

TOMORROW starts here.



Cisco *live!*

Remote Access Using Clientless VPN

BRKSEC-2697

Håkan Nohre

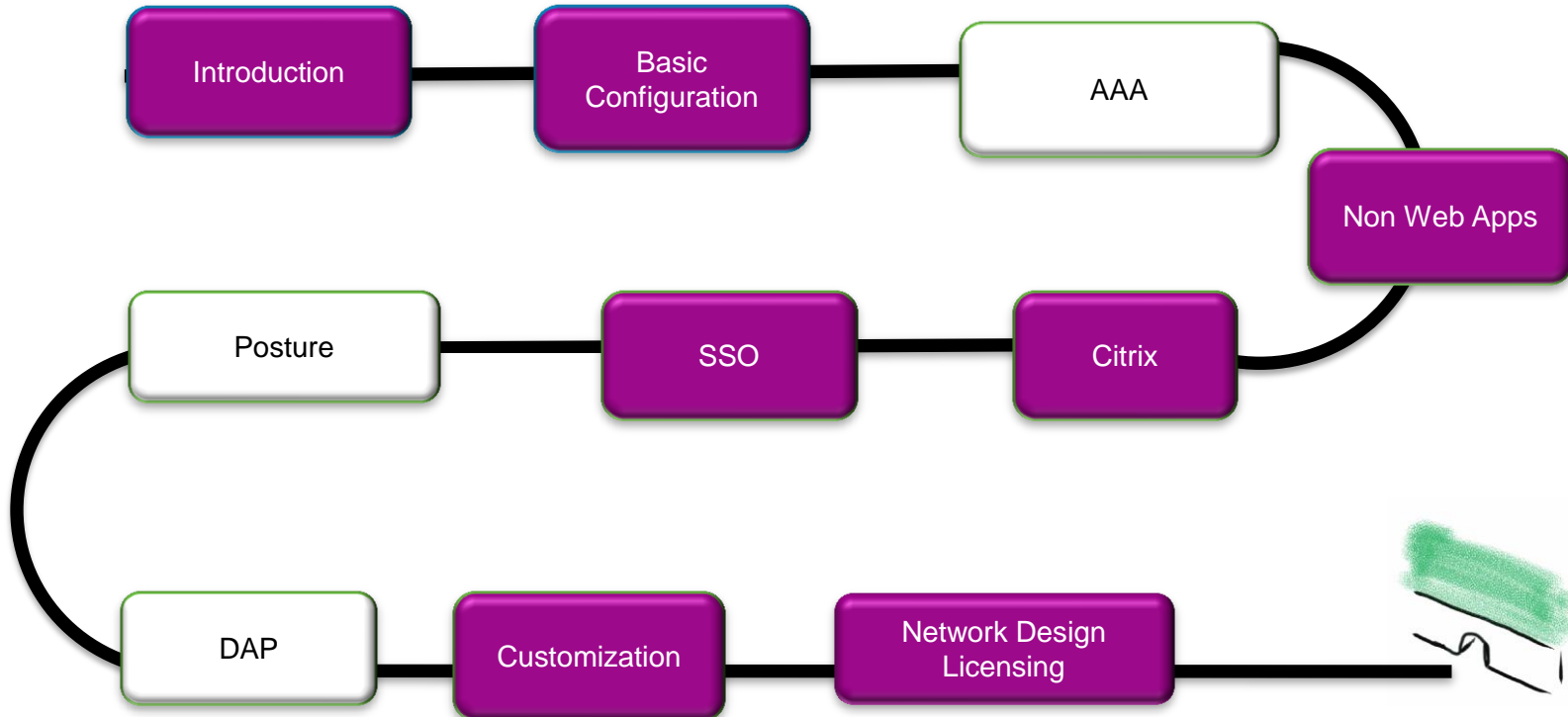
Consulting Systems Engineer

Agenda Comparison

BRKSEC-2697 (Clientless) vs BRKSEC-3033 (AnyConnect)

New in 2697

Big Overlap

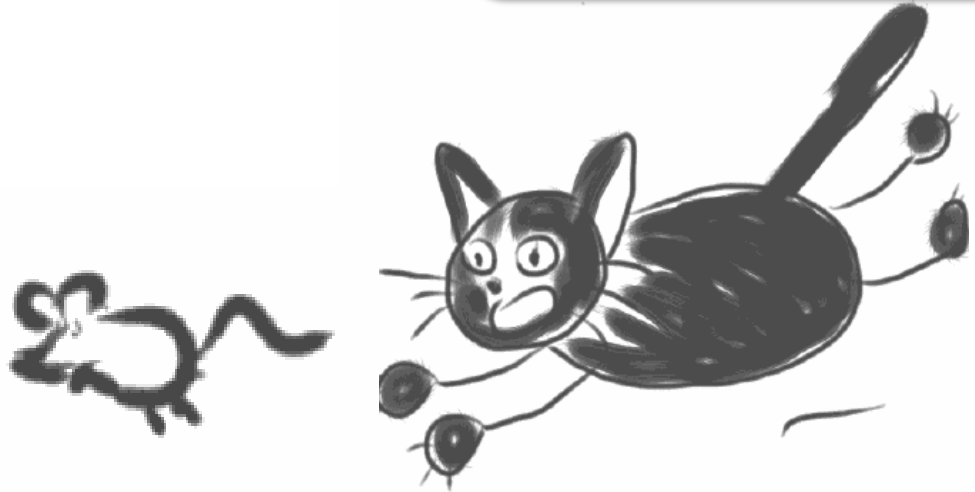


The Scenario : Labrats

- Pharmaceutical Research **Conglomerate***
run by Rats and Cats
- Using Corporate Devices
 - Windows, MAC, iPADS
- **Embracing BYOD**
- **Heavy use of Consultants**
- **Key Requirements :**
 - **Security**
 - **Easy to Use**
 - **IPv6**

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

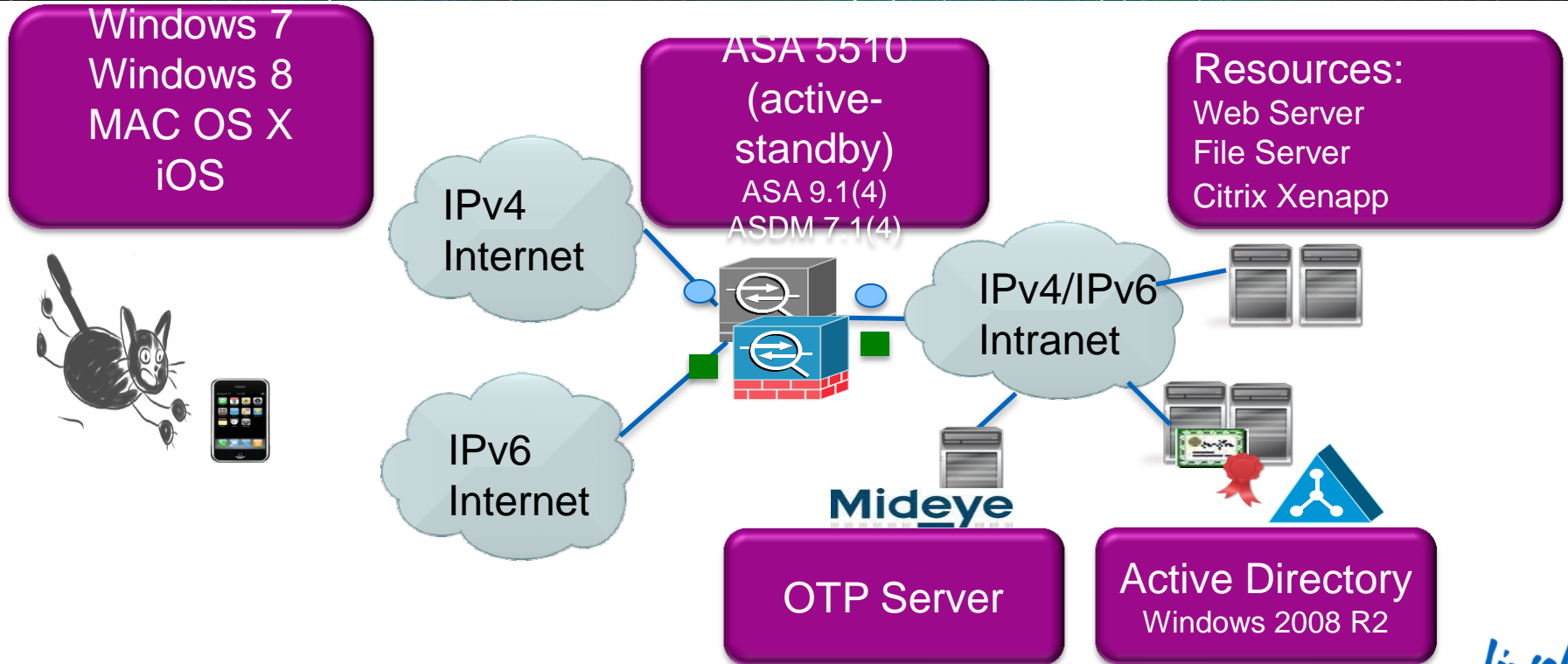
Wikipedia definition



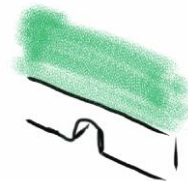
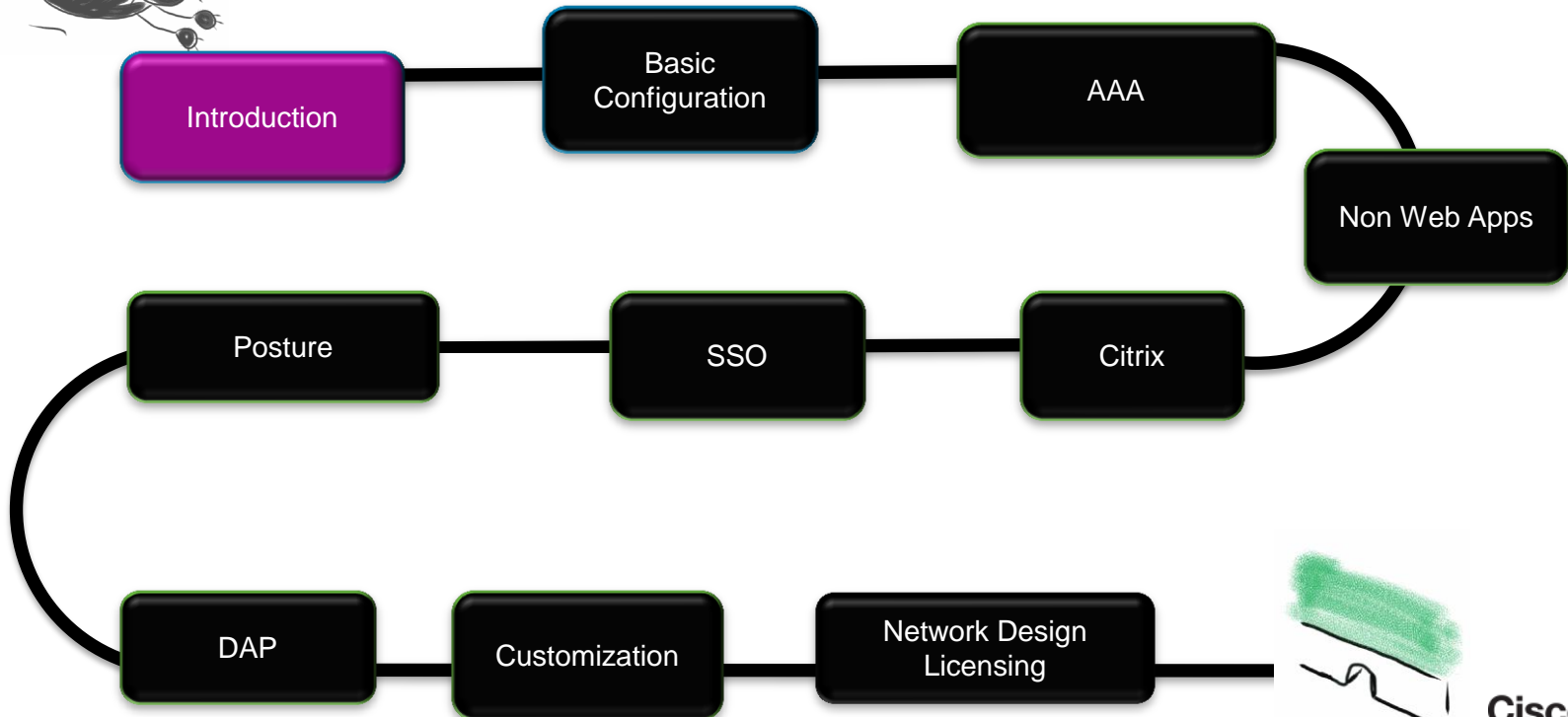


The Scenario : Labrats

Network Design and Versions Used



Agenda



Choosing Clientless SSL VPN or AnyConnect?

	Clientless SSL VPN	AnyConnect
End User Experience	Web Browser to access some applications	Just like in the Office
Access Control	Granular at URL level	Network ACL: IP and TCP/UDP port
Installation of client SW	No, uses browser.*	Yes, Thick Client
Maintenance	New versions of browsers, java, applications...	Once setup works fine

* Features may depend on OS, browser, Java, Active-X, endpoint security settings.

Clientless SSL VPN : Key Takeaways

- It is not completely Clientless
- It is not easier to implement than AnyConnect
- User experience will be different from “in-the-office”

- Clientless SSL VPN still has a role to play for remote access
- With ASA 5500 we can combine Clientless with AnyConnect!
- Key Objective of this breakout:
 - What we can do with Clientless SSL VPN
 - Limitations
 - How we configure it
 - Helping to choose wisely: When to use clientless

Important Web Protocols and Mechanisms

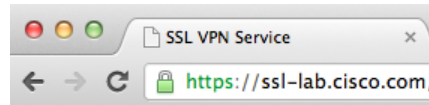
- HTML
 - Hypertext Markup Language : Defines the structure of web page
- CSS
 - Cascading Style Sheets : Defines the look and feel of web page
- JavaScript
 - Script run inside the browser
- Java Applets
 - Java code compiled to independent machine language downloaded to client
 - Runs inside Java Sandbox
- ActiveX
- Flash

Javascript is NOT the same as Java/Java Applets

Secure Sockets Layer (SSL) Overview

- A “**Secure Protocol**” developed by Netscape for secure e-commerce.
- SSL2.0 released in 1994, but had flaws and was replaced by SSL 3.0. Transport Layer Security (TLS) was published after that and continued to evolve.
- Creates a *tunnel* between web browser and web server
 - Authenticated and encrypted (RC4, 3DES, DES, AES)
- **https://**

