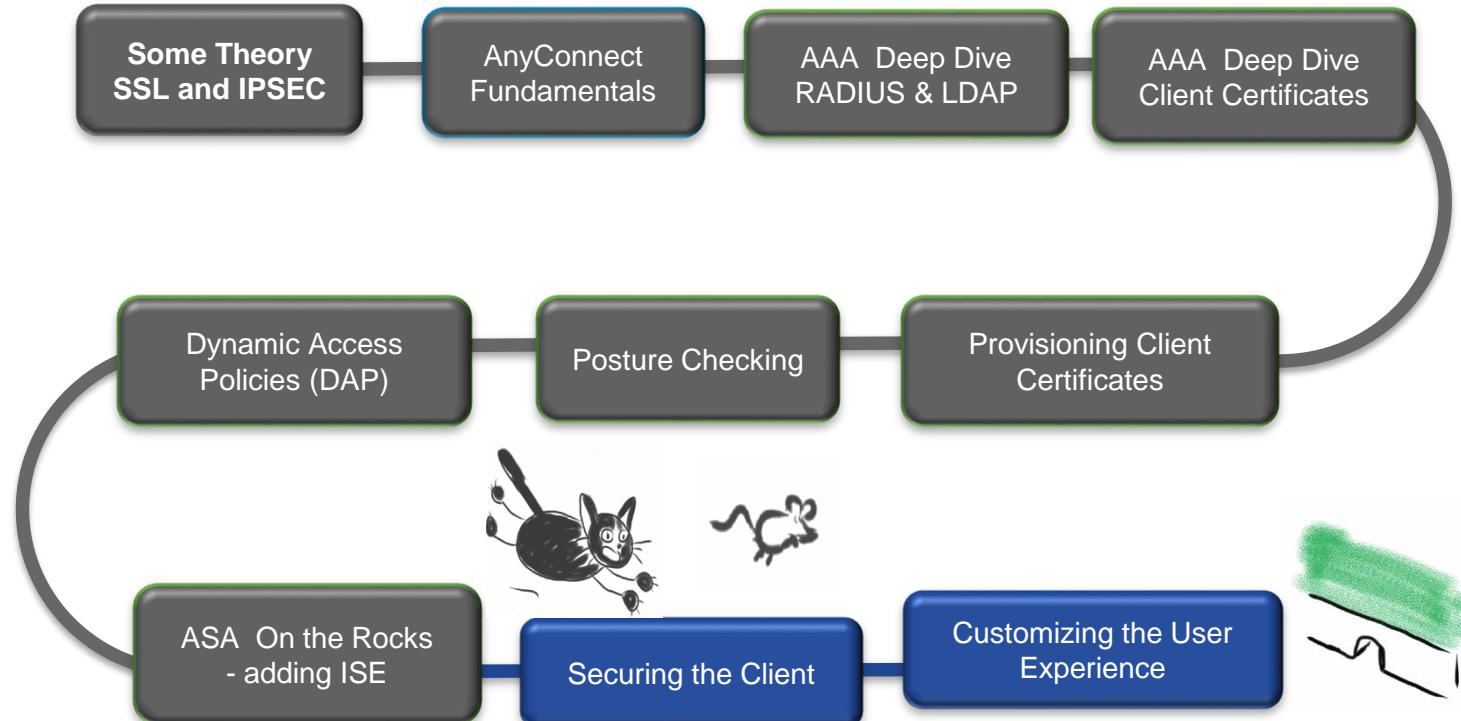
1 Connected | 0 Failed | 0 Disconnected | 1 Total

Distribution

	Endpoints ordered based on recent activity.
► Authorization Profile (1)	Unknown <input checked="" type="checkbox"/> scratchy@labrats.se, 192.168.1.2, -
► Identity Group (1)	All Locations, All Device Types#AS..., Posture-ASA,Quarant...
► Identity Store (1)	
► Location (1)	
► Network Device (1)	
► Network Device Type (1)	
► Posture Status (1)	
▼ Security Group (1)	
Quarantine (1)	



Agenda



(No) Split Tunnelling Policy

- Defined in Group Policy : whether to allow traffic outside of the tunnel

Edit Internal Group Policy: CatsCorp

The VPN client makes split tunneling decisions on the basis of a network list that can be defined here.

