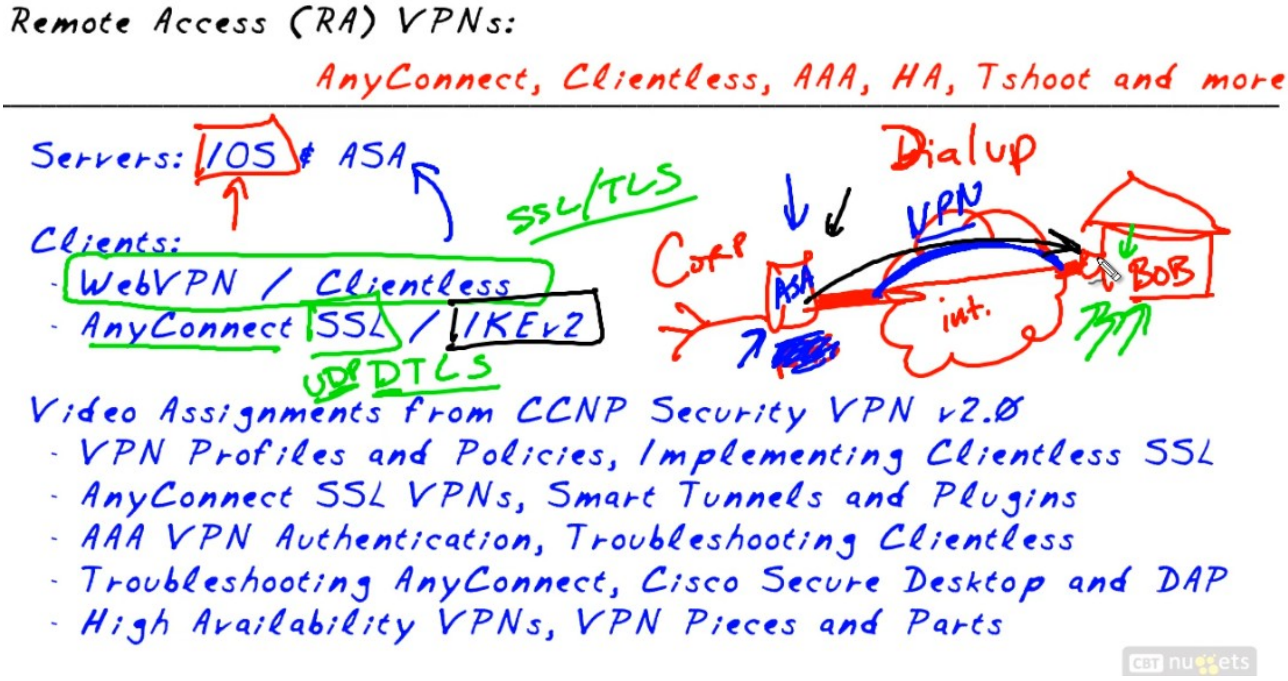
RA VPN (Remote Access VPN):



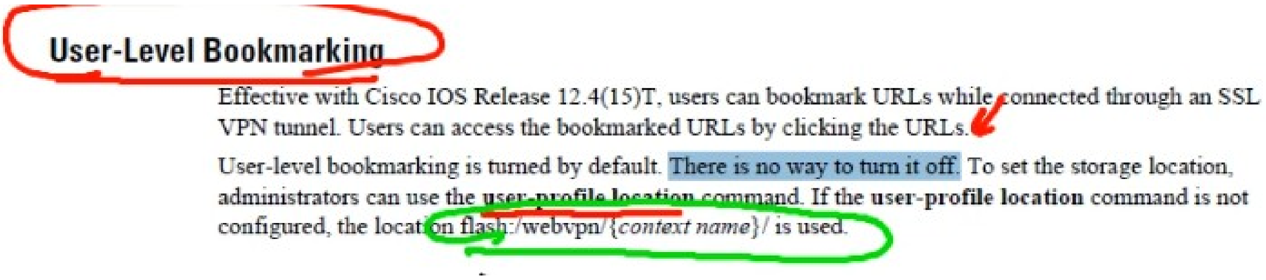
Remote Access (RA) VPNs:

AnyConnect, Clientless, AAA, HA, Tshoot and more

Servers: IOS & ASA

Clients:
- WebVPN / Clientless
- AnyConnect SSL / IKEv2

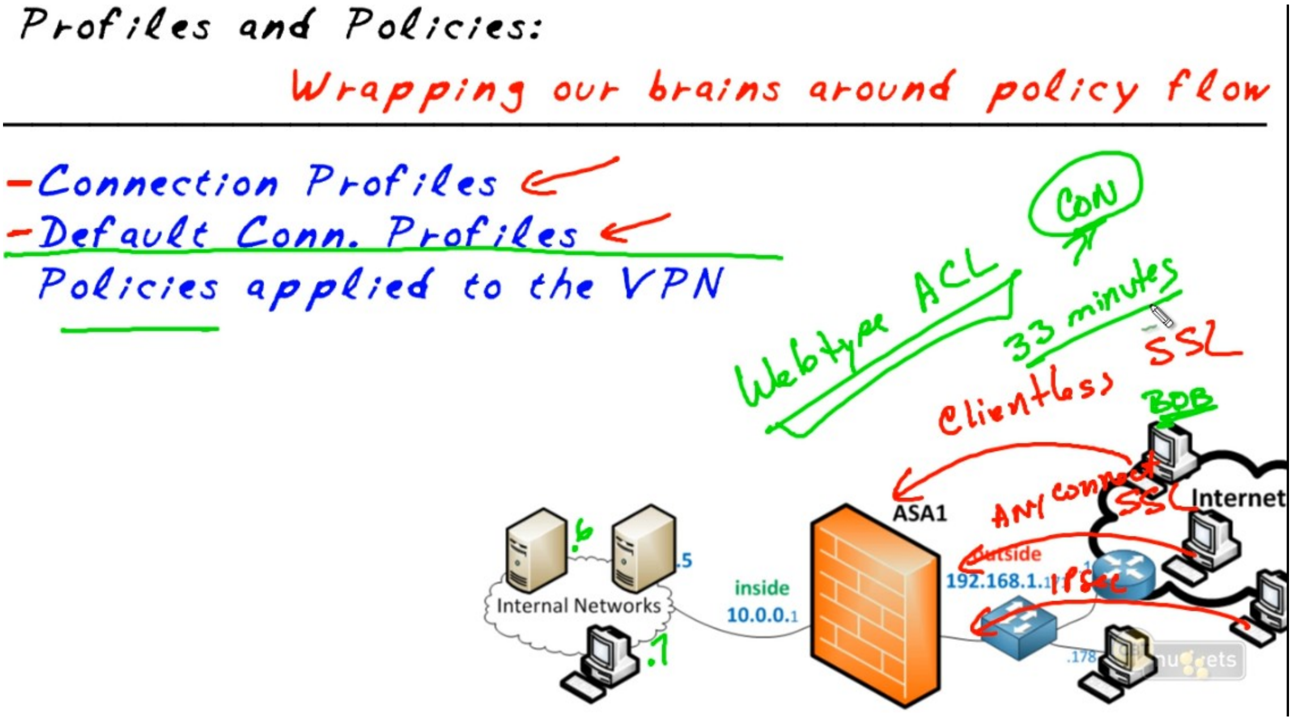
Video Assignments from CCNP Security VPN v2.0
- VPN Profiles and Policies, Implementing Clientless SSL
- AnyConnect SSL VPNs, Smart Tunnels and Plugins
- AAA VPN Authentication, Troubleshooting Clientless
- Troubleshooting AnyConnect, Cisco Secure Desktop and DAP
- High Availability VPNs, VPN Pieces and Parts



User-Level Bookmarking

Effective with Cisco IOS Release 12.4(15)T, users can bookmark URLs while connected through an SSL VPN tunnel. Users can access the bookmarked URLs by clicking the URLs.

User-level bookmarking is turned by default. There is no way to turn it off. To set the storage location, administrators can use the **user-profile location** command. If the **user-profile location** command is not configured, the location flash:/webvpn/{*context name*}/ is used.



Profiles and Policies:

Wrapping our brains around policy flow

- Connection Profiles
- Default Conn. Profiles

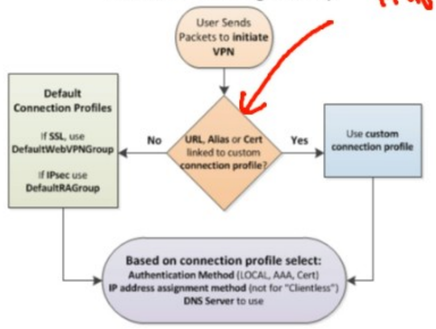
Policies applied to the VPN

Profiles and Policies:

Wrapping our brains around policy flow

Connection Profiles
Default Conn. Profiles
Policies applied to the VPN

Connection Profile (aka Tunnel Group) controls the "Pre-logon Policy"



User Sends Packets to **initiate** VPN

URL, Alias or Cert linked to custom **connection profile?**

No

Yes

Default Connection Profiles
If **SSL**, use **DefaultWebVPNGroup**
If **IPsec** use **DefaultRAGroup**