Usually over port :TCP/443

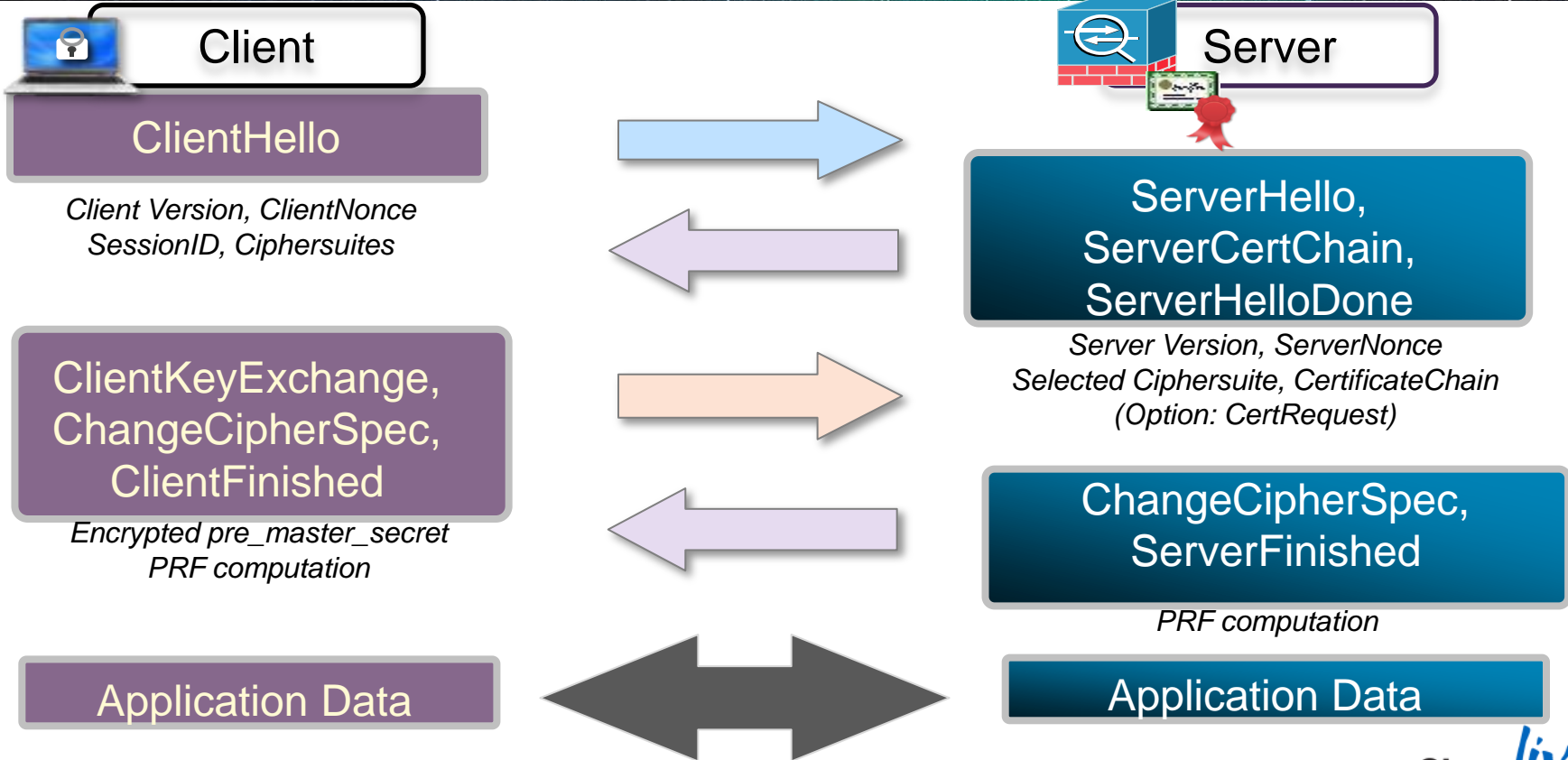


Refer to RFC 2246, for TLS 1.0

Refer to RFC 4346, 2006 for TLS 1.1

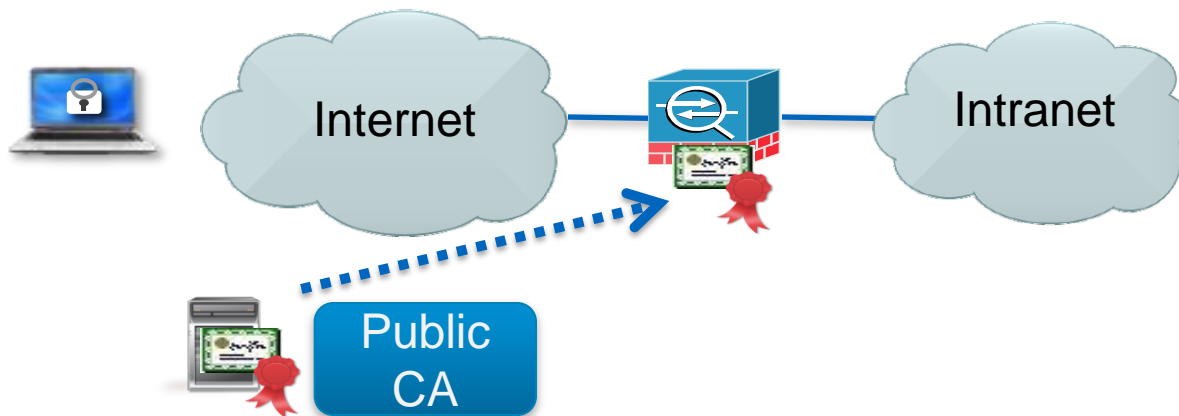
Refer to RFC 5246, 2008 for TLS 1.2

The TLS Handshake



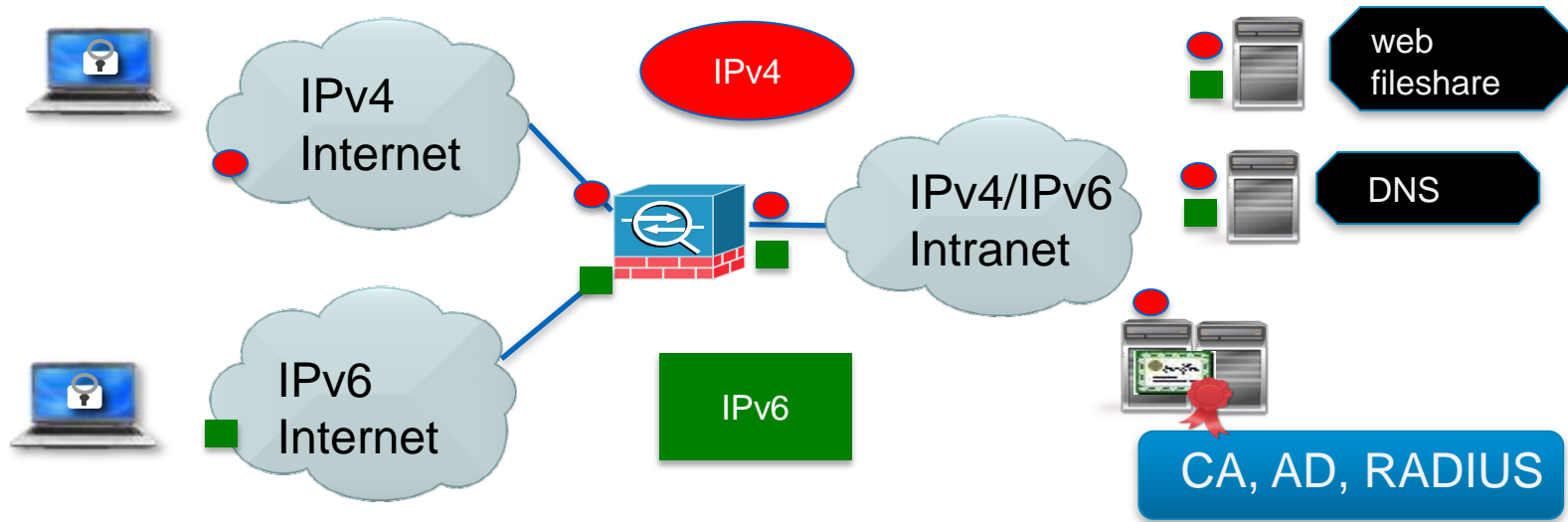
SSL Fundamentals : ASA Server Certificate

- 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)
- FQDN in Subject Name : roddy.labrats.se



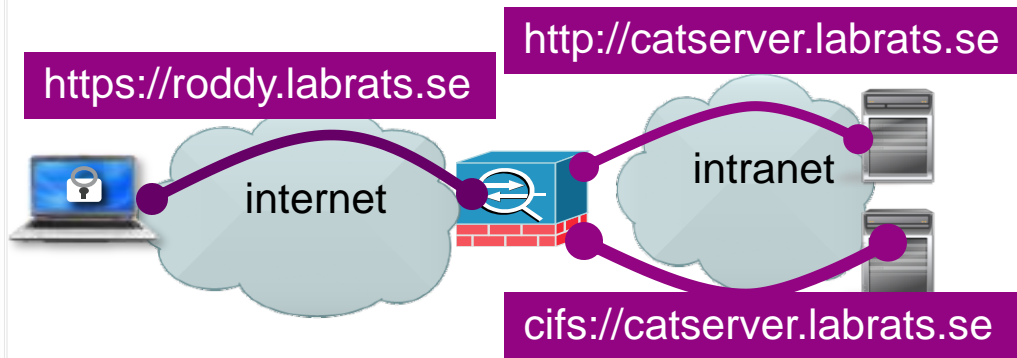
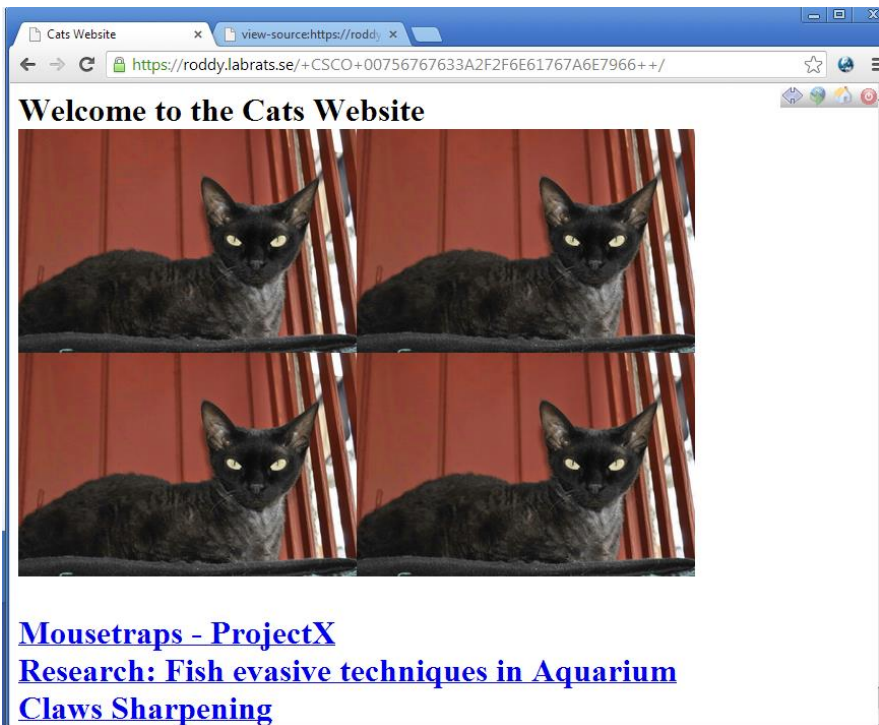
Clientless SSL Fundamentals : IPv4 and IPv6

- ASA can proxy between **IPv4** or **IPv6**
 - management/control servers (CA, AD, RADIUS) IPv4 only



HTTPS Proxy to HTTP(S), CIFS and FTP

- ASA proxies HTTPS to HTTP(S), CIFS or FTP
- ASA publishes bookmarks (collection of links to click) to access service

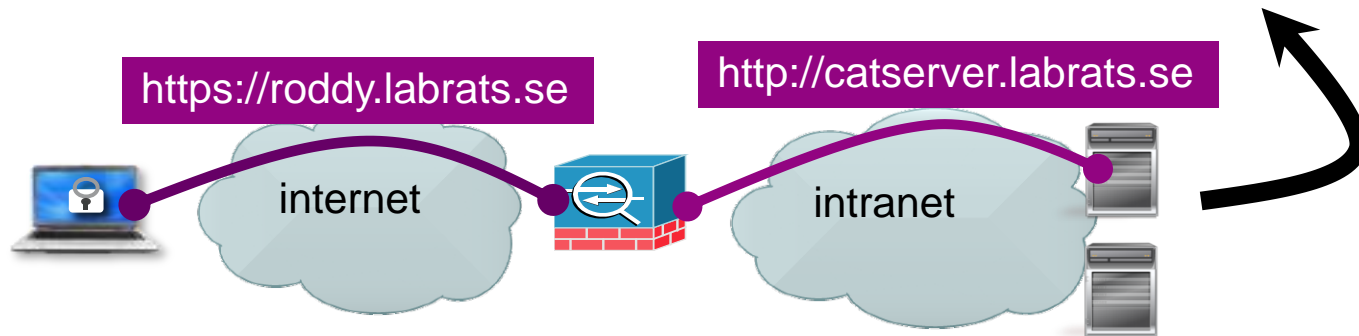


HTTP(S) Proxy and Content Transformation Engine

- ASA Content Transformation Engine Rewrites HTML, Javascript, Flash, CSS...
- Required, since internal names and IP addresses are not visible on the outside

Original HTML on Server

```
<a href="http://catserver.labrats.se/mousetraps.html">Mousetraps - ProjectX</A>  
<a href="fish.html">Research: Fish evasive techniques in Aquarium</a>
```



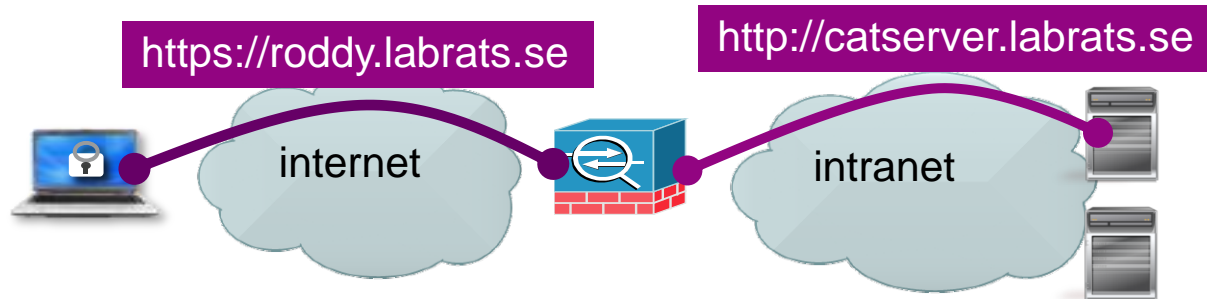
HTTP(S) Proxy and Content Transformation Engine

- ASA Content Transformation Engine Rewrites HTML, Javascript, Flash, SVG, CSS...
- Required, since internal names and IP addresses are not visible on outside

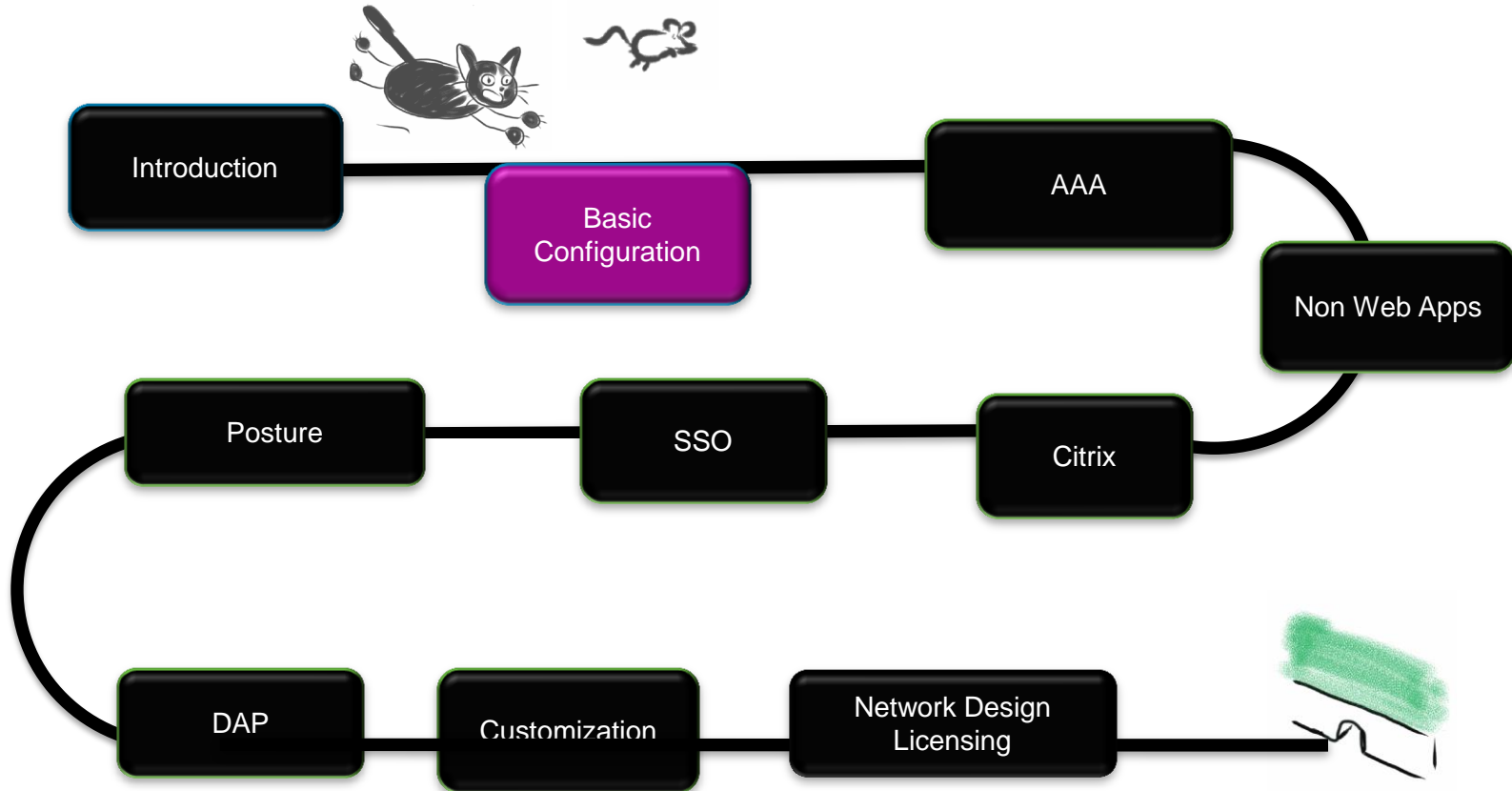
Modified HTML Rendered to Client

```
<a href="https://roddy.labrats.se/+CSCO+0E..6++/mousetraps.html" >Mousetraps - ProjectX</a>
```

```
<a href="-CSCO-3h--fish.html" >Research: Fish evasive techniques in Aquarium</a>
```

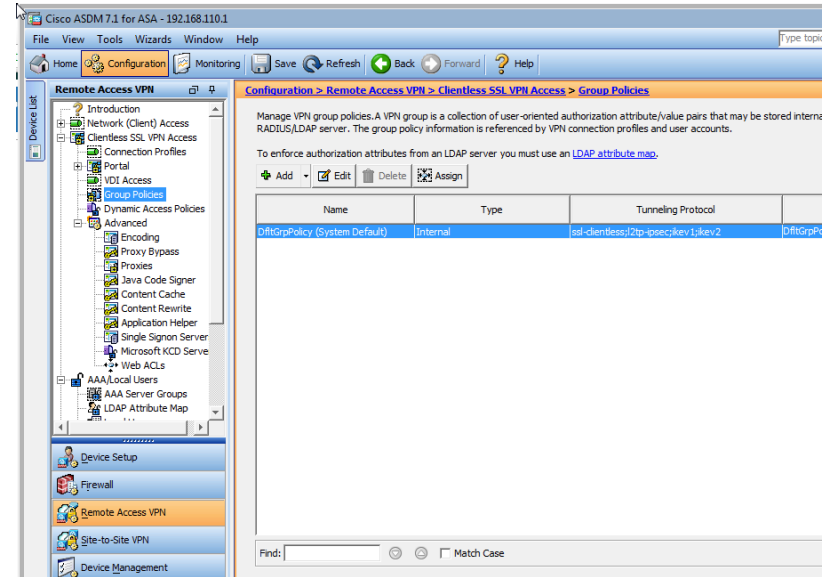


Agenda



How to configure Clientless SSL VPN

- Command Line Interface
 - Not really feasible : a lot of configuration in XML files
- ASDM
 - Easiest Option, used in this breakout
- Cisco Security Manager
 - For configuring many ASAs
 - ... but does not support 100% of features



We could use the Wizard... but Man or Mouse?

Cisco ASDM 7.1 for ASA - 192.168.110.1

File View Tools Wizards Window Help

Home Conf

Remote Access

VPN Wizards

- Startup Wizard...
- VPN Wizards
 - Site-to-site VPN Wizard...
 - AnyConnect VPN Wizard...
 - Clientless SSL VPN Wizard...
 - IPsec (IKEv1) Remote Access VPN Wizard...
- High Availability and Scalability Wizard...
- Unified Communication Wizard...
- Packet Capture Wizard...

Device List

AAA/Local Users

Host Scan Image

Secure Desktop Manager

Certificate Management

Language Localization

Load Balancing

DHCP Server

DNS

Advanced

The [ASDM Assistant](#) provides simple "How Do I" steps for configuring Clientless SSL VPN A

Important Concepts

Following are some important concepts for setting up a connection.

1. User and connection profile

As in accessing any secure web site, remote users must first login into the corporate portal page. They need to specify the name of a connection profile in the login page. This connection profile specifies how the security appliance authenticates the user.

You configure user account database in [AAA/Local Users](#).

You configure connection profile in [Connection Profiles](#).

2. Portal resource

Remote users access corporate networks, applications and other information by clicking on links shown in the portal web pages. Such links are called portal resources.

You configure portal resources in [Portal](#).

3. Access policy

Access policies control how remote users can access corporate networks. An access policy includes the following:

- Session control - how long a session can remain idle before it is closed.
- Resource control - specifies which portal resources can be accessed.
- Endpoint security - determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date.

You configure session control and resource control policies in [Dynamic Access Policies](#) or [Group Policies](#).

You configure endpoint security policies in [Secure Desktop Manager](#).

Device Setup

Firewall

Remote Access VPN



Use
Wizard!

Step-by-Step Wizard that
configures Clientless SSL
VPN

Fundamental Settings : ASA DNS Client

- ASA needs to resolve DNS
 - It is a Proxy!
- (not configured by Wizard)

The screenshot shows the ASA configuration page for the DNS Client. The breadcrumb trail is Configuration > Device Management > DNS > DNS Client. The page title is "Specify how to resolve DNS requests." Under "DNS Setup", the "Configure one DNS server group" radio button is selected. The "Primary DNS Server" field contains two IP addresses: 2001:470:dfed:41::10 and 10.1.41.10. The "Domain Name" field contains labrats.se. Under "DNS Lookup", a table shows the "outside" interface with "DNS Enabled" set to "True".

Configuration > Device Management > DNS > DNS Client

Specify how to resolve DNS requests.

DNS Setup

Configure one DNS server group Configure multiple DNS server groups

Primary DNS Server: 2001:470:dfed:41::10
10.1.41.10

Secondary Servers:

Domain Name: labrats.se

DNS Lookup

To configure DNS, enable DNS lookup on at least one interface.