Advanced

- Split Tunneling
- Browser Proxy
- AnyConnect Client
- IPsec(IKEv1) Client

DNS Names: Inherit

Send All DNS Lookups Through Tunnel: Inherit Yes No

Policy: Inherit Tunnel All Networks

IPv6 Policy: Inherit Tunnel All Networks

Network List: Inherit

Split DNS

Split IPv4

Split IPv6

DENIED

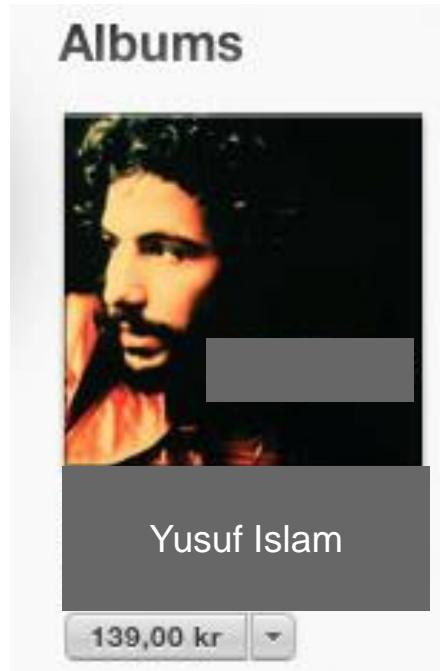
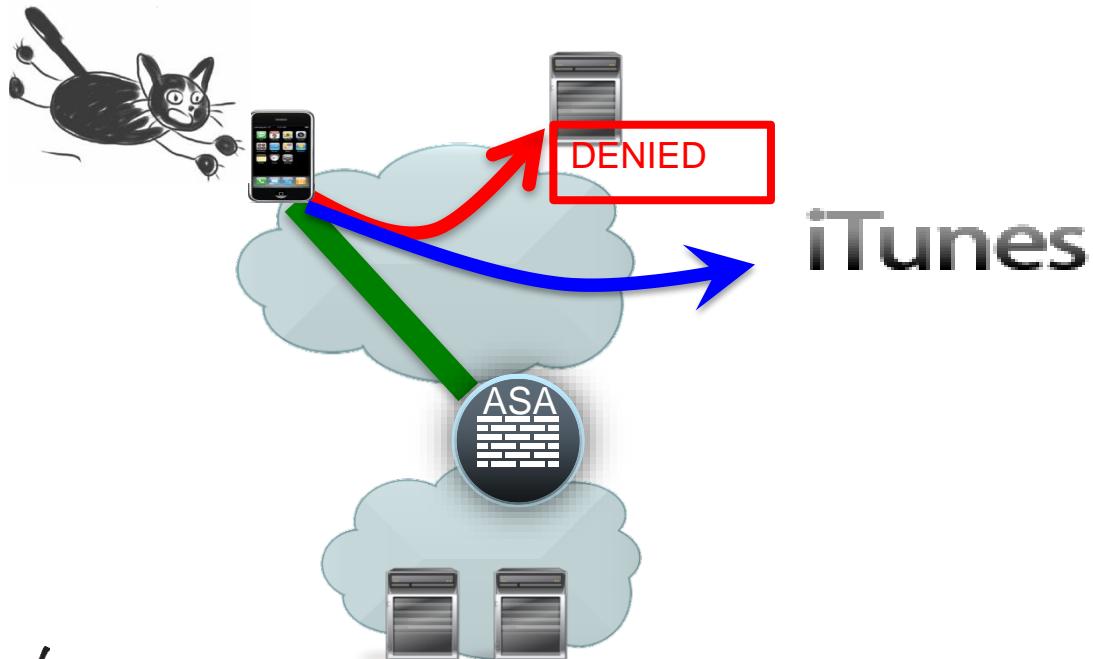
Internet

ASA

Cisco live!

Note on Split Tunnelling Policy for mobile devices

- Even with no Split Tunneling (Tunnel All Networks), certain traffic from mobile devices (e.g. iTunes) goes outside the tunnel



Split Tunneling Example (IPv4 and IPv6)

The screenshot shows the Cisco ACL Manager interface. At the top, there are three policy sections: Policy (Inherit, Tunnel Network List Below), IPv6 Policy (Inherit, Tunnel Network List Below), and Network List (Inherit, SplitACL-v4v6). A blue callout points to the Network List entry, stating "Extended ACL (extended ACLs are unified v4 v6)".

The main window displays an "Extended ACL" table with the following data:

#	Enabled	Action	Source	Destination	Service
1	<input checked="" type="checkbox"/>	Permit	Infrastructure-network/24	any	IP ip
2	<input checked="" type="checkbox"/>	Permit	Infrastructure-network6/64	any	IP ip

A blue callout points to the "Source" column, stating "Add IPv4 and IPv6 networks in the Source".

At the bottom right of the dialog are buttons for OK, Cancel, and Help.

No Split Tunneling but Allow Local LAN Access

Group Policy

Policy: Inherit
IPv6 Policy: Inherit
Network List: LOCAL-LAN-v4v6

Exclude Network List Below
Exclude Network List Below
LOCAL-LAN-v4v6

Must also be allowed per client profile

ACL Manager

Exclude Network List 0.0.0.0/32 ::/128

Standard ACL Extended ACL

#	Enabled	Action	Source	Destin...	Service
1	<input checked="" type="checkbox"/>	Permit	0.0.0.0	any	IP ip
2	<input checked="" type="checkbox"/>	Permit	::	any	IP ip

AnyConnect Client Profile Editor - HiSec

Profile: HiSec

VPN Preferences (Part 1) Preferences (Part 2)

Backup Servers Certificate Matching

Local Lan Access User Controllable

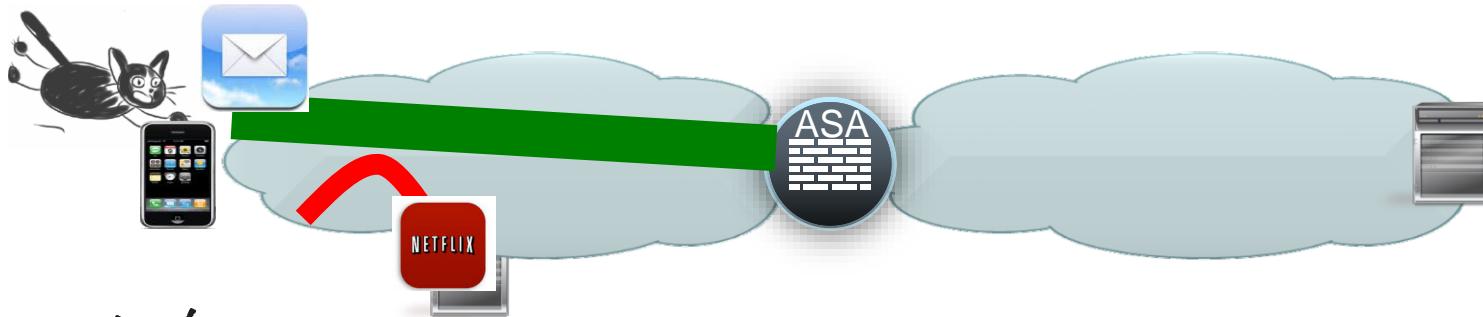
DENIED

ASA

cisco live!