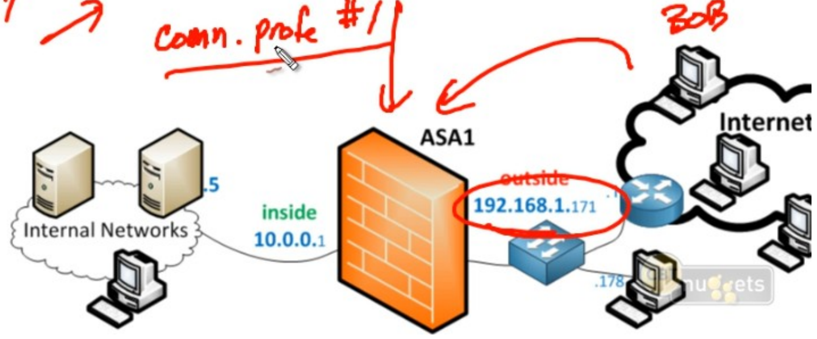
Use custom connection profile

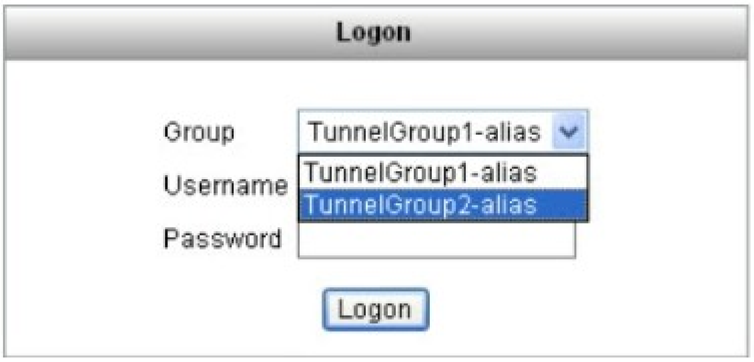
Based on connection profile select:
Authentication Method (LOCAL, AAA, Cert)
IP address assignment method (not for "Clientless")
DNS Server to use

Https://192.168.1.171/custom-url

conn. profe #1

SSL
TCP
← 443



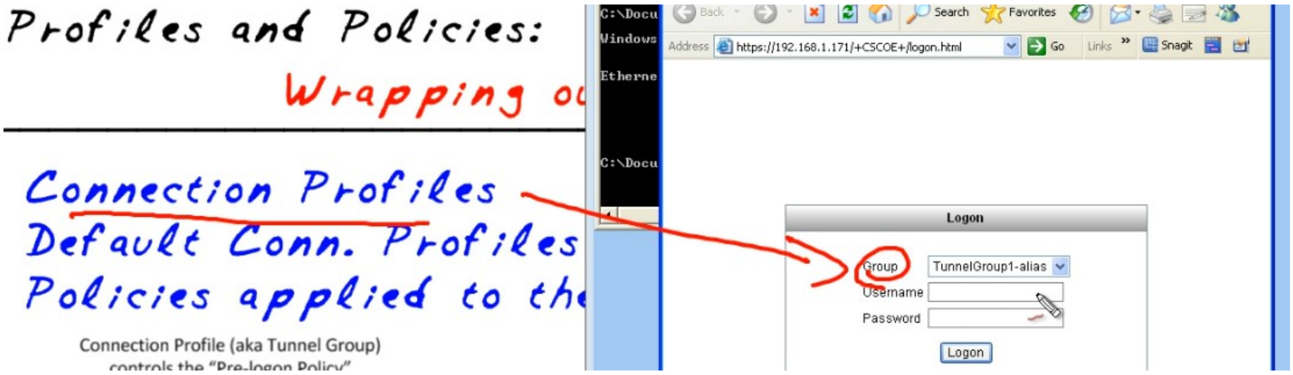


Logon

Group: TunnelGroup1-alias

Username

Password



Profiles and Policies:

Wrapping ou

Connection Profiles
Default Conn. Profiles
Policies applied to the

Connection Profile (aka Tunnel Group)
controls the "Pre-logon Policy"

```
C:\Docu
Windows
Etherne

C:\Docu
```