Interface	DNS Enabled
infrastructure	True
outside	

ASA needs a certificate

- Certificate should be trusted by clients to avoid warnings and errors
- Import cert + keys in PKCS#12
or
- Create CSR (Certificate Signing Request), then installed signed cert from CA

The screenshot shows the 'Add Identity Certificate' dialog box within the Cisco ASA configuration interface. The breadcrumb path at the top is 'Configuration > Device Management > Certificate Management > Identity Certificates'. The dialog box has a title bar with a close button (X) and the text 'Add Identity Certificate'. The 'Trustpoint Name' field is set to 'ASDM_TrustPoint1'. There are two radio buttons: 'Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):' (unselected) and 'Add a new identity certificate:;' (selected). Under the first option, there are fields for 'Decryption Passphrase:' and 'File to Import From:' with a 'Browse...' button. Under the second option, there is a 'Key Pair:' dropdown menu set to '<Default-RSA-Key>' with 'Show...' and 'New...' buttons, and a 'Certificate Subject DN:' field set to 'CN=roddy' with a 'Select...' button. There are also two checkboxes: 'Generate self-signed certificate' (unchecked) and 'Act as local certificate authority and issue dynamic certificates to TLS-Proxy' (unchecked). At the bottom right is an 'Advanced...' button, and at the bottom center are 'Add Certificate', 'Cancel', and 'Help' buttons.

Enable Clientless SSL VPN on Interface

Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles

Access Interfaces

Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	<input checked="" type="checkbox"/>

Device Certificate ...

Specify Certificate

Specify Device Certificate

Device certificate is a digital certificate that identifies this ASA to the clients.

Device Certificate: ASDM_TrustPoint0:cn=roddy, hostname=roddy.labrats.... Manage ...

OK Cancel Help

Connection Profiles

Connection profile (tunnel group) specifies how to authenticate and more.

Group Policy - authorization

Name	Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPGROUP	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy

Group Policy

Group Policy

- The Group Policy defines Authorization, **what** the client can do, **when** and **how**
 - **Bookmark List**, Allowing URL Entry, Timeouts, Look-and-feel etc.
- DfltGrpPolicy defines default Policy, that can be overridden by more specific Policy

The screenshot shows the configuration page for Group Policies. The breadcrumb navigation is: Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies. The main title is "Edit Internal Group Policy: DfltGrpPolicy". On the left, a tree view shows "General" and "Portal" (selected), with "More Options" expanded to show "Customization", "Login Setting", "Single Signon", "VDI Access", and "Session Settings". The main content area has the following settings:

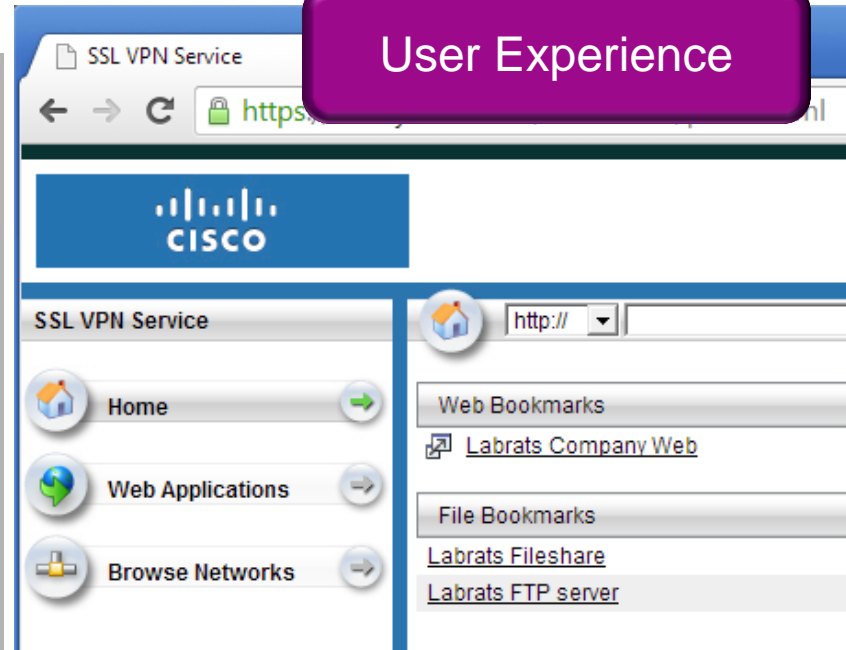
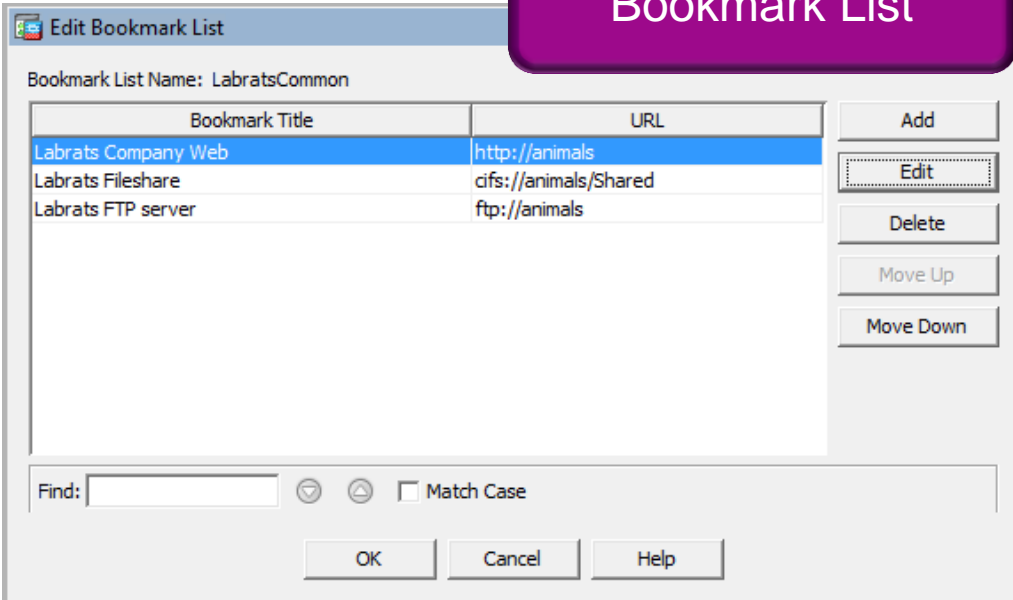
- Bookmark List: LabratsCommon (with a "Manage..." button)
- URL Entry: Enable Disable
- File Access Control section:
 - File Server Entry: Enable Disable
 - File Server Browsing: Enable Disable
 - Hidden Share Access: Enable Disable

Bookmark List

List of URLs to publish to the end user

Bookmark List

User Experience



Web ACLs

- URL based ACL
- Can be assigned per Group Policy (...or DAP, covered later)
- Limits user to certain path on specific servers

The screenshot shows the Cisco ISE configuration interface. A blue callout box highlights the 'Group Policy - cats' configuration. The 'More Options' section shows 'Web ACL' set to 'catsACL'. A purple callout box highlights the 'WebACL permitting http://webserver.labrats.se/cats/*'. Below this, the ACL Manager table shows a rule for 'catsACL' with the URL 'http://webserver.labrats.se/cats/*' and the action 'Permit'.

Group Policy - cats

Name: cats

Banner: Inherit

More Options

Tunneling Protocols: Inherit Clientless SSL VPN SSL VPN Client IPsec IKEv1 IPsec IKEv2 L2TP/IPsec

Web ACL: Inherit catsACL Manage...

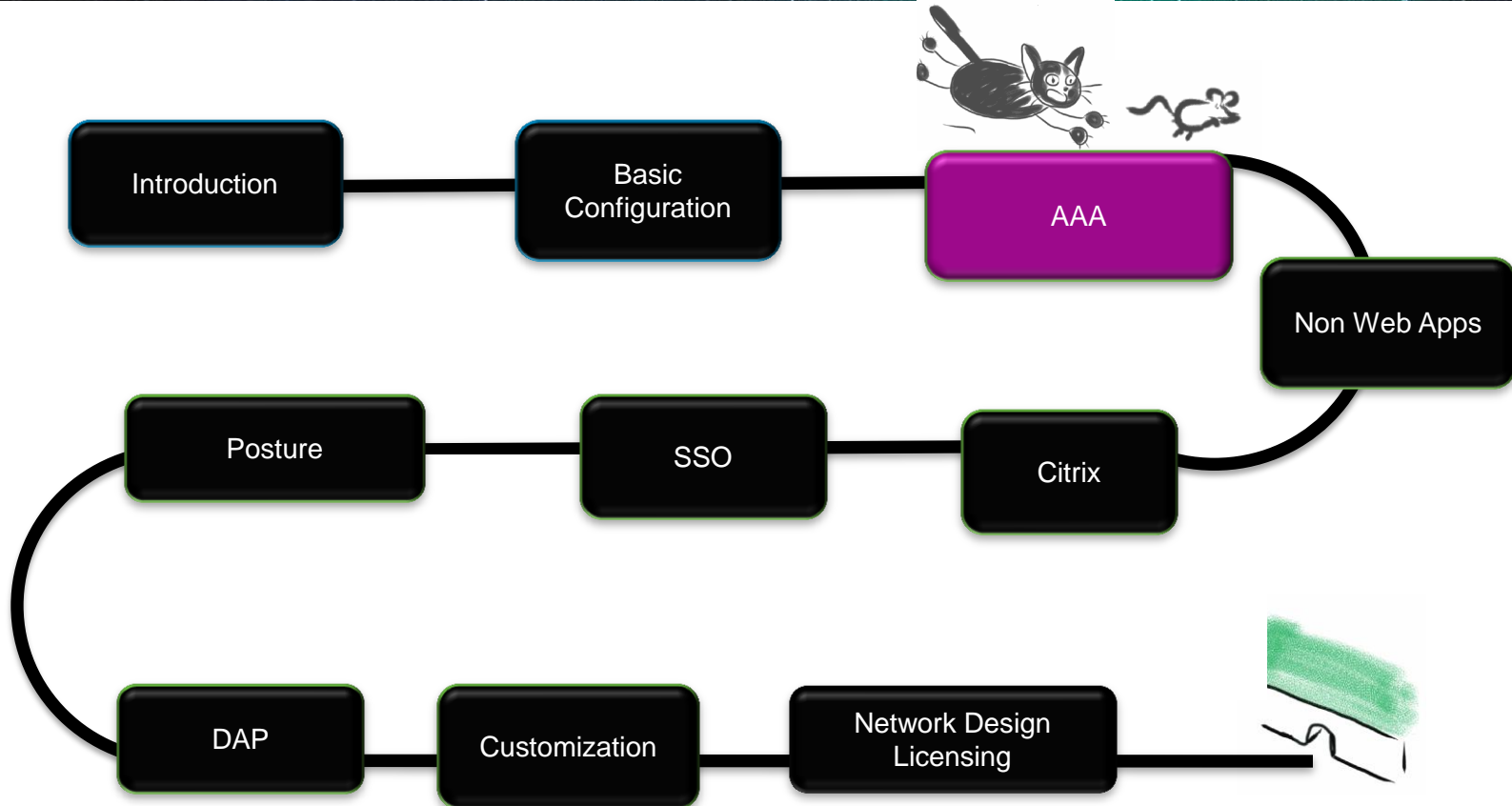
ACL Manager

No	Address	Service	URLs	Action	Time
catsACL					
1			http://webserver.labrats.se/cats/*	✓ Permit	



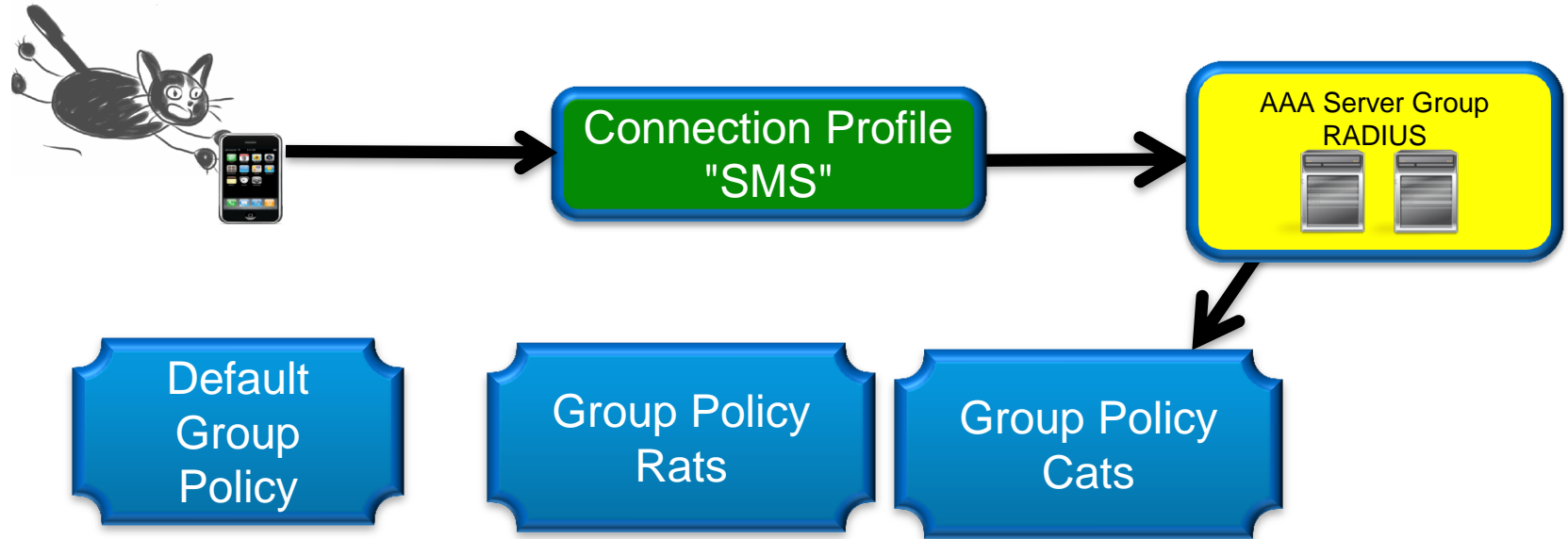
CLIENTLESS SSL VPN USER EXPERIENCE

Agenda



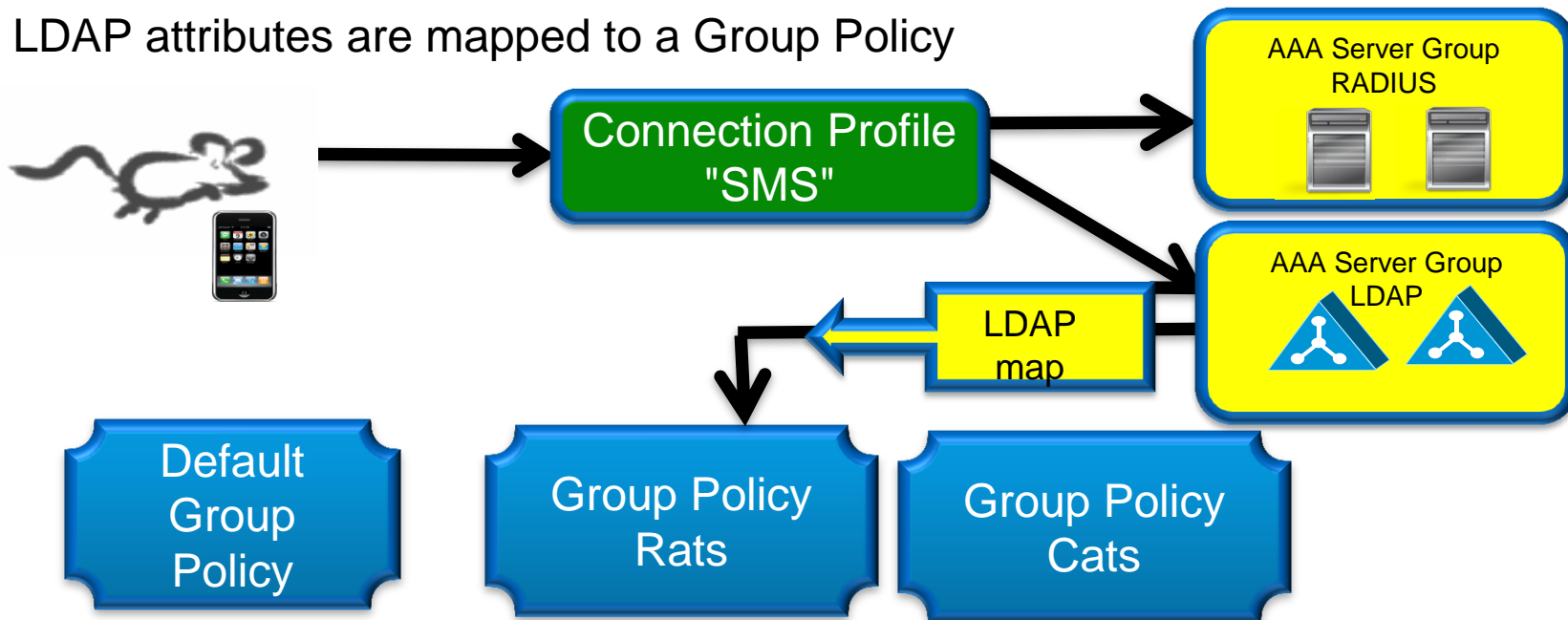
Authentication and Authorization by RADIUS

- 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 defines how to Authenticate

Edit AnyConnect Connection Profile: SMS-OTP

Connection Profile

Alias : Shown as drop-down selection to user

Method: AAA Certificate Both

AAA Server Group: SMS

AAA server group

AAA Server Group RADIUS

Group-Policy used unless overwritten by Authorization Server

Group Policy: DftGrpPolicy

Configuration Fields:

- Name: SMS-OTP
- Aliases: SMS
- Authentication Method: AAA (selected), Certificate, Both
- AAA Server Group: SMS
- Use LOCAL if Server Group fails:
- Client Address Assignment: DHCP Servers: [Empty]
- Client Address Pools: pool4-Default
- Client IPv6 Address Pools: pool6-Default
- Default Group Policy: Group Policy: DftGrpPolicy

Connection Profile defines how to Authorize

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

AAA server group used for Authorization

AAA Server Group
AD_SamAccount (LDAP)

User Selection of Connection Profile

Edit AnyConnect Connection Profile: SMS-OTP

Basic
Advanced
 General
 Client Addressing
 Authentication
 Secondary Authentication
 Authorization
 Accounting
 Group Alias/Group URL

Enable the display of Radius Reject-Message on the login screen when authentication is rejected

Enable the display of SecurId messages on the login screen

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.

+ Add [Delete] (The table is in-line editable.) ⓘ

Alias	Enabled
Login	
SMS	

Group URLs

This SSL VPN access method will automatically select the connection profile, without the need for user selection.

+ Add [Delete] (The table is in-line editable.) ⓘ

URL	Enabled
https://roddy.labrats.se/SMS	

Do not run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored.)

Alias for drop-down at login page

URL to land on this connection profile

User Selection of Connection Profile (2)

[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 authentication (EAP) over the tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

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 type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Device Certificate ...


Port Settings ...

Enable inbound VPN sessions to bypass interface access lists. Group policy and p...

Login Page Setting

Allow user to select connection profile, identified by its alias, on the login page.

Drop-Down list allows user to select login method (Connection Profile)




Login

Please enter your username and password.