Per App VPN

- Available for iOS 7.0+, Samsung Knox, Generic Android 5.0+
- Allows for tunneling specified subset of apps through one AnyConnect tunnel
 - save resources : don't Netflix over VPN tunnel
 - security: don't allow non enterprise apps on enterprise network
- Configured via DAP
- Works with or without an Enterprise MDM

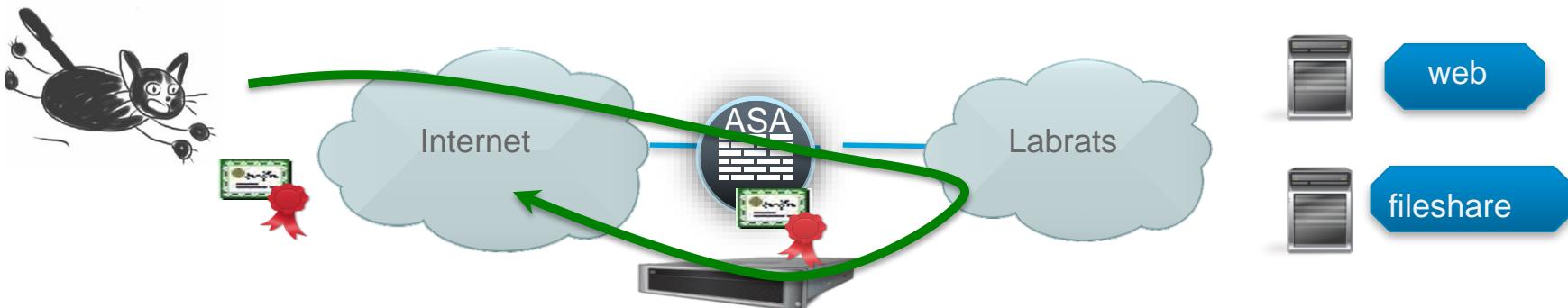


Seamless Security with Always-On

- Encourage/force (some) users to always be connected over VPN when off-premises
 - works on Windows, MAC
- Objective #1 : Seamless, simple user experience
 - Automatic Connection, "I am always at work" ☺
- Objective #2: Increased Security if surfing out via Enterprise Proxy or NGFW

Trusted Network Detection
automatically establishes tunnel if not on enterprise network

Always On
Blocks traffic until tunnel is established,



AnyConnect Client Profile with Always-On

AnyConnect
Client Profile

- Define conditions for Trusted Network Detection
 - DNS Servers and Domain
 - **AC 4.2: https:// reachability**
- Define Always-On (must also define Server List)
- Connection Failure Policy : Open or Closed
 - Balance Security Requirements vs. Risk of No Network...
 - If Closed, specify if traffic will be allowed for X minutes if Captive Portal is **detected**
 - "Last VPN Local Resource Rules" : Last Client Firewall Rules

The screenshot shows the 'Profile: vpnalwayson' configuration window. On the left, there's a sidebar with icons for VPN, Preferences (Part 1), Preferences (Part 2) (which is selected), Backup Servers, Certificate Matching, Certificate Enrollment, Mobile Policy, and Server List. The main area is titled 'Preferences (Part 2)'.

Trusted Network Detection: automatically establishes tunnel if not on enterprise network

Always On: Blocks traffic until tunnel is established, except if Captive Portal is detected

Performance Improvement Threshold (%): 0%

Automatic VPN Policy: Selected. Options: Trusted Network Policy, Untrusted Network Policy.

Trusted DNS Domains: labrats.se

Trusted DNS Servers: Note: adding all DNS servers in use is recommended with Trusted Network Detection.

Trusted Servers @ https://<server>[:<port>]: https://test.labrats.se:443

Certificate Hash: DD66B76A9138BB4168DEC1D2A797A16276E4D7EC60BBB2F5F293A26B88EBD7C7

Always On: Selected. (More Information)

Allow VPN Disconnect: Selected

Connect Failure Policy: Closed

Allow Captive Portal Remediation: Selected

Remediation Timeout (min.): 5

Apply Last VPN Local Resource Rules: Unselected

Disabling Always-On with DAP

- Always-On can be disabled by DAP
- AnyConnect will remember this setting when disconnected

The screenshot shows the Cisco DAP (Dynamic Access Policy) configuration interface. It displays two main sections: 'User has ANY of the following AAA Attributes values...' and 'and the following endpoint attributes are satisfied.' Both sections include 'Add', 'Edit', and 'Delete' buttons.

AAA Attribute Operation/Value:

AAA Attribute	Operation/Value
ldap.memberOf	= CompetitiveAnalysis

Endpoint ID Name/Operation/Value:

Endpoint ID	Name/Operation/Value
policy	location = CorporateWindows
av.ClamAV	description = ClamWin Antivirus lastupdate < 1 activescan = ok

Advanced

Access/Authorization Policy Attributes

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Action Network ACL Filters (client) Webtype ACL Filters (clientless) Functions Port Forwarding Lists Bookmarks Access Method AnyConnect

Always-On VPN for AnyConnect client: Unchanged Use AnyConnectProfile setting Disable

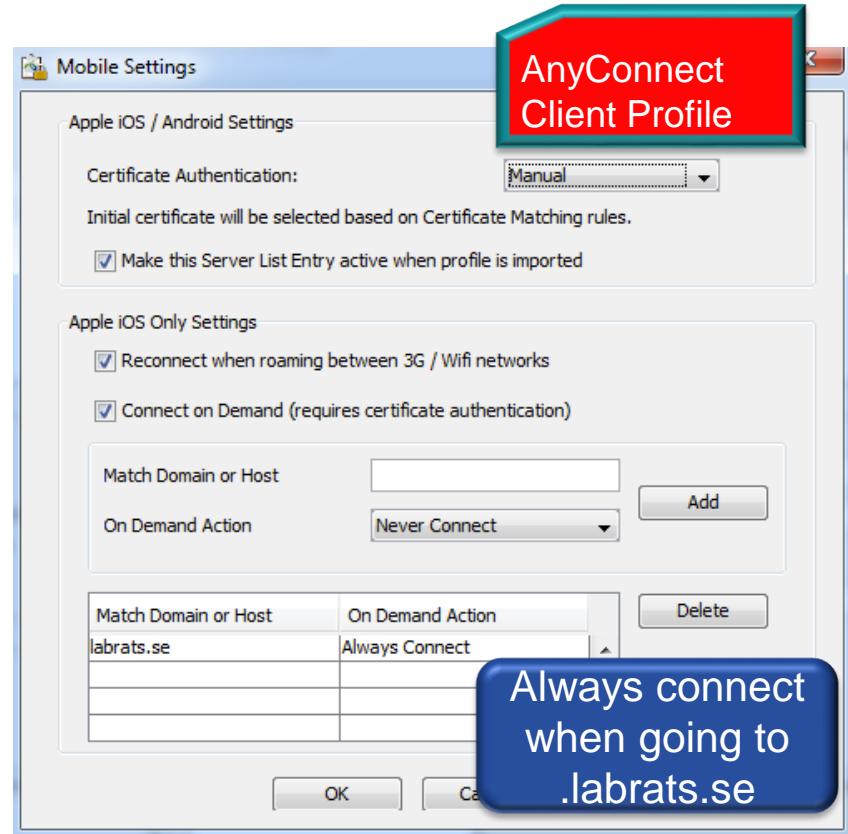
Always On does not work for Mobile Devices

- Forcing Always-On not possible due to lack of OS APIs
 - ... vendor considerations for battery life, security
- Trusted Network Detection (TND) for Android
- On Demand VPN for iOS

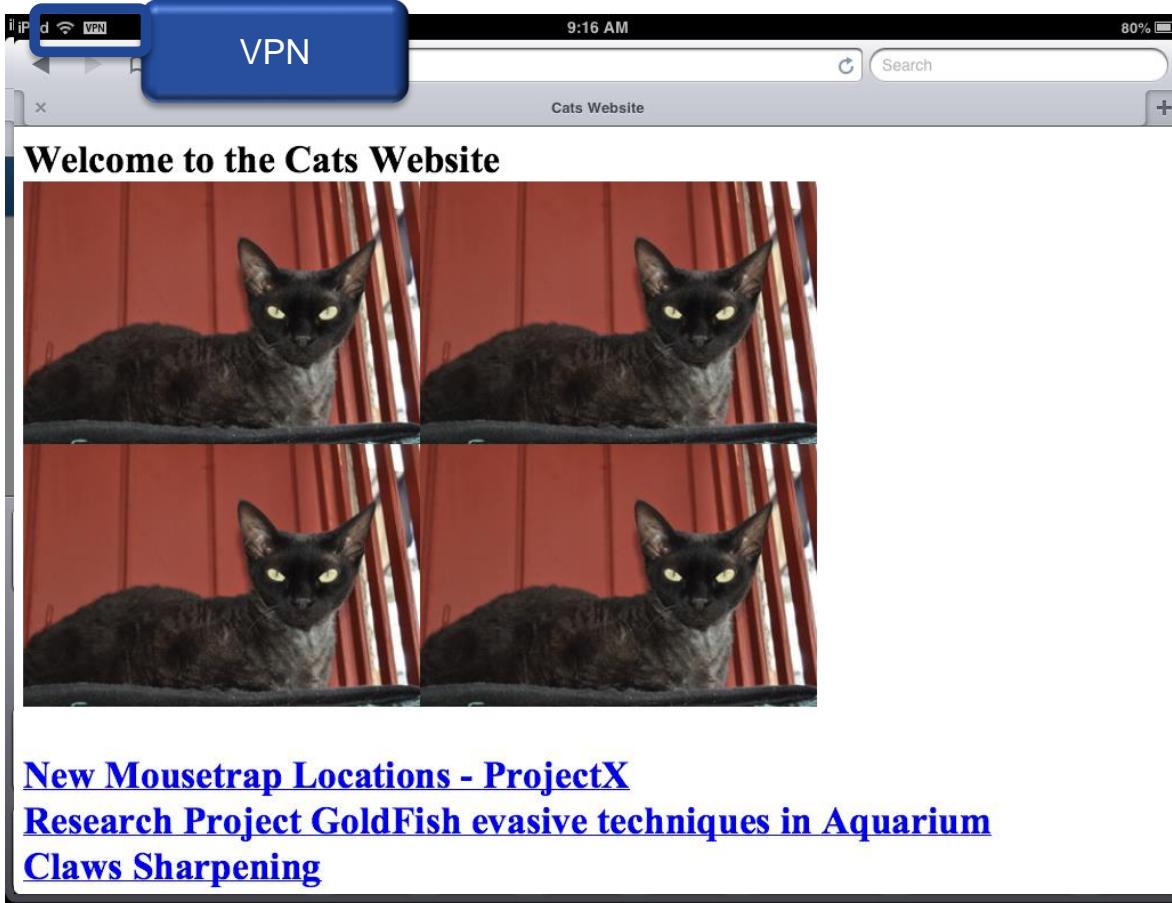


On Demand VPN for iOS - Configuration

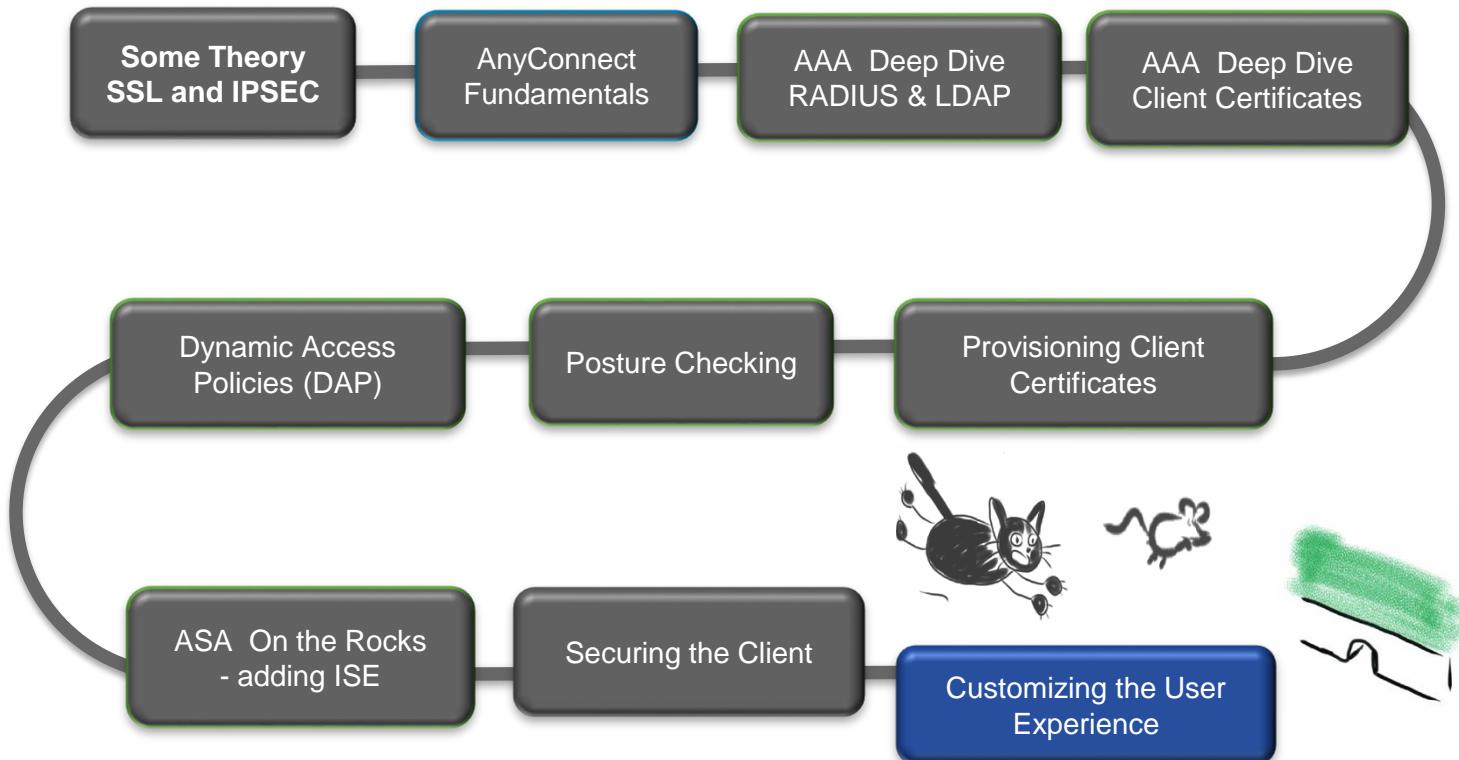