GROUP:

USERNAME:

PASSWORD:



AAA Server Groups

AAA Server Group

LDAP



AAA Server Group

RADIUS



- Using the same authentication protocol and characteristics

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

AAA Server Groups

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

Same Protocol but different Groups if different characteristics

Servers in the Selected Group

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

Several Servers in a Group for redundancy

RADIUS Server Definition

Server Group: SMS

Interface Name: Infrastructure

Server Name or IP Address: mideye.labrats.se

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1645

Server Accounting Port: 1646

Retry Interval: 10 seconds

Server Secret Key:

Common Password:

ACL Netmask Convert: Standard

Microsoft CHAPv2 Capable:

SDI Messages

Message Table

OK Cancel Help

Double check port numbers on RADIUS server

Shared Secret must match with RADIUS server

LDAP Server Definition (Active Directory)

Server Group: AD_SamAccount

Interface Name: Infrastructure

Server Name or IP Address: ratbert.labrats.se

Timeout: 10 seconds

LDAP Parameters for authentication/authorization

Enable LDAP over SSL

Server Port: 636

Server Type: Microsoft

Base DN: dc=labrats,dc=se

Scope: All levels beneath the Base DN

Naming Attribute(s): sAMAccountName

Login DN: roddy@labrats.se

Login Password:

LDAP Attribute Map: ADmemberOf

LDAP over SSL

Domain is labrats.se

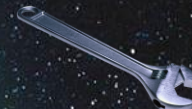
Attribute for user lookup

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 window with the following structure:

- Address bar: CN=Scratchy Cat,CN=Users,DC=labrats,DC=se
- Menu: File, Edit, View, Tools, Help
- Toolbar: Navigation and editing icons
- Filter: (objectClass=*)
- Left pane: Tree view of LDAP structure, including CN=Scratchy Cat.
- Right pane: Attribute-value table for the selected entry.

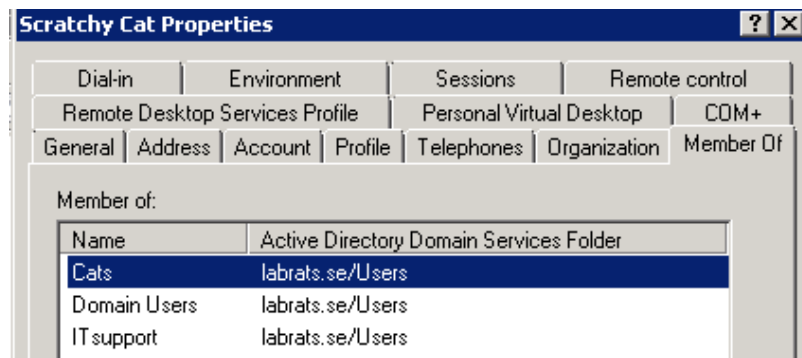
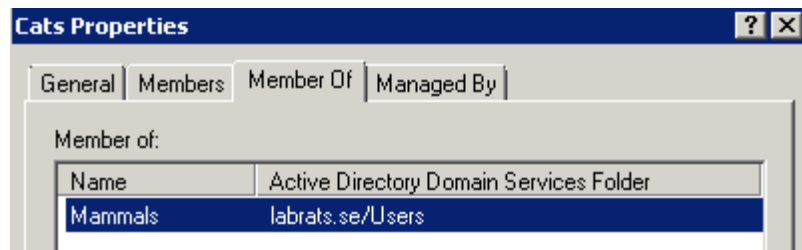
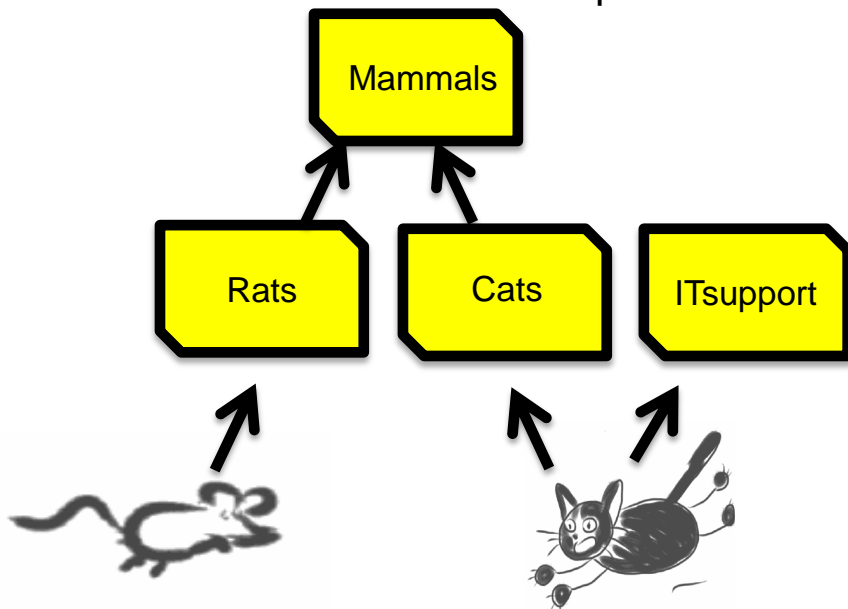
Name	Value
memberOf	CN=ITsupport,CN=Users,DC=labrats,DC=se
memberOf	CN=Cats,CN=Users,DC=labrats,DC=se
mobile	
modifyTime	
name	CN=ITsupport,CN=Users,DC=labrats,DC=se
objectCategory	CN=Cats,CN=Users,DC=labrats,DC=se
objectClass	person
objectClass	organizationalPerson
objectClass	user
objectGUID	D1 32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

Callouts in the image:

- A purple box highlights the **memberOf** attribute and its values.
- A purple box highlights the **name** attribute with the value **CN=ITsupport,CN=Users,DC=labrats,DC=se**.
- A purple box highlights the **objectCategory** attribute with the value **CN=Cats,CN=Users,DC=labrats,DC=se**.
- A purple box highlights the **sAMAccountName** attribute with the 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



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”)
- DAP (covered later) allows for more flexibility in handling “many memberOf”



LDAP map

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

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

Troubleshooting AAA server

- Test that AAA server works

Servers in the Selected Group

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

Buttons: Add, Edit, Delete, Move Up, Move Down, Test (highlighted)

Find:

LDAP Attribute:

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:

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	1	1	48

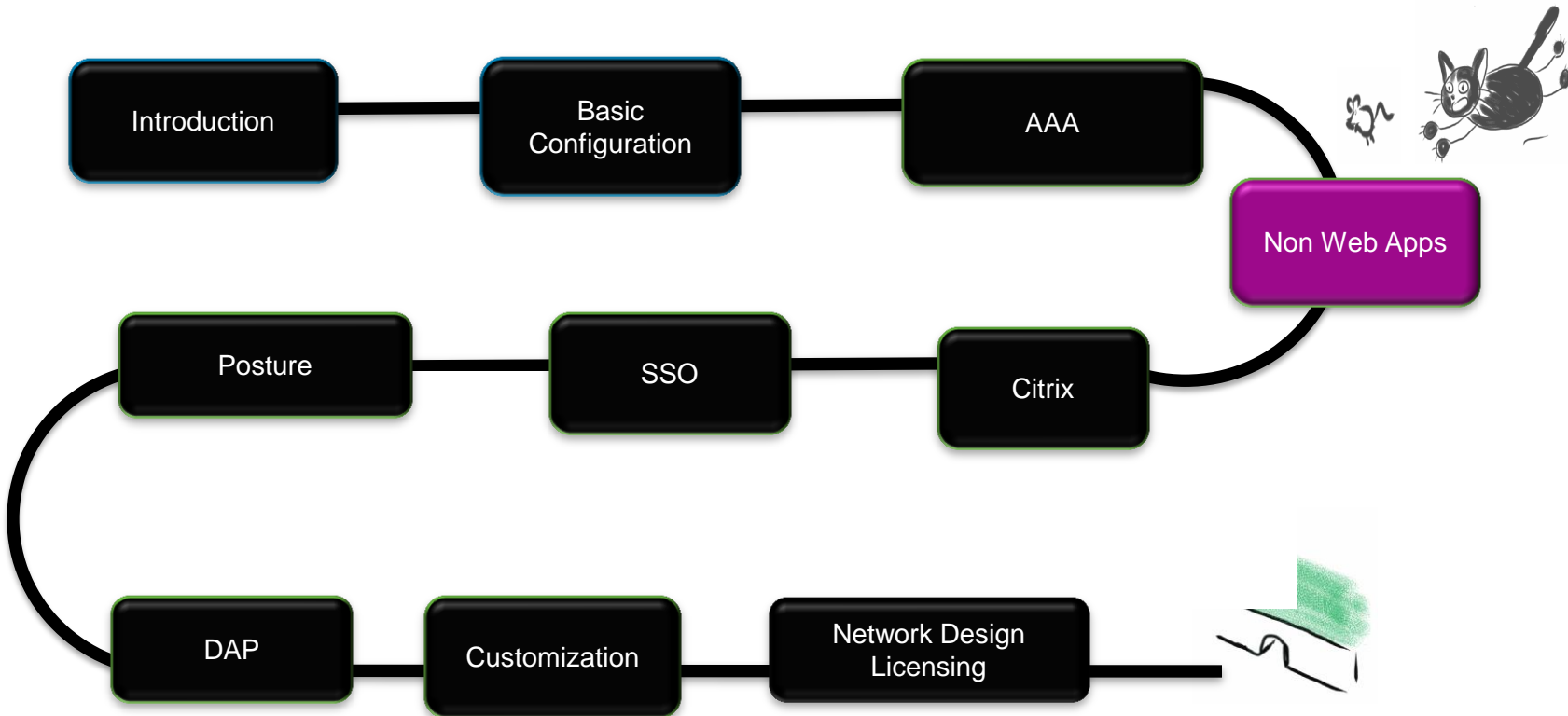
Filter By: Username

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



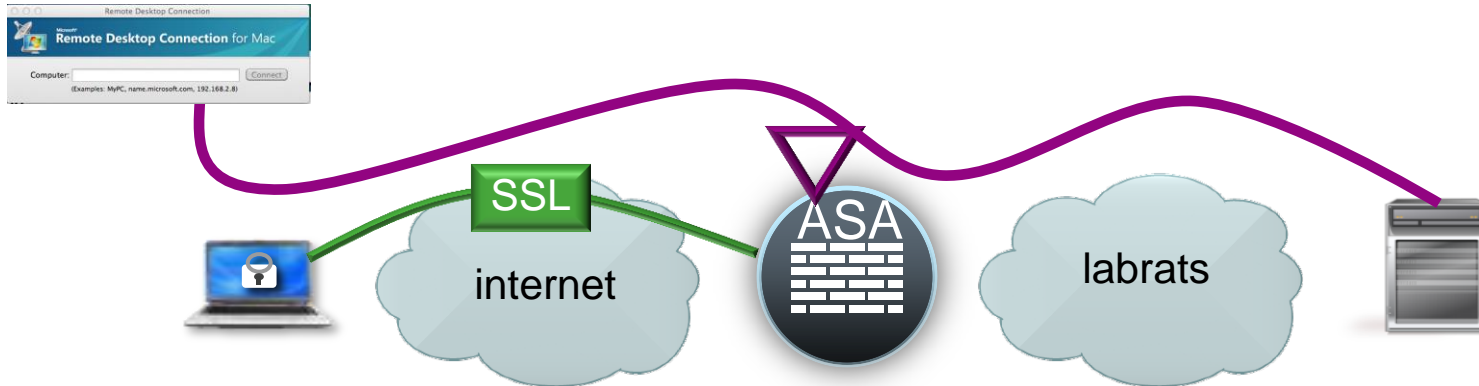
LOGIN WITH OTP USER MAPPED TO GROUP POLICY

Agenda



Smart Tunnel

- Downloads a Java (or Active-X) component that relays/tunnels application over https session
- Works for Windows and MAC (x86 and 64 bit)
- Works for TCP based applications (example : Remote Desktop)
- Does not require administrative privileges on client



Configuring Smart Tunnels







[Configuration](#) > [Remote Access VPN](#) > [Clientless SSL VPN Access](#) > [Portal](#) > [Smart Tunnels](#)

For Smart Tunnel Application List, Auto Sign-on Server List, and Networks, you can enforce them to group policy or user policy by clicking on the Assign button above the respective table.

Method to Log Off Smart Tunnel Session

- Logoff the smart-tunnel when its parent process, such as a browser, terminates
- Click on smart-tunnel logoff icon in the system tray

Smart Tunnel Application List

 Add  Edit  Delete  Assign Find:   Match Case

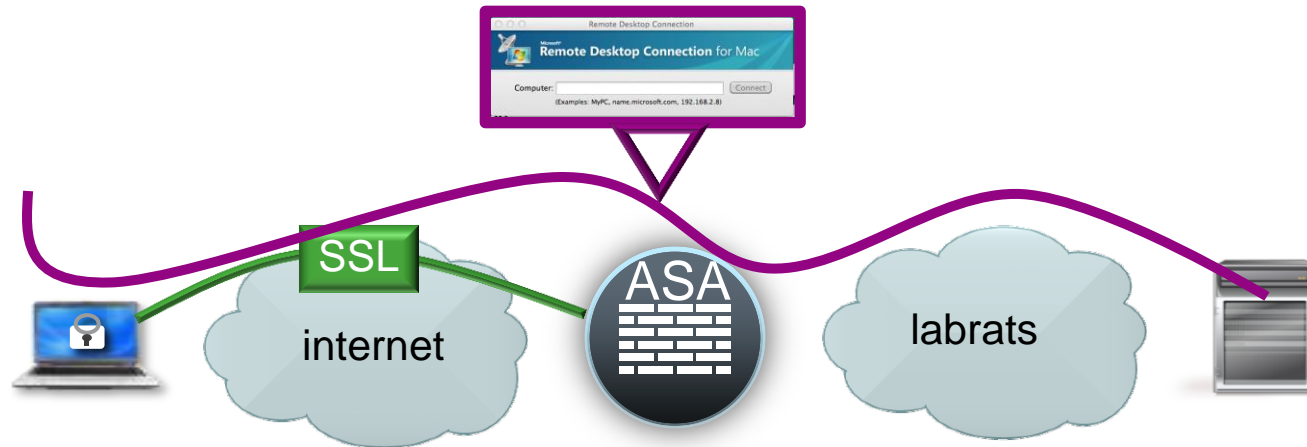
List Name	Application ID	Process Name	OS	Hash	Group Policies/User Policies Assigned to
Remote-Desktop	Remote-Desktop	mstsc.exe	Windows		DfltGrpPolicy

Process
Name

Group Policy

Plugins Deliver the Application from ASA

- Plugins are java apps downloaded from ASA to end system
 - Remote Desktop, VNC, SSH/Telnet, TN3270.... and Citrix Receiver
- Downloaded Application tunneled over SSL connection to server
- Windows and MAC OS





Download plugins from CCO

... the most difficult step.... Where do I find them?

Download Software

Download Cart (0 items) [\[-\] Feedback](#) [Help](#)

[Downloads Home](#) > [Products](#) > [Security](#) > [Firewalls](#) > [Adaptive Security Appliances \(ASA\)](#) > [Cisco ASA 5500-X Series Next-Generation Firewalls](#) > [Cisco ASA 5520 Adaptive Security Appliance](#) > [Remote Access Plugins for Adaptive Security Appliance \(ASA\)-1.1.1](#)

Cisco ASA 5520 Adaptive Security Appliance

[Expand All](#) | [Collapse All](#)

▼ All Releases
▼ 1
1.1.1
1.0.0



Release 1.1.1

File Information	Release Date ▼	Size	
SSH client plugin for ASA. ssh-plugin.130918.jar	18-SEP-2013	0.36 MB	Download Add to cart Publish
Terminal Service client plugin for ASA. rdp_09.11.2012.jar	30-OCT-2012	0.66 MB	Download Add to cart Publish
SSH client plugin for ASA. ssh-plugin.120911.jar	30-OCT-2012	0.36 MB	Download Add to cart Publish

Uploading Plugins

[Configuration](#) > [Remote Access VPN](#) > [Clientless SSL VPN Access](#) > [Portal](#) > [Client-Server Plug-ins](#)

Import plug-ins to the security appliance. A browser plug-in is a separate program that a Web browser invokes to perform a dedicated function, such as connecting a client to a server within the browser window.

 Import  Delete

Client-Server Plug-ins	Hash	Date
rdp	YRifY44c8WEw8lcMPwlzi0EZabQ=	Tue, 11 Sep 2012 23:27:14 GMT
ssh,telnet	p4/Zl8Gg4lOGtEwJfy2Sx1+4JZw=	Wed, 18 Sep 2013 17:09:28 GMT
vnc	1S6oYFbMvsosSSEHNeKnmS6o7EQ=	Tue, 18 Oct 2011 18:11:43 GMT

Import Client-Server Plug-in [X]

Plug-in Name (Protocol):

Select a file _____

Local computer

Path:

Flash file system

Path:

Remote server

Path ://

Configuring URLs for Plugins



Edit Bookmark

Bookmark Title: RDP plugin to Ratbert

URL: rdp://ratbert.labrats.se/?cscso_sso=1&domain=labrats.se

URL
rdp://ratbert.labrats.se

Single Sign On
cscso_sso=1

Domain
domain=labrats.se

The Java Problem

- Plugins and Smarttunnels require Java...
- Java Runtime Environment needs to be enabled on the client
 - Not installed by default OS installation
- **Java has a recent history of serious security issues**
- Many Enterprises disable Java
- Apple, Mozilla etc. have also disabled Java
- **No guarantee that Java will work on unmanaged remote clients**

SECURITY

Exploits no more! Firefox 26 blocks all Java plugins by default

Click-to-run activated even for latest version

By Neil McAllister, 10th December 2013

[Follow](#) 475 followers

37

[Disaster recovery protection level self-assessment](#)

The latest release of the Firefox web browser, version 26, now blocks Java software on all websites by default unless the user specifically authorizes the Java plugin to run.