- VPN automatically connected when traffic directed to predefined domain
- Requires client certificate
- Configured in Client Profile/Server List/Additional Mobile Only Settings



On Demand VPN for iOS – User Experience

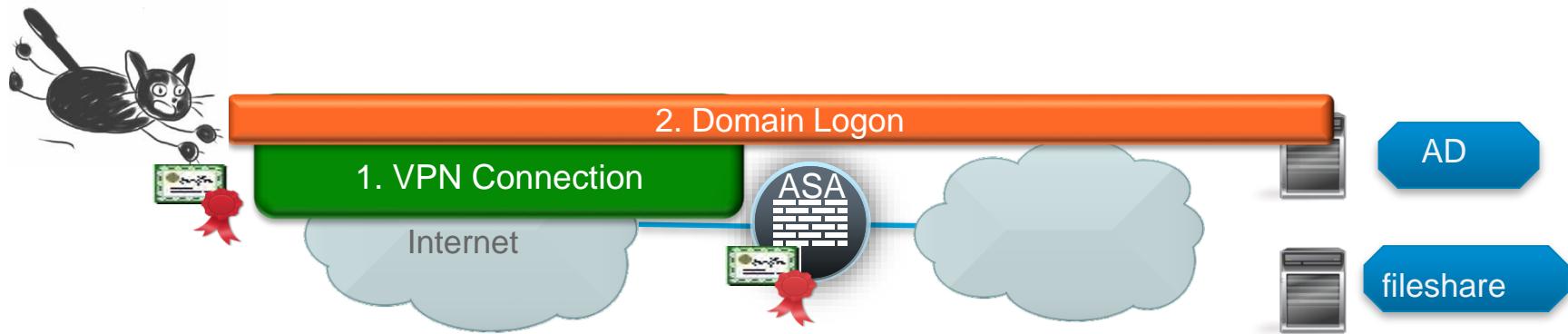


Agenda



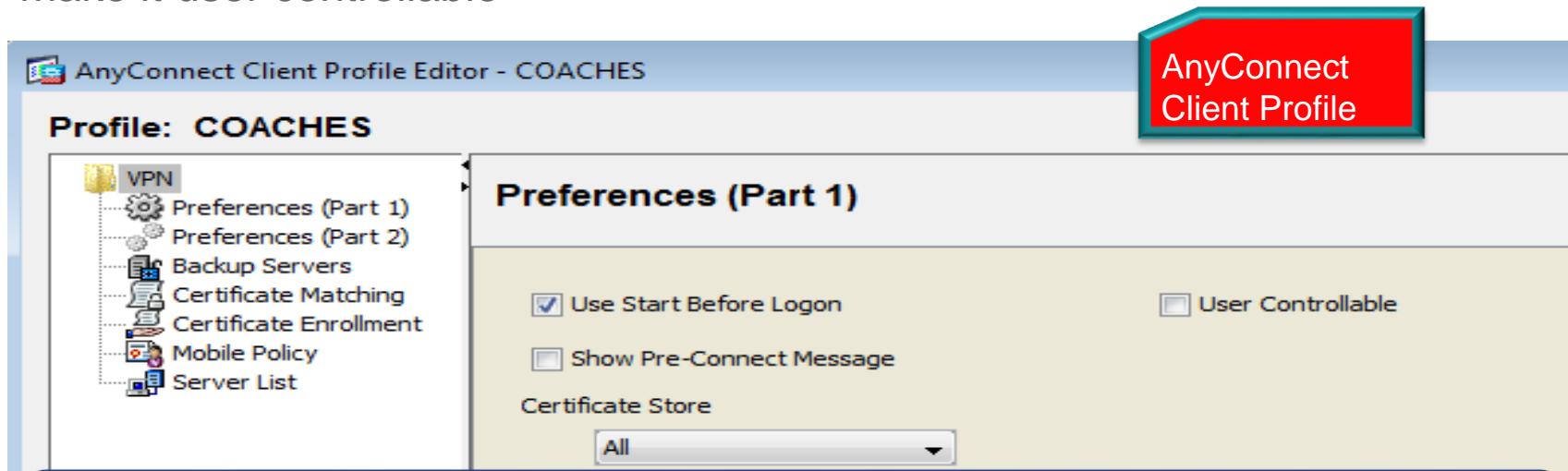
Seamless Office Experience by Start-Before-Logon