RELATED STORIES

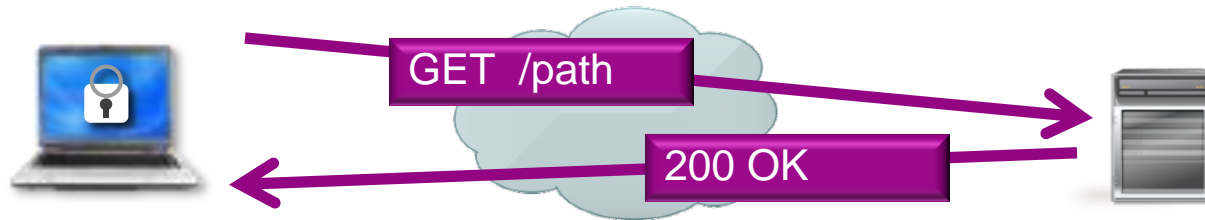
Poker ace's vanishing hotel laptop WAS infected by

The change has been a long time coming. The Mozilla Foundation had originally planned to make click-to-run the default for all versions of the Java plugin beginning with Firefox 24, but decided to delay the change after dismayed users [raised a stink](#).

http://www.theregister.co.uk/2013/12/10/firefox_26_blocks_java/

Tomorrow Starts Here : HTML5 and WebSockets

- Widely supported in different OS and Browsers
- Full-duplex and asynchronous communication between client and server
- Ideal for very dynamic user interface experience, like games and VDI



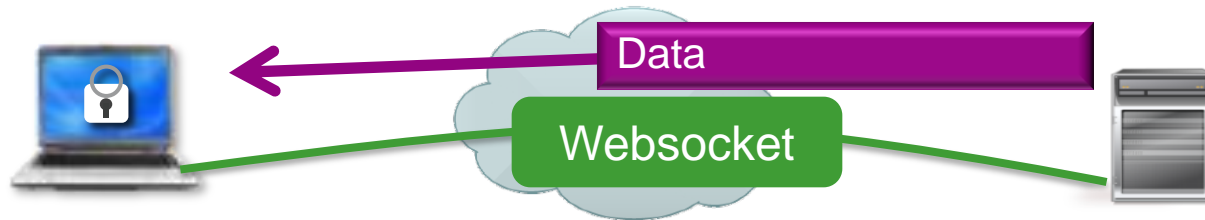
Tomorrow Starts Here : HTML5 and WebSockets

- Widely supported in different OS and Browsers
- Full-duplex and asynchronous communication between client and server
- Ideal for very dynamic user interface experience, like games and VDI



Tomorrow Starts Here : HTML5 and WebSockets

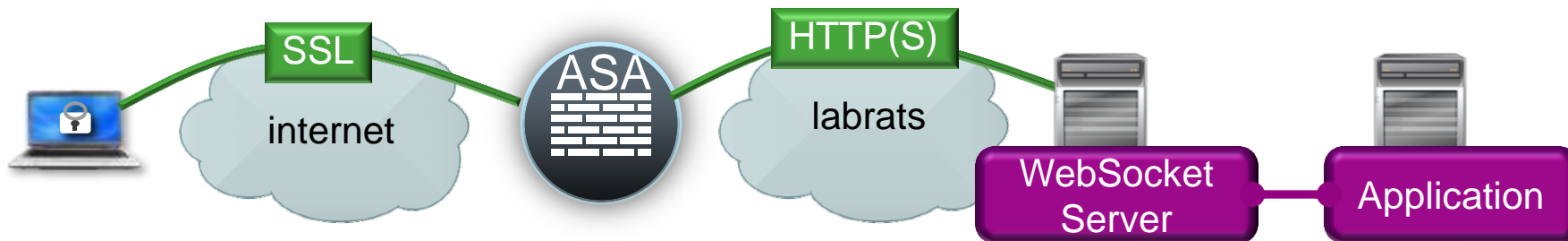
- Widely supported in different OS and Browsers
- Full-duplex and asynchronous communication between client and server
- Ideal for very dynamic user interface experience, like games and VDI



ASA Support for WebSockets

New in
9.1.4

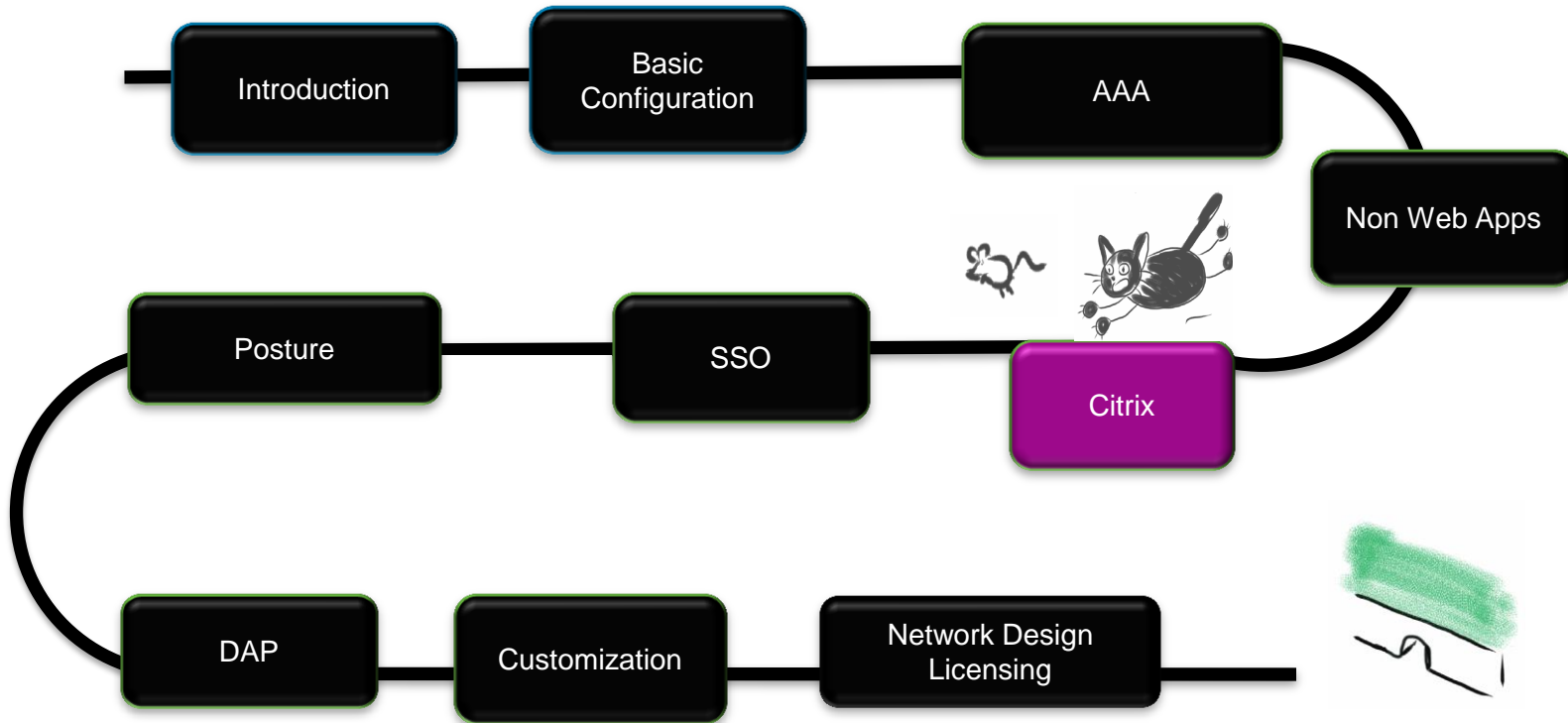
- ASA works as a proxy for websockets
- Need WebSocket Server on inside
- No changes to CLI or ASDM
- WebSocket Server communicates with end application
- No change in ASA configuration
 - Configured as normal http(s) bookmark





RDP JAVA PLUGIN HTML5 WEBSOCKETS

Agenda

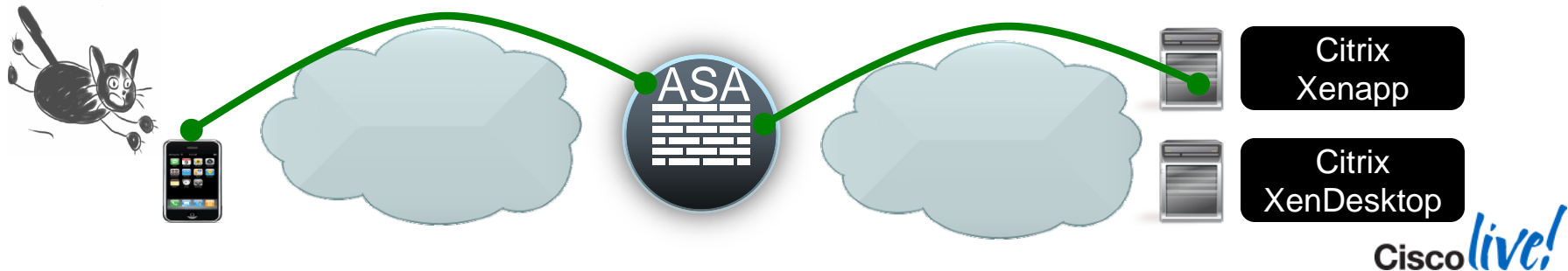


Citrix Integration

- Citrix provides application and desktop virtualization with XenApp and XenDesktop
- Both use the ICA protocol that transfers keyboard/mouse events and screen update between a client receiver and the XenApp/XenDesktop servers
- Many possible ways to integrate Cisco Remote Access with ASA and Citrix
 - Cisco AnyConnect tunneling Citrix receiver to the Citrix Servers
 - Cisco ASA as a proxy between Citrix mobile receivers and XenApp/XenDesktop
 - Citrix Plugin

Citrix Mobile Receiver

- This feature provides secure remote access for Citrix Receiver applications running on **mobile devices** to XenApp and XenDesktop
- ASA acts as proxy for ICA protocol
- **Supported Mobile Devices**
 - iPad — Citrix Receiver version 4.x or later
 - iPhone/iTouch — Citrix Receiver version 4.x or later
 - Android 2.x/3.x/4.0/4.1 — Citrix Receiver version 2.x or later



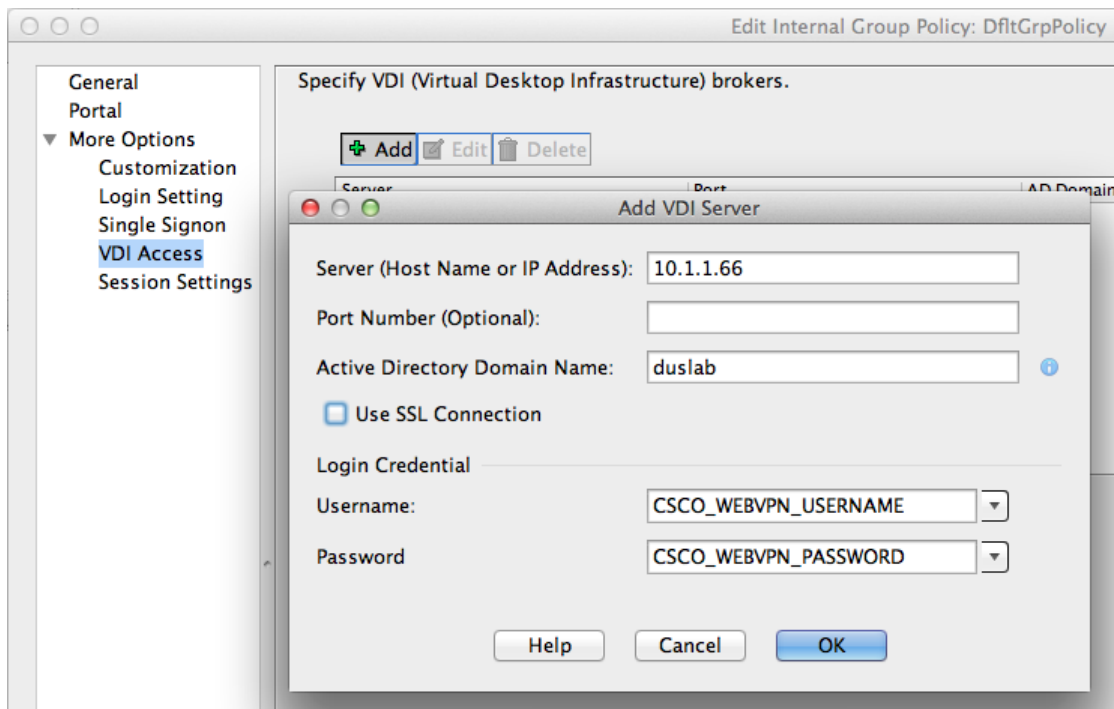
Citrix Mobile Receiver – Implementation Details

- Only default connection profile is supported
- One XenApp or XenDesktop server at a time
- Requires XML service on XenApp and XenDesktop servers
- Requires trusted identity certificate for ASA
- No support for
Client Certificates, Smart Cards, Double Authentication, Internal passwords

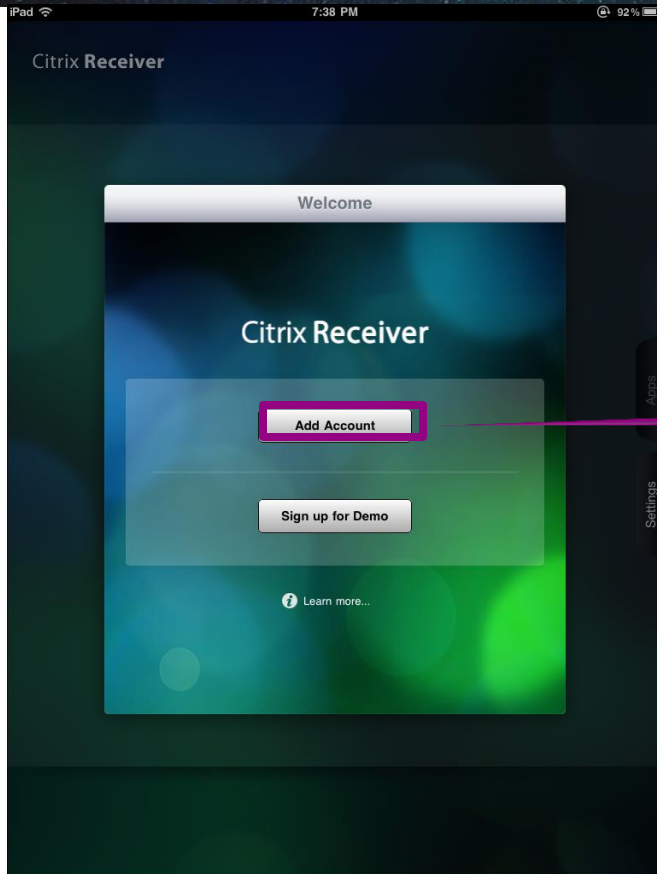


Fixed in
9.1.4

Citrix Mobile Receiver – ASA configuration

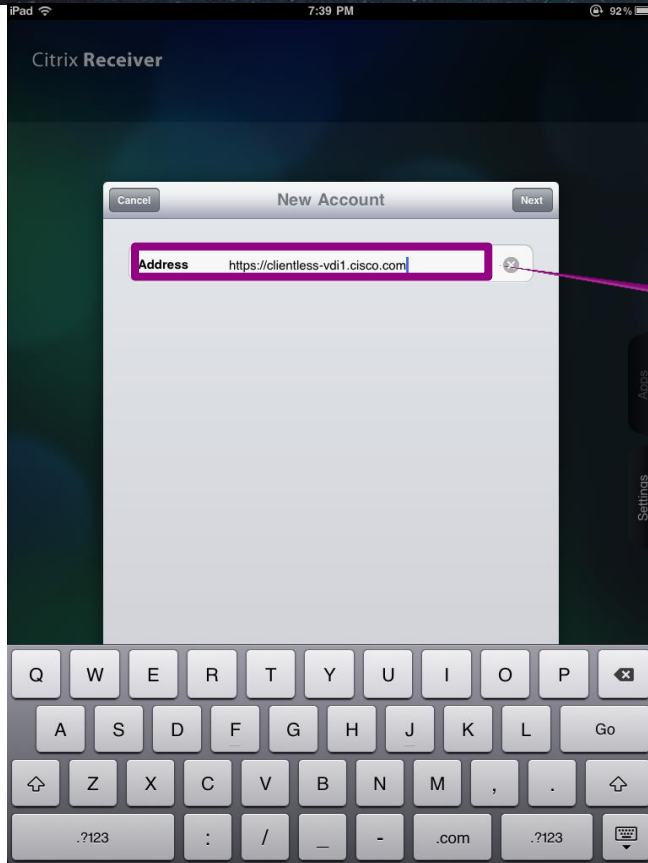


Citrix Receiver Client Configuration

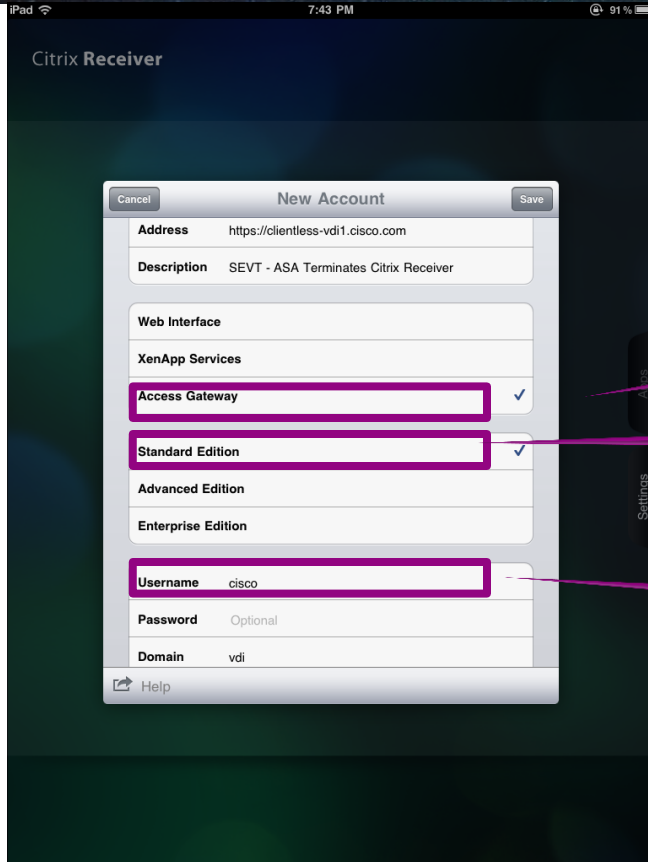


User adds an account

Citrix Receiver Client Configuration: ASA FQDN



Citrix Receiver Client Configuration (3)