- Allows (some) Windows users to connect VPN before logging into computer
- Why? Allow domain-logon, GPOs, logon-scripts, change passwords, etc...
- Can be used with or without Always-On



Configuring SBL in Client Profile

- May make it user controllable

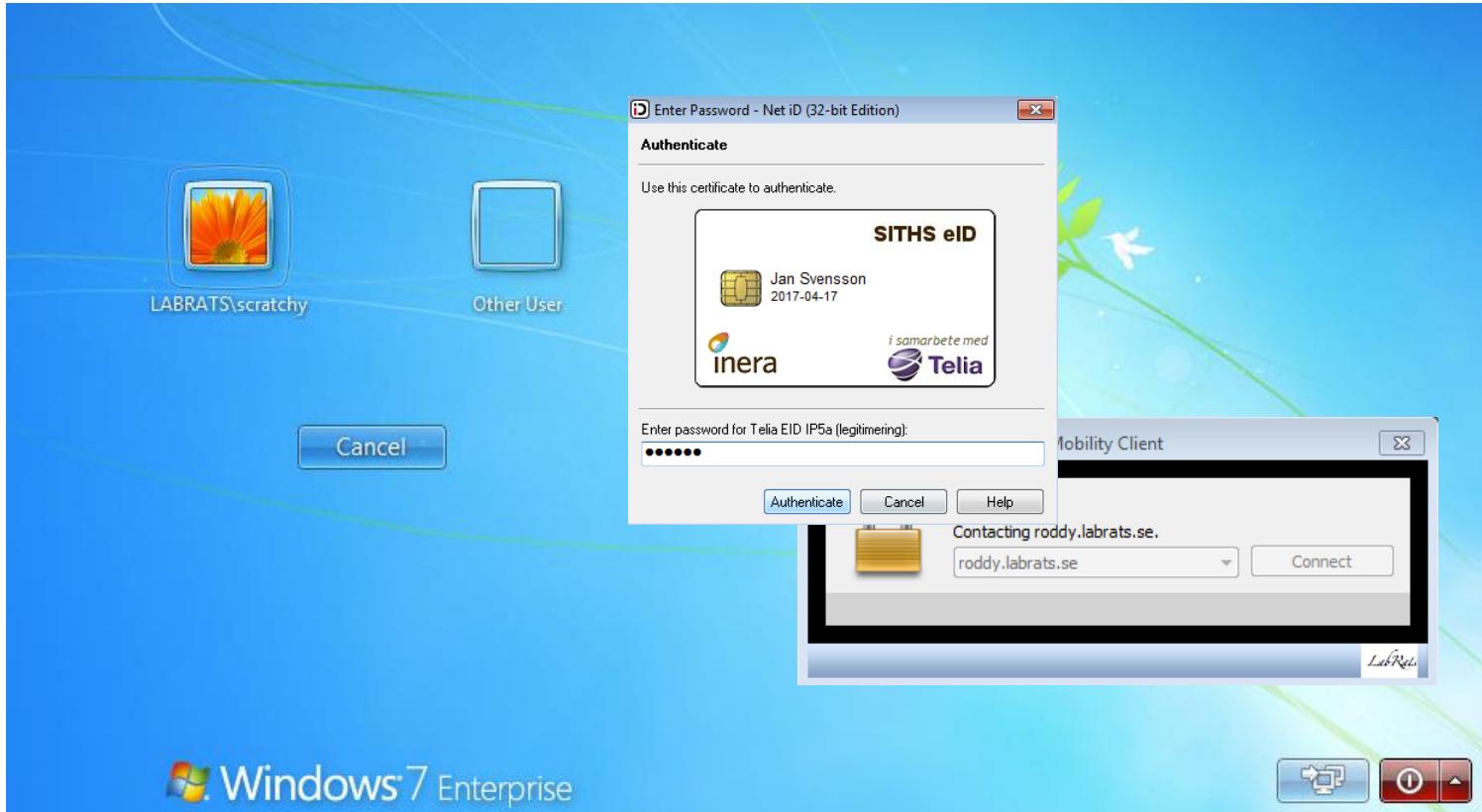


Note : Client certificates in User Store typically not accessible before logon (no knowledge of who the user is).
Client certificates on Smart Cards will work!