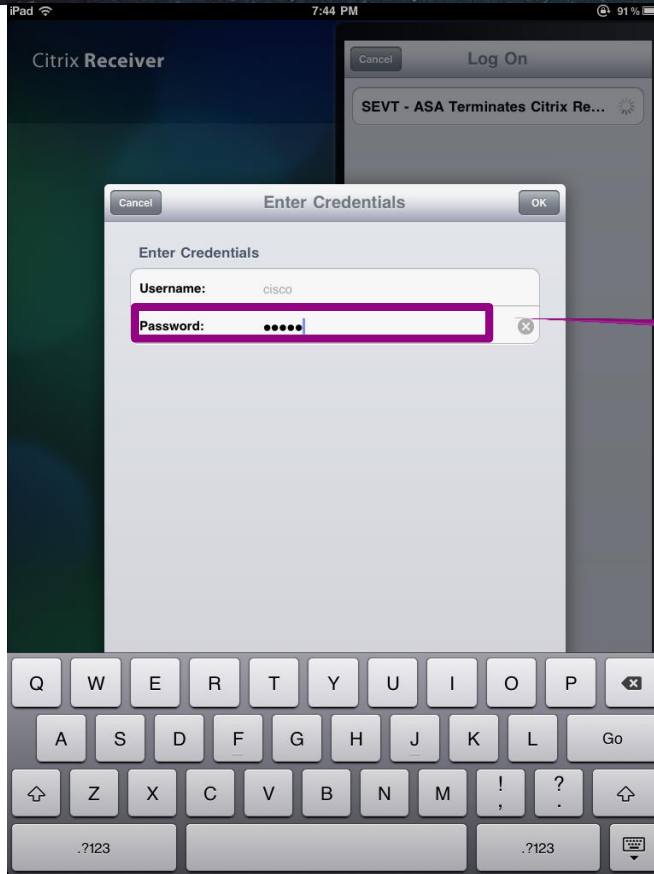


Choose Access Gateway

Choose Standard Edition

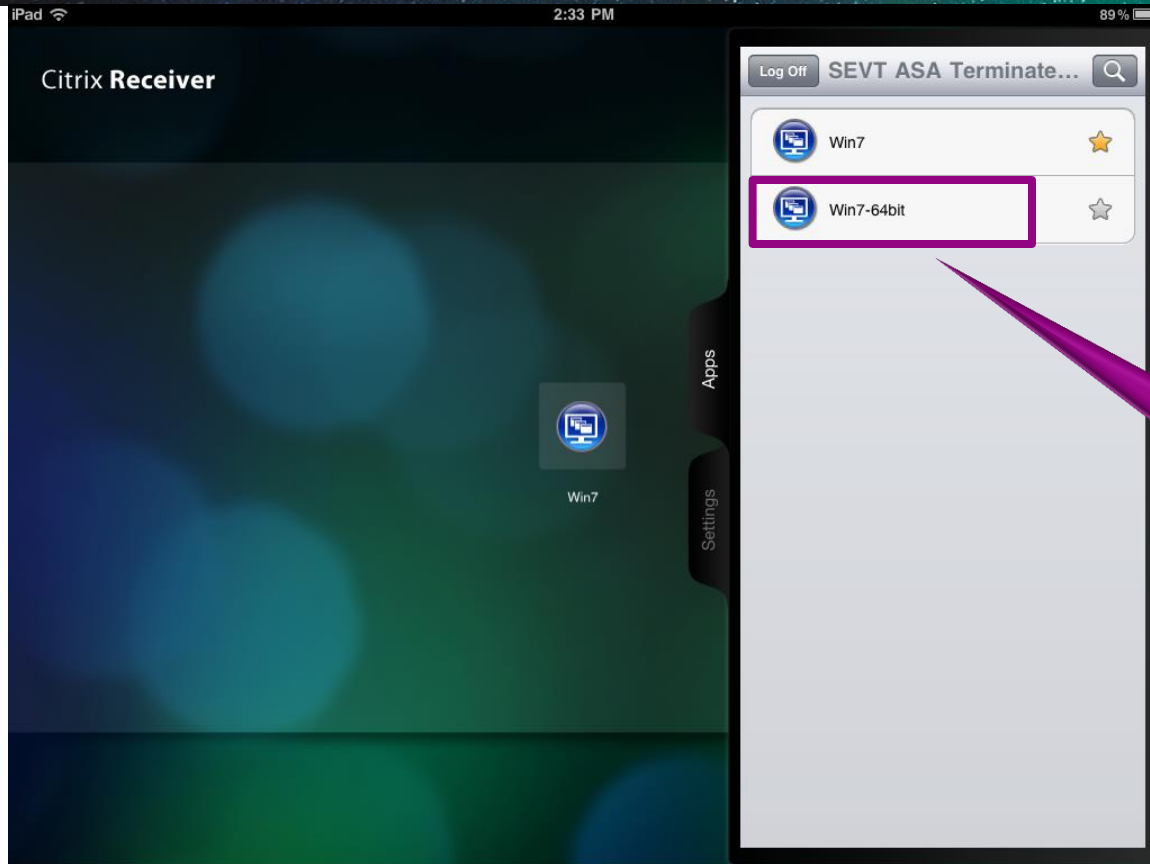
Enter Username

Connecting to ASA with Citrix Mobile Receiver



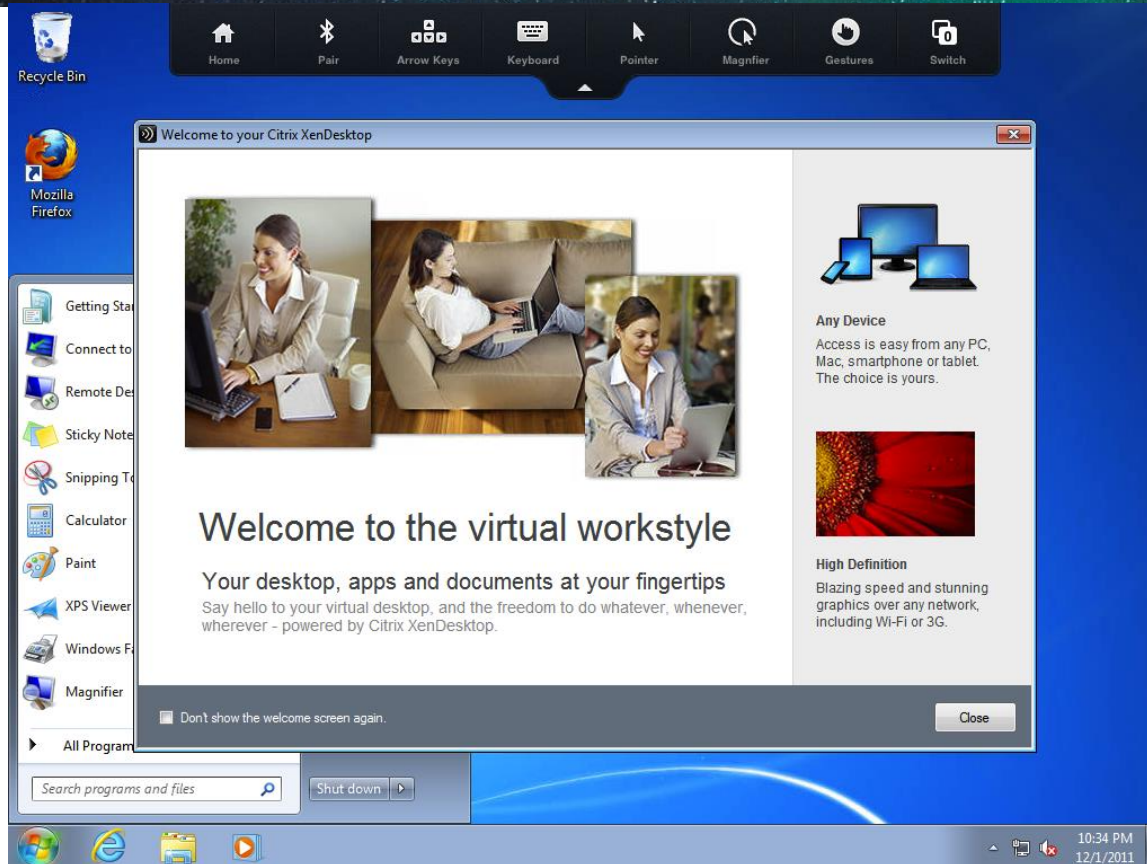
Enter Password

Every day experience

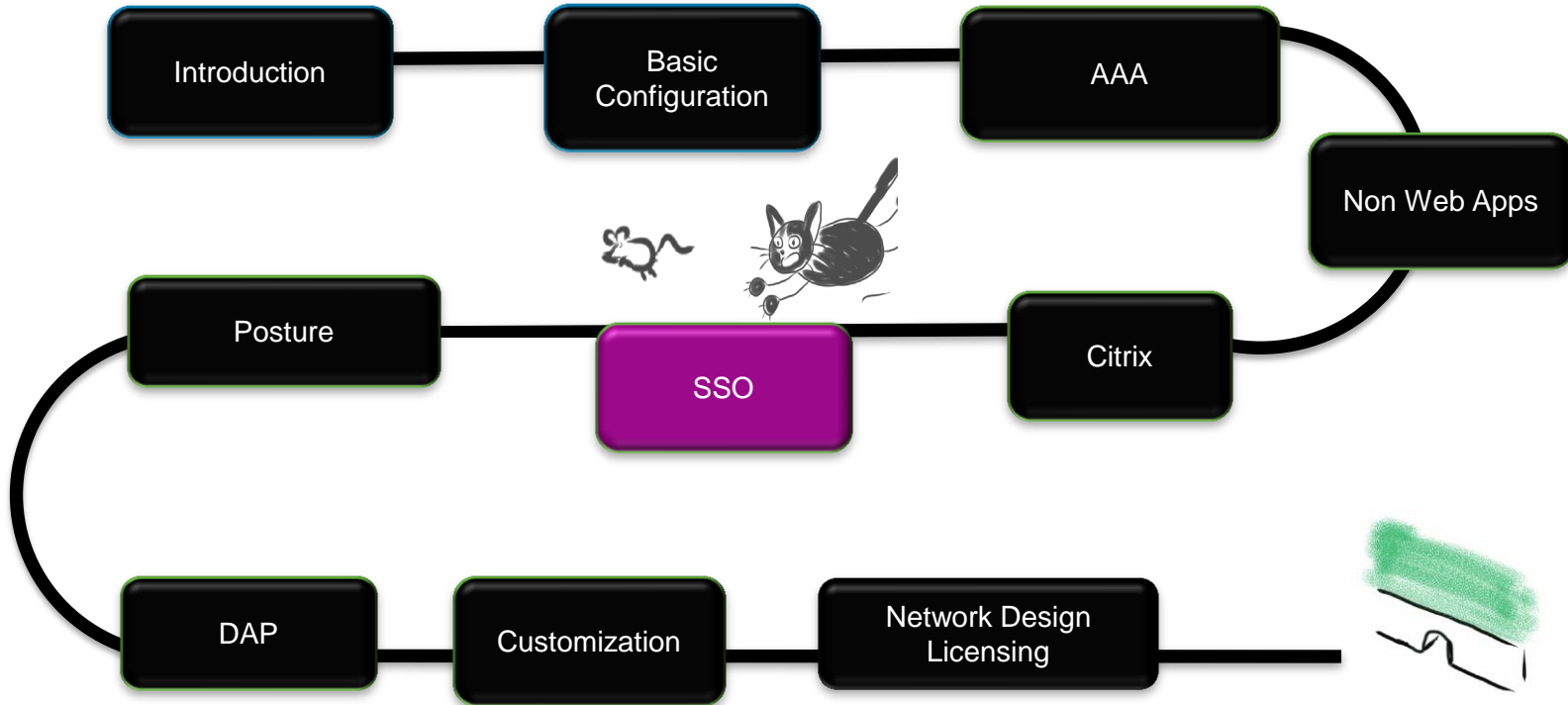


Select your Desktop

Every day experience (XenDesktop)



Agenda

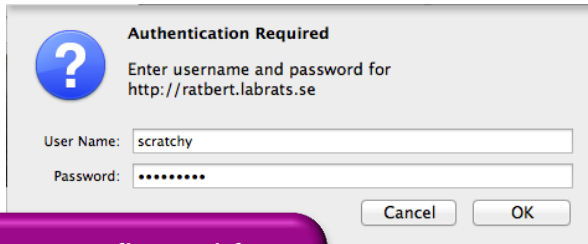


Single-Sign-On to Internal Applications

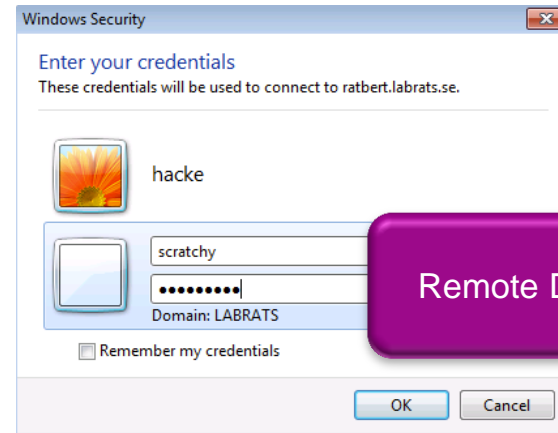
- Auto Sign-On
 - Leverages Username/Password entered by user to authenticate against ASA
- Kerberos Constrained Delegation
 - Leverages Kerberos but only works for Kerberized Applications
 - Also works if no static password given (e.g. client certificates, RSA OTP)
- External SSO Servers (SAML 1.1 only)

Auto Sign-On: Known Protocols

- Many applications, including Microsoft IIS, Microsoft Remote Desktop, can leverage protocol (HTTP, RDP, SSH) built-in authentication methods:

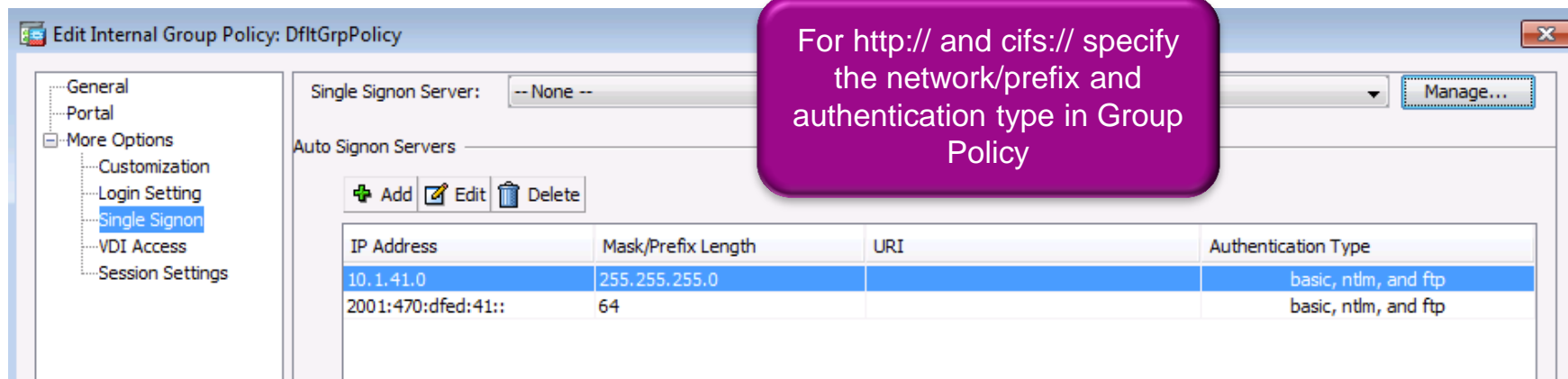


Web Server configured for authentication. Sends HTTP 401 Unauthorized back to client initiating login



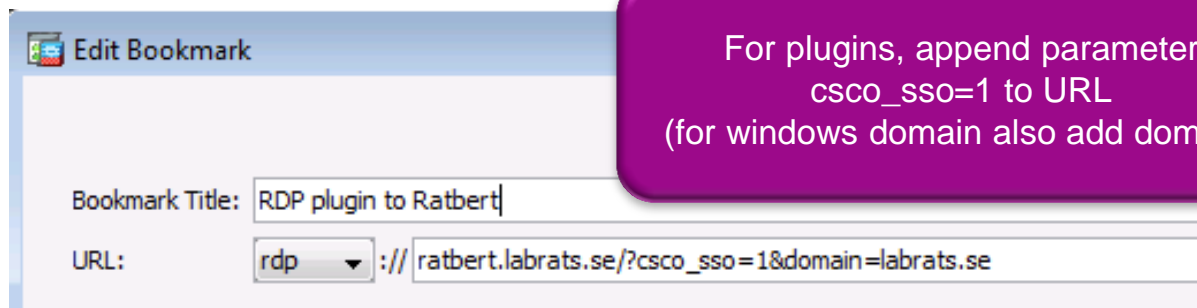
Remote Desktop Logon

Configuring Auto Sign-On for Known Protocols



For http:// and cifs:// specify the network/prefix and authentication type in Group Policy

IP Address	Mask/Prefix Length	URI	Authentication Type
10.1.41.0	255.255.255.0		basic, ntlm, and ftp
2001:470:dfed:41::	64		basic, ntlm, and ftp



For plugins, append parameter cisco_sso=1 to URL (for windows domain also add domain)

Bookmark Title: RDP plugin to Ratbert

URL: rdp :// ratbert.labrats.se/?cisco_sso=1&domain=labrats.se

Auto Sign-On : HTML Form Based Authentication

- Many custom Web Applications use their own HTML authentication forms to authenticate user.

```
<form>  
First name: <input type="text" name="uname"><br>  
Last name: <input type="password" name="passwd">  
</form>
```

- ASA must know (or be configured with) the names of the input fields
- ASA has templates for common applications
- ASA can discover input fields for other applications

Microsoft® Outlook Web App

Your session has timed out. To protect your account from unauthorized access, the connection to your mailbox is closed after a period of inactivity. Please re-enter your user name and password.

Security ([show explanation](#))

- This is a public or shared computer
- This is a private computer
- Use the light version of Outlook Web App

User name:

Password:

Sign in

Configuring Auto Sign-On : Form based Authentication

Edit Bookmark List

Bookmark List Name: LabratsCommon

Bookmark Title	URL
Labrats Company Web	http://animals

Add

Select Bookmark Type

Select an option to use for bookmark creation:

URL with GET or POST method

This is the traditional bookmark using the GET method, or the POST method with parameters.

Predefined application templates (Microsoft OWA, SharePoint, Citrix XenApp/XenDesktop, Lotus Domino)

This option simplifies bookmark creation with users selecting a predefined ASDM template that contains the pre-filled necessary values for certain well-defined applications like Microsoft OWA 2010 and Citrix XenApp.

HTML form auto-submit

This option lets you create bookmark for any complex auto sign-on application. It will require two steps:

- 1- Define the bookmark with some basic initial data and without the post parameters. Save and assign the bookmark to use in a group policy or user.
- 2- Edit the bookmark in ASDM again. Use the capture function to capture the SSL VPN parameters and edit them in the bookmark.

OK Cancel Help

Predefined Templates for Microsoft OWA, Sharepoint, Citrix XenApp/XenDesktop, Lotus Domino

Auto Submit uses capture function to “learn” the input fields

Configuring Auto Sign-On: Form based Authentication

Application Parameters ⬆

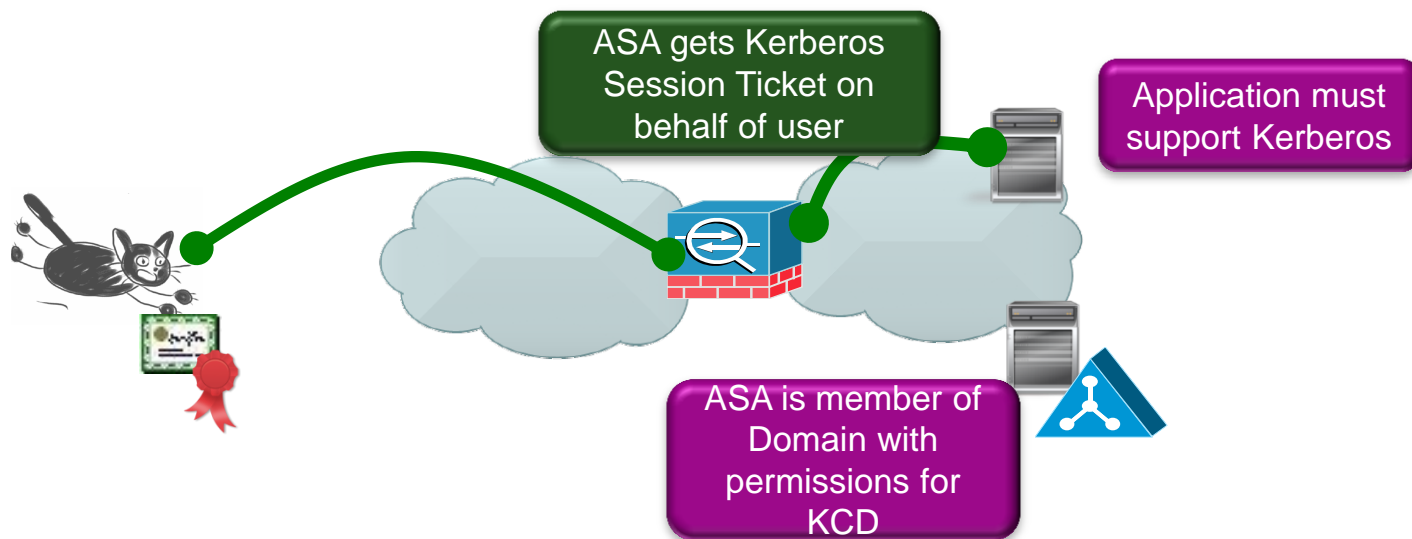
Configure auto sign-on parameters for Microsoft Outlook Web Access 2010

Protocol:	<input type="text" value="https"/>	<input type="button" value="Select Variable"/>
Host Name:	<input type="text" value="owa.labrats.se"/>	
Port Number:	<input type="text" value="443"/>	
URL Path Appendix:	<input type="text" value="/owa"/>	
User Name:	<input type="text" value="CSCO_WEBVPN_USERNAME"/>	<input type="button" value="Select Variable"/>
Password:	<input type="text" value="CSCO_WEBVPN_PASSWORD"/>	<input type="button" value="Select Variable"/>

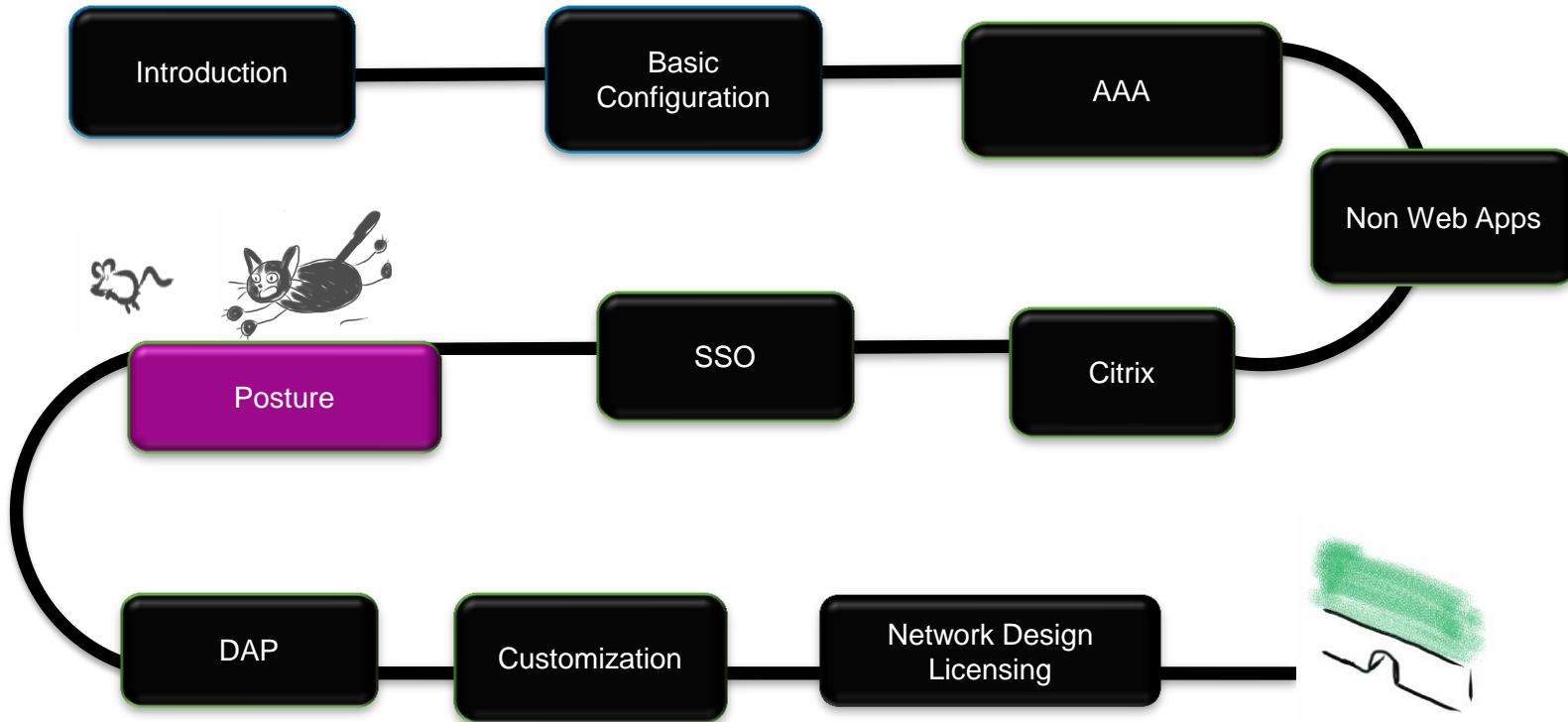
Change for
CSCO_WEBVPN_INTERNAL_PASSWORD
If necessary

Kerberos Constrained Delegation - KCD

- Allows for SSO when ASA has no access to the user's AD password
 - Client certificates
 - OTP systems that does not prompt for AD password
- Require support by application (i.e Microsoft IIS)

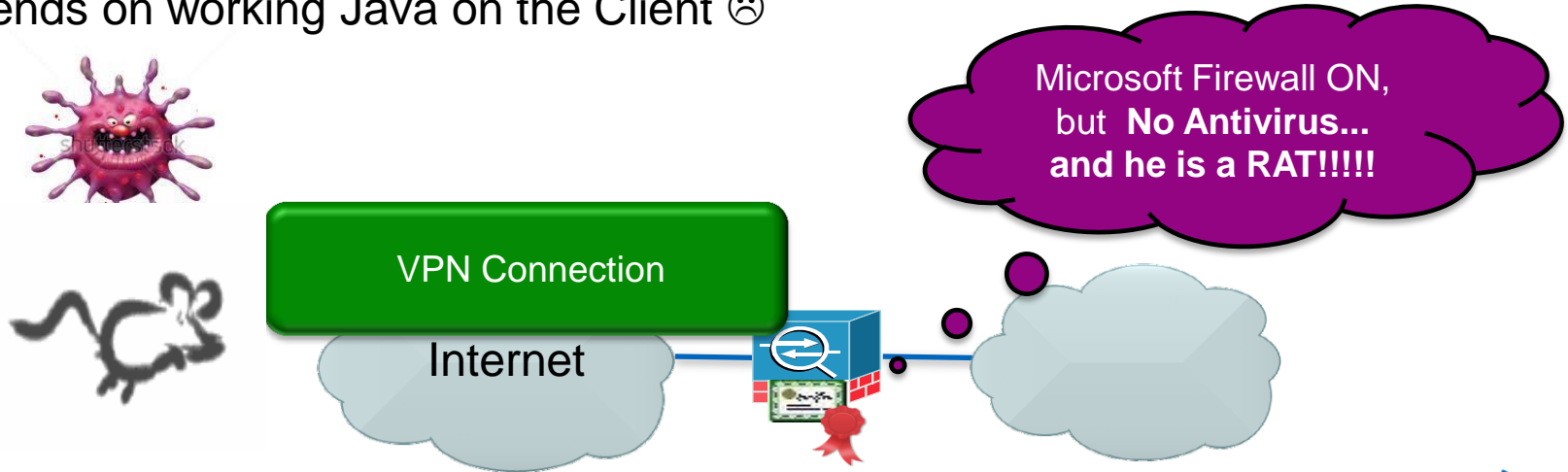


Agenda

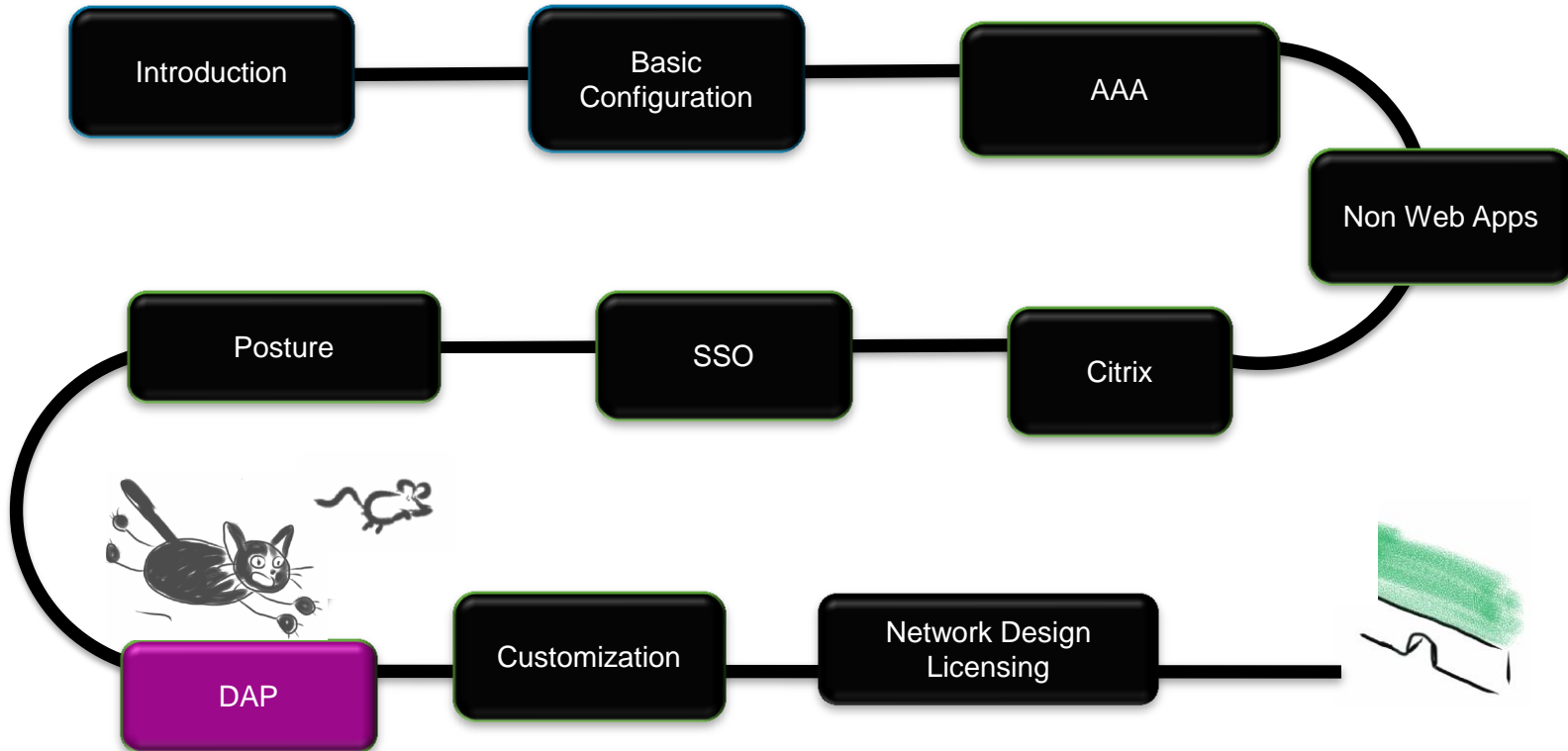


Posture : Do the Clients Meet Requirements?

- 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
- Depends on working Java on the Client ☹️

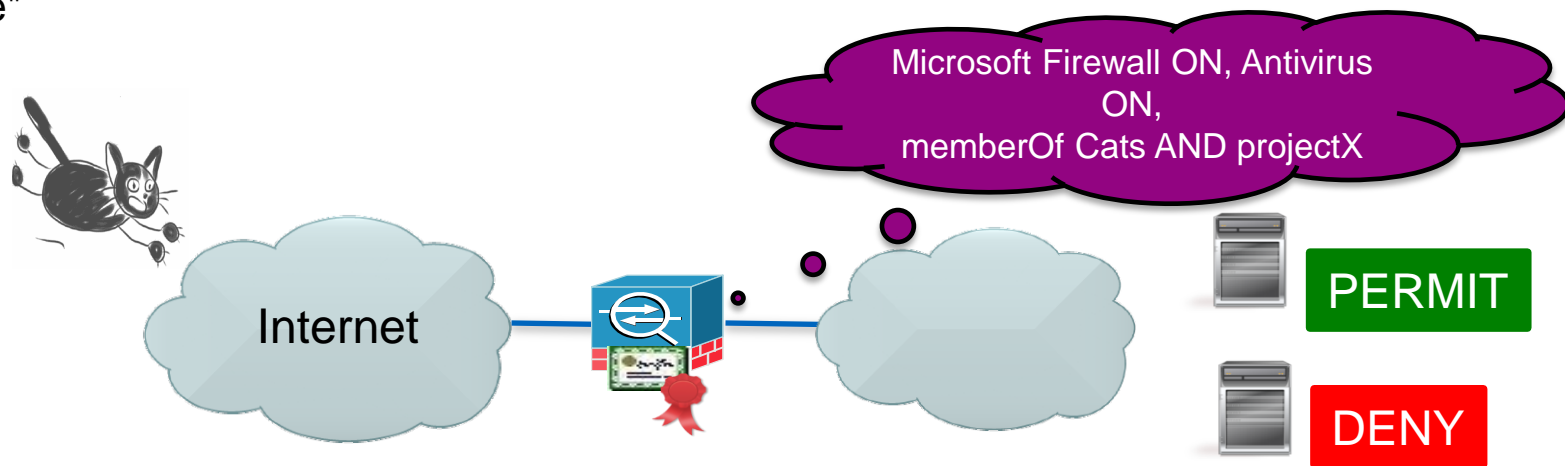


Agenda

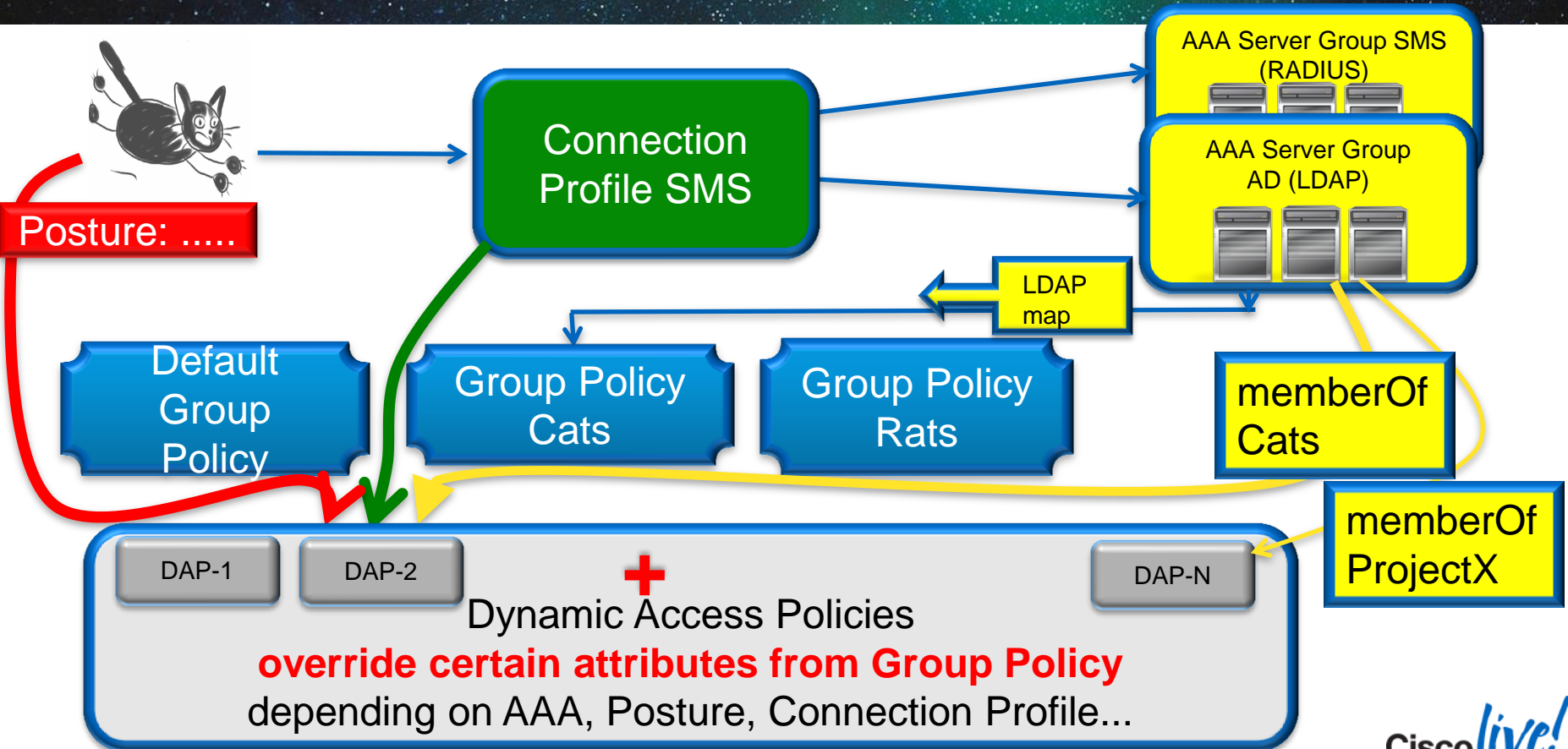


Dynamic Access Policies (DAP) : Granular Access Control

- DAP allows granular access 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

Policy Name:

Description: ACL Priority:

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
disco.tunnelgroup	= SMS-OTP
ldap.memberOf	= Cats
ldap.memberOf	= ProjectX

and the following endpoint attributes are satisfied.