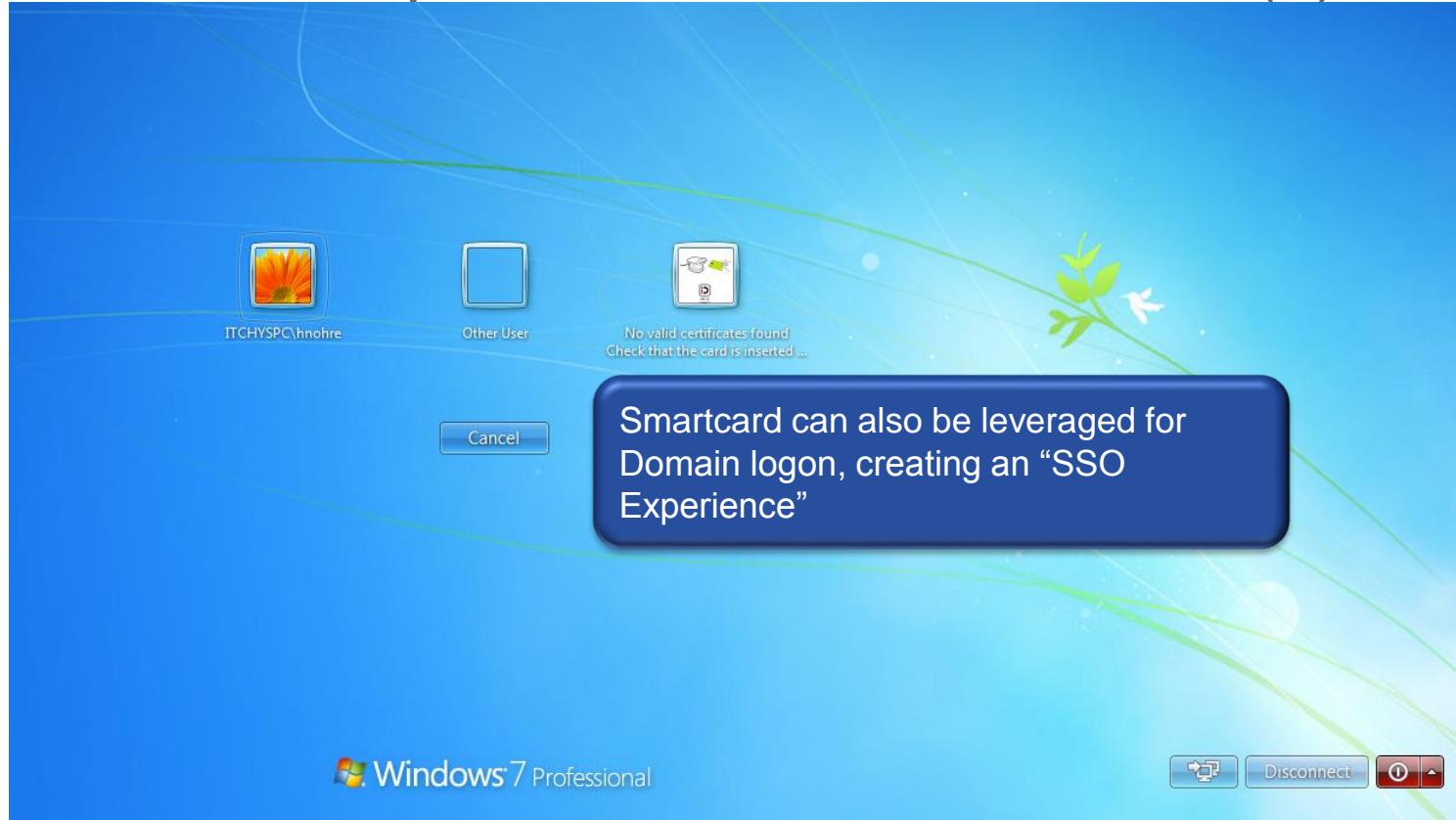
SBL User Experience



SBL User Experience with Smart Cards (2)

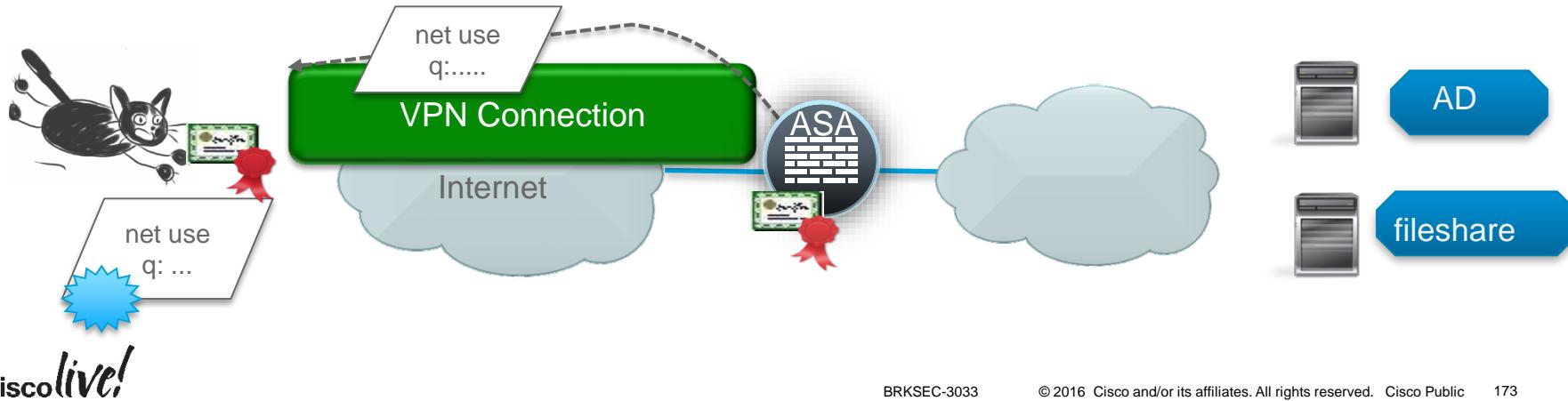


SBL User Experience with Smartcards (3)



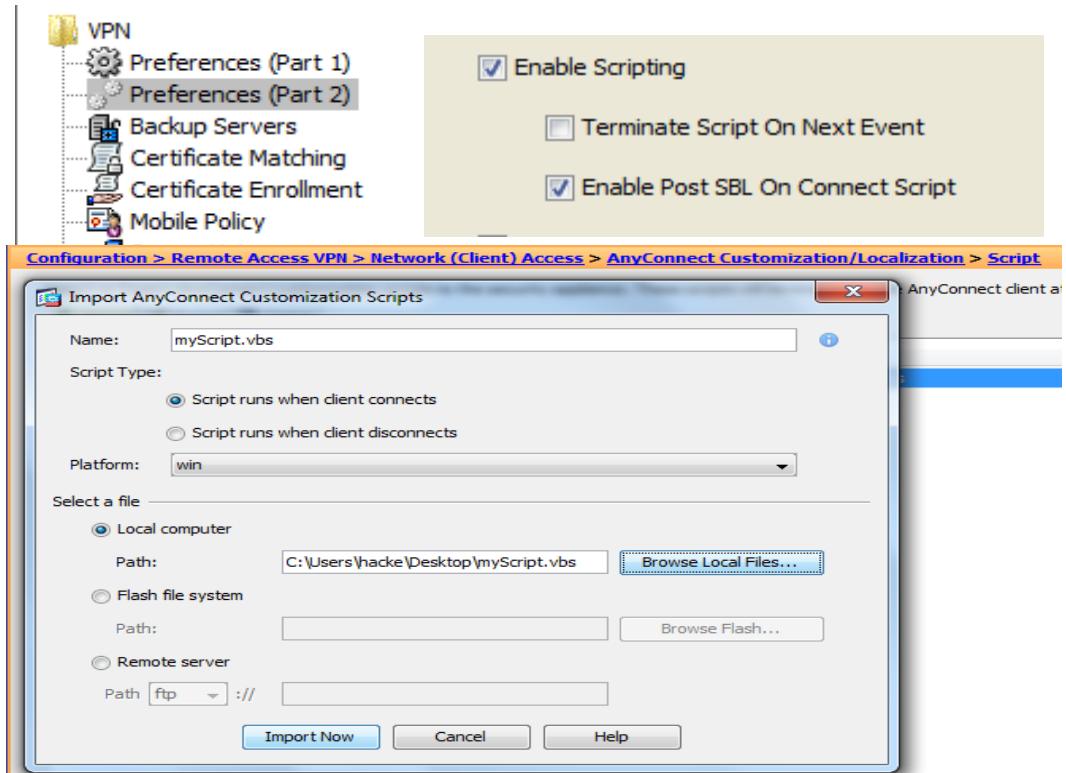
Running Scripts after Connect and Disconnect

- Runs a predefined script when (some) users connect to (or disconnect from VPN)
- Any native script language understood by client (*.vbs, *.sh etc)
- Script can be downloaded from ASA, or distributed by some other means
- Why?
 - Allow mapping of drives, GPO-update when SBL is not possible (e.g. behind a captive portal).
 - Also works on non domain members, including MAC, Linux



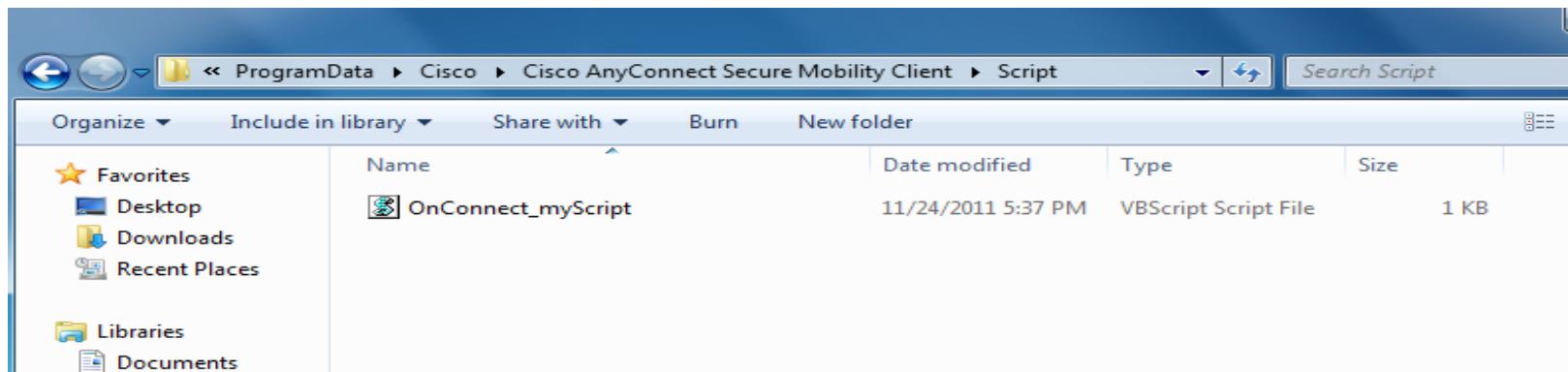
Configuring Scripting

- Enable Scripting in AnyConnect Client Profile
- Optionally : Import script to ASA for download to **all** clients
- Alternatively, use other means of putting the script in the script directory for desired clients



On the Client : The Scripts Folder

- AnyConnect executes the script in the folder that starts with "OnConnect"/"OnDisconnect" after VPN connection/disconnection
- Only one script is executed, but that script can launch other scripts
- Troubleshooting :
 - Check that script exists in folder and that AnyConnect Profile allows scripting.
 - Check that script executes ok when invoked from local machine (permissions etc).



Conclusion

- Secure Client with a Seamless User Experience
- Strong authentication and Granular Access Control with AAA and DAP
- Consider using ISE for Unified Access (VPN, Wired, Wireless)
- Find Balance between Requirements and Complexity (testing, maintenance)
- Good security and networking skills are essential, but also knowledge of adjacent technologies such as Active Directory, LDAP and PKI, ISE... as well as different client platforms

Complete Your Online Session Evaluation

- Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a \$750 Amazon gift card.
- Complete your session surveys through the Cisco Live mobile app or from the Session Catalog on CiscoLive.com/us.



Don't forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online

Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Table Topics
- Meet the Engineer 1:1 meetings
- Related sessions

Continue Your IPv6 Education

- Demos in the Cisco campus: SRv6, 6CN (DevNet Zone)
- Walk-in Self-Paced Labs: LABCRS-1000, LTRRST-2016
- Lunch & Learn: Tuesday, Wednesday
- Meet the Engineer 1:1 meetings
- Related sessions: BRKRST-2667, BRKRST-2616, BRKSEC-2003, BRKSEC-3033, BRKSEC-3771, BRKRST-3304, BRKRST-2044, BRKRST-2312, BRKRST-3045, BRKSEC-3003, BRKRST-2022, BRKSPG-2300, BRKSEC-3200
- World of Solutions: **ask about IPv6 support ;-)**

Security Joins the Customer Connection Program

Customer User Group Program

- **Who can join:** Cisco customers, service providers, solution partners and training partners
- **Private online community** to connect with peers & Cisco's Security product teams
- Monthly **technical & roadmap briefings** via WebEx
- Opportunities to **influence product direction**
- Local **in-person meet ups** starting Fall 2016
- **New member thank you gift* & badge ribbon** when you join in the **Cisco Security booth**
- **Other CCP tracks:** Collaboration & Enterprise Networks



Join in World of Solutions

Security zone → Customer Connection stand

- Learn about CCP and Join
- New member thank-you gift*
- Customer Connection Member badge ribbon

Join Online

www.cisco.com/go/ccb

Come to Security zone to get your new member gift* and ribbon

Thank you



Cisco *live!*

July 10-14, 2016 • Las Vegas, NV