Endpoint ID	Name/Operation/Value
av.Clam_AV	description = ClamAV lastupdate < 259200 activescan = ok

Advanced

Access/Authorization Policy

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

Bookmarks

projectX-Bookmark

If member of Cats and ProjectX logged on with OTP

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

Bookmarklist and WebACL

Default DAP (DfltAccessPolicy)

[Configuration](#) > [Remote Access VPN](#) > [Clientless SSL VPN Access](#) > [Dynamic Access Policies](#)

ACL Priority	Name	Webtype ACL List	Description
100	IT Support	ITsupport	IT Support with Clean PCs
90	Cats Project X	projectX-WebACL	Allow Accessto Project X t...
70	Rats	rats-WebACL	Access from AD group Rats
-	DfltAccessPolicy		

Condition

ITSupport w clean PC

Cats+ProjectX w clean PC

Rats

Bookmark + WebACL

RDP to WebServers

ProjectX WebSite

Rats WebSite

If no DAP matches
then
DfltAccessPolicy
Applies

DfltAccessPolicy

Action=
Terminate

DAP Grows On You! (DAP accumulates)

[Configuration](#) > [Remote Access VPN](#) > [Clientless SSL VPN Access](#) > [Dynamic Access Policies](#)

ACL Priority	Name	Webtype ACL List	Description
100	IT Support	ITsupport	IT Support with Clean PCs
90	Cats Project X	projectX-WebACL	Allow Accessto Project X t...
70	Rats	rats-WebACL	Access from AD group Rats
-	DfltAccessPolicy		

Condition

ITSupport w clean PC

Cats+Project X w clean PC

Rats

Bookmark + WebACL

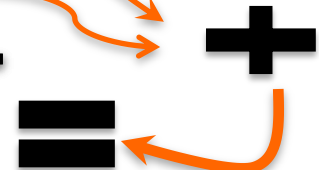
RDP to Webservers

ProjectX WebSite

Rats WebSite

RDP to everything
Rats Website

Matching
Several conditions
Accumulates
Access Rights

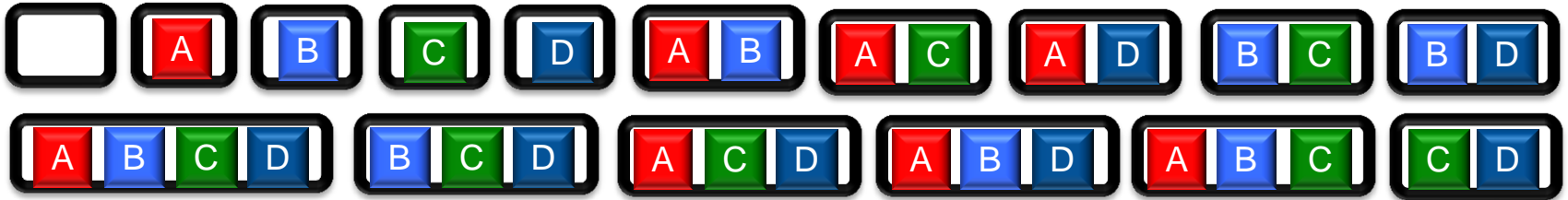


Cisco *live!*

The Power of DAP

- Very flexible mapping to multiple "memberOf"

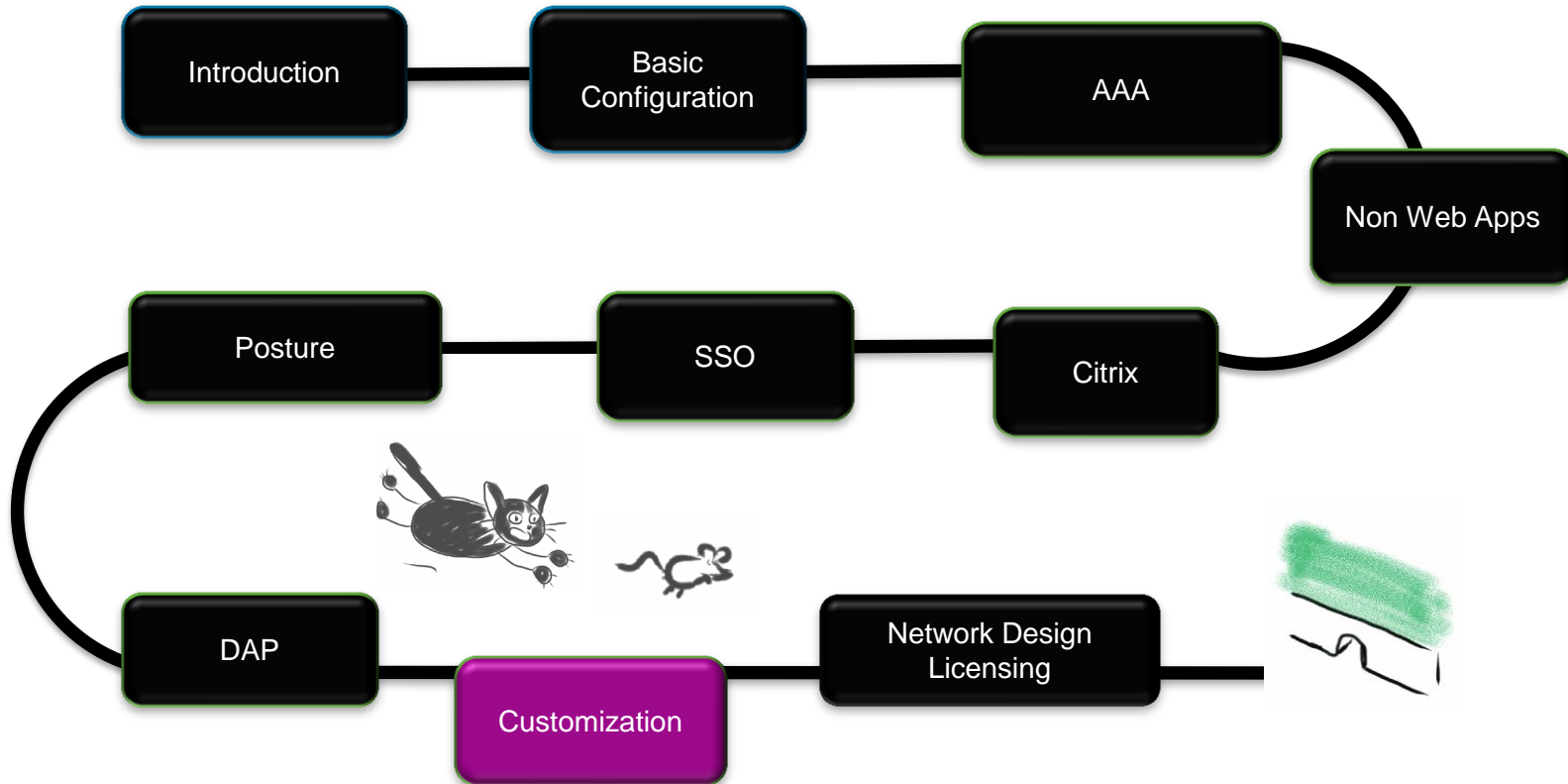
- Example : 4 groups in Directory **A** **B** **C** **D**
- A user may be a member of 0 to 4 groups : 16 combinations (2^n)



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

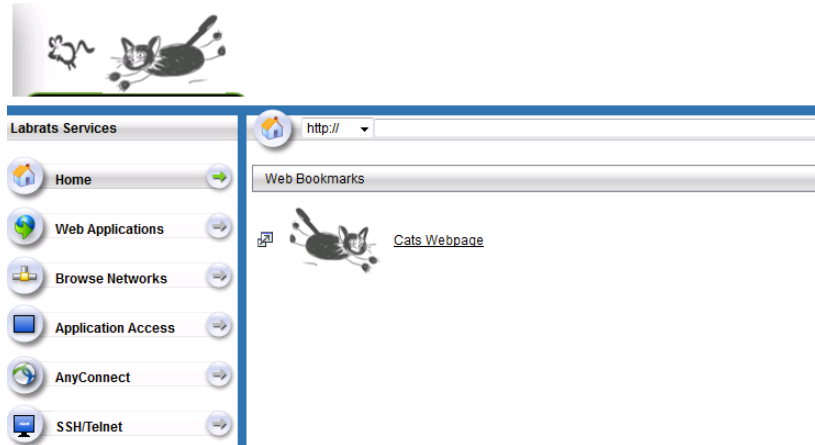
Condition (memberOf)	BookmarkList	WebACL
A	BookmarkList-A	WebACL-A
B	BookmarkList-B	WebACL-B
C	BookmarkList-C	WebACL-C
D	BookmarkList-D	WebACL-D

Agenda



Customizing the Web Portal

- Login Portal, Portal and Logoff Portal can be completely customized
- Images, Icons, Text, Font, Background Colors...
- Full Customization with HTML and Javascript
- Possible with different customizations per Connection Profile and Group Policy
- Possible to include external web page in portal



Configuring Customization (1)

[Configuration](#) > [Remote Access VPN](#) > [Clientless SSL VPN Access](#) > [Portal](#) > [Customization](#)

Edit Customization Object

Customization Object Name:

Connection Profiles

Use this customization object in existing SSL VPN connection profiles.
(The table is in-line editable.) ⓘ

Connection Profile	Use
DefaultRAGroup	<input checked="" type="checkbox"/>
DefaultWEBVPNGroup	<input checked="" type="checkbox"/>
SMS-OTP	<input checked="" type="checkbox"/>
ADpassword	<input checked="" type="checkbox"/>

Group Policies

Use this customization object in existing SSL VPN group policies.
(The table is in-line editable.) ⓘ

Group Policy	Use
cats	<input checked="" type="checkbox"/>
rats	<input checked="" type="checkbox"/>
DfltGrpPolicy	<input checked="" type="checkbox"/>

Navigation tree:

- General
- Logon Page
 - Title Panel
 - Language
 - Logon Form
 - Logon Form Fields Order
 - Informational Panel
 - Copyright Panel
- Portal Page
 - Title Panel
 - Toolbar
 - Applications
 - Custom Panes
 - Home Page
 - Timeout Alerts
- Logout Page
- External Portal Page

Specify Connection Profiles where to apply this customization

Specify Group Policies where to apply this customization

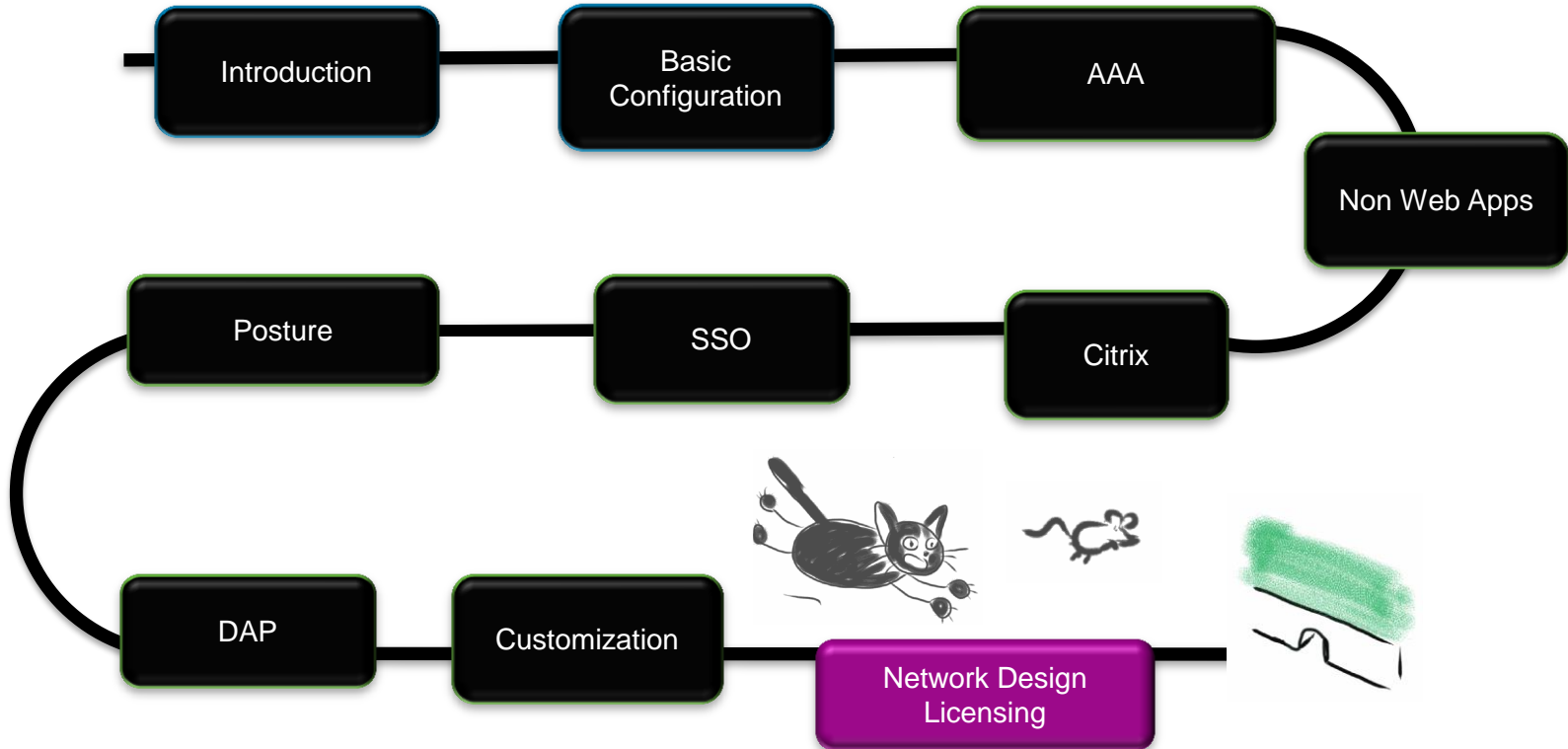
Configure Customization (2)

The screenshot shows a window titled "Edit Customization Object" with a tree view on the left and configuration options on the right. The tree view includes "General", "Logon Page", "Portal Page", and "External Portal Page". Under "Portal Page", "Title Panel" is selected. The configuration options on the right include:

- Display title panel
- Text: Labrats Services
- Logo Image: /+CSCOU+/labrats.png (with a "Manage..." button)
- Style section:
 - Font Weight: Normal
 - Font Size: 150%
 - Font Color: (dark red color swatch)
 - Background Color: (white color swatch)
- Use gradient
- Style (CSS): (empty text box)

* Style(CSS) will take precedence over the user-selected style including the default style.

Agenda



Clientless SSL VPN Platforms and Performance

- Performance more related to number of simultaneous users and transactions per second than throughput
- Figures below are **maximum**

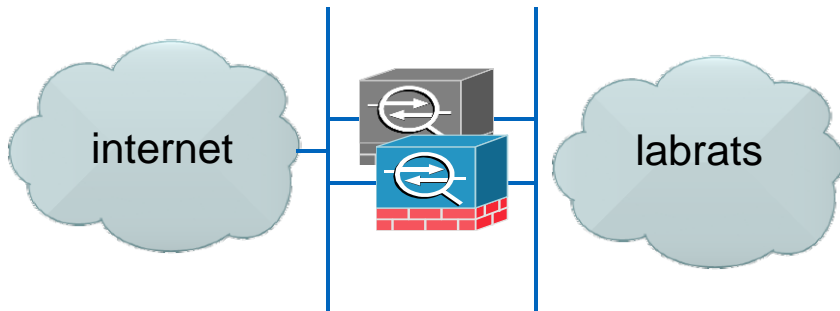
Platform	Max Users
ASA 5585-X (SSP20,SSP40,SSP60)	10.000
ASA5585-X (SSP10)	5.000
ASA5555-X	5.000
ASA5545-X	2.500
ASA5525-X	750
ASA5515-X, ASA5512-X	250
ASA5505	25

Cisco SSL VPN Premium Licenses

- Required for Clientless SSL VPN (and AnyConnect with premium features like hostscan, Always-On)
- Eternal license (one-off purchase)
- Counts simultaneously connected endpoints
- **Cannot** be combined with AnyConnect Essentials on same ASA

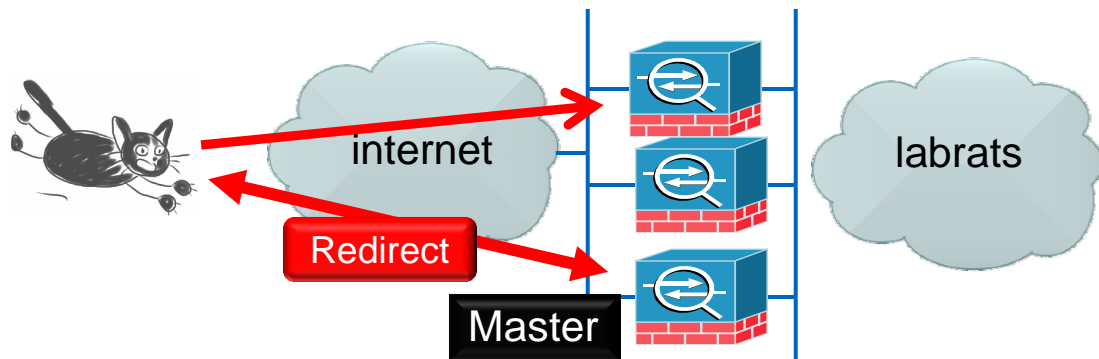
Clientless SSL VPN with Failover

- SSL VPN supports failover between 2 ASAs in Active-Standby
- Since ASA 8.3, Licenses **only required on primary**
- Stateful failover (sessions are synchronized)
 - Exceptions :Smart Tunnels, Plugins, all IPv6 Clientless, Citrix
- Configuration data is synchronized
 - CLI, DAP, Certificates with public and private keys



Clientless SSL VPN with RA VPN Clustering

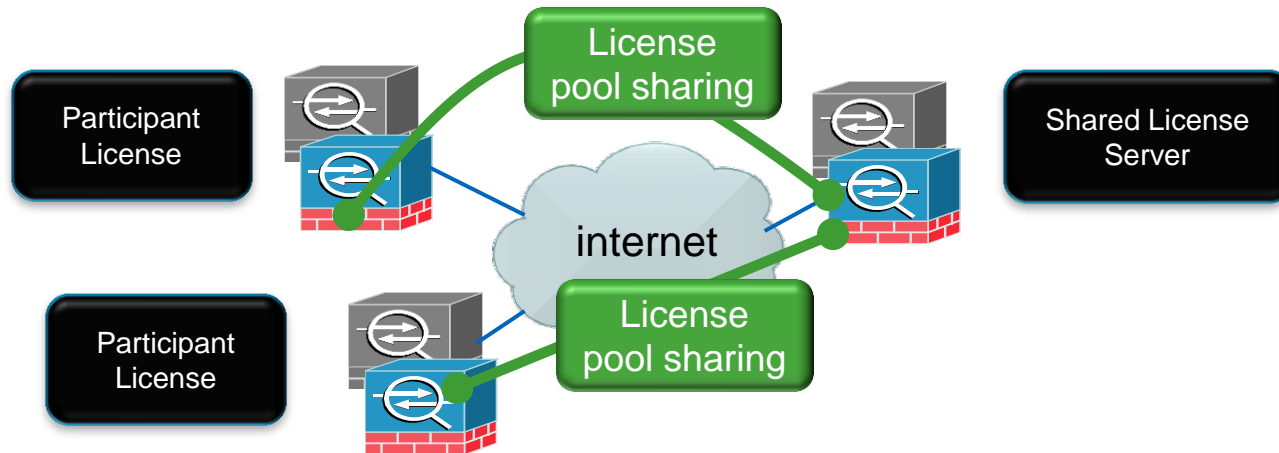
- Cluster of up to N ASAs sharing the load
 - ASAs must be on same LANs
- Client connects to virtual ip owned by master, redirected to least loaded member
- SSL VPN Premium licenses required on all members
- No synchronization of sessions or configurations



Note: This is not the same feature as clustering ASA in DC (does not support RA VPN)

Global Deployment with Shared Licenses

- Several ASA (typically active-standby) deployments around the world
- License sharing through common pool of shared licenses
- One ASA is license server (keep track of license pool)
- Participant license ASAs only have participants license (cheap)



Conclusion

- Clientless SSL VPN offers
 - Very granular access control, depending on authentication, AD membership, posture...
 - Support for many applications apart from web applications
- Clientless is **not always** Clientless
 - No guarantee that **all** features will work on **any** unknown device (java, privileges etc)
- Use AnyConnect (BRKSEC-3033) for more transparent in-the-office experience
- Clientless SSL VPN can be a complement to AnyConnect
 - To access resources where granular access control is required
 - For specific use cases where AnyConnect Installation not desirable

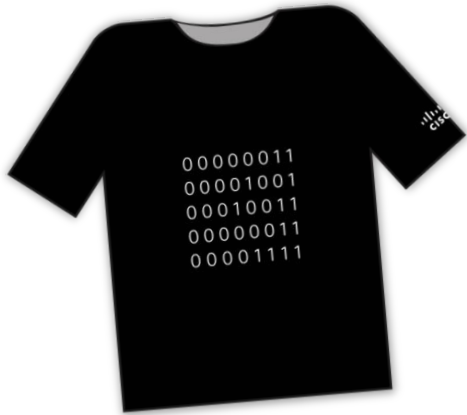
Call to Action...

Visit the World of Solutions:-

- **Cisco Campus**
- **Walk-in Labs**
- **Technical Solutions Clinics**
- **Meet the Engineer**
 - Håkan Nohre, Jeff Fanelli, Thorsten Rosendahl
- **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

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





CISCO™