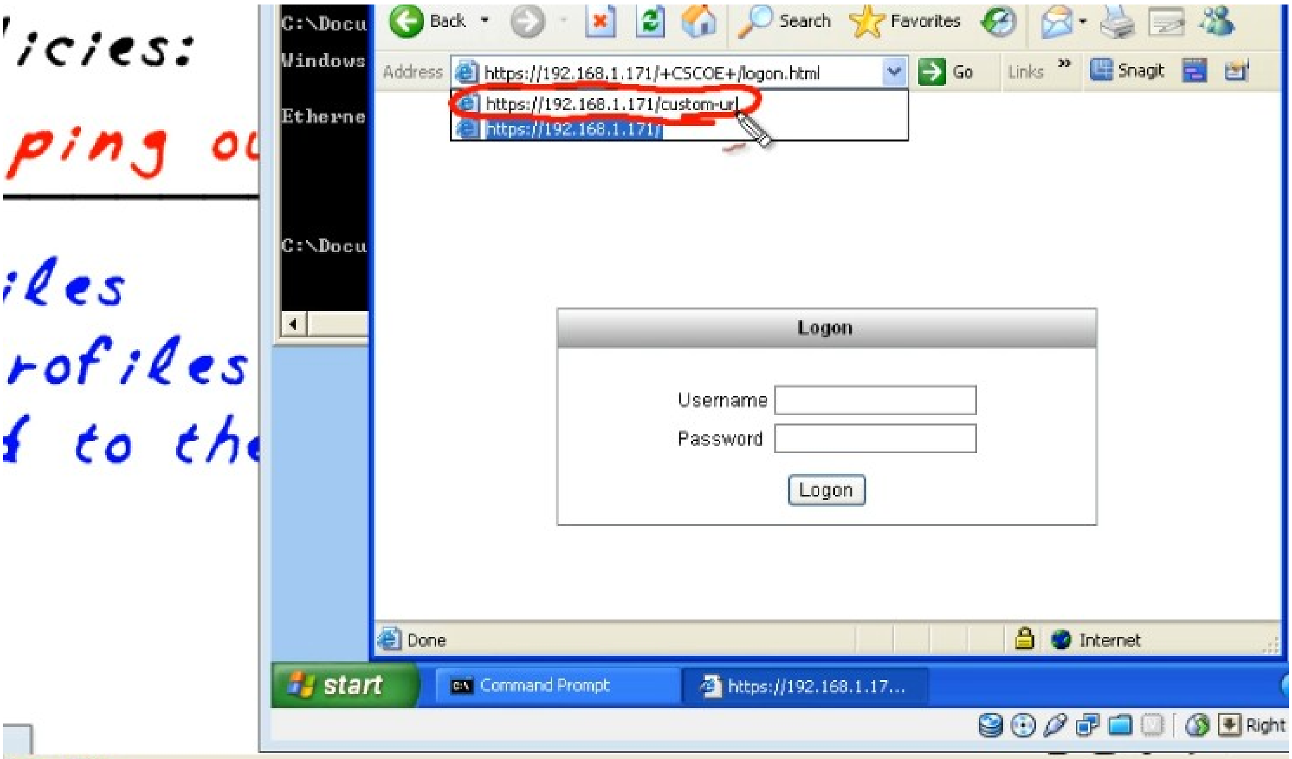
Address https://192.168.1.171/+CSCOE+/logon.html

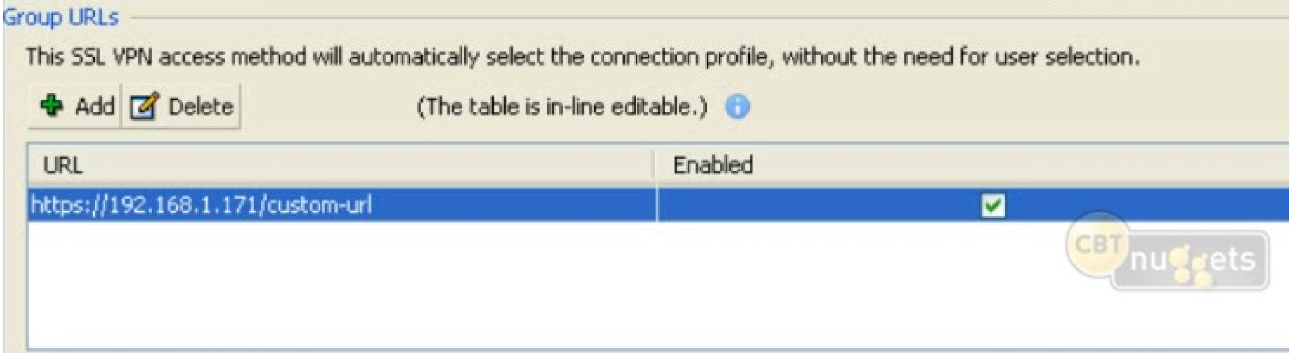
Logon

Group: TunnelGroup1-alias

Username

Password





Group URLs

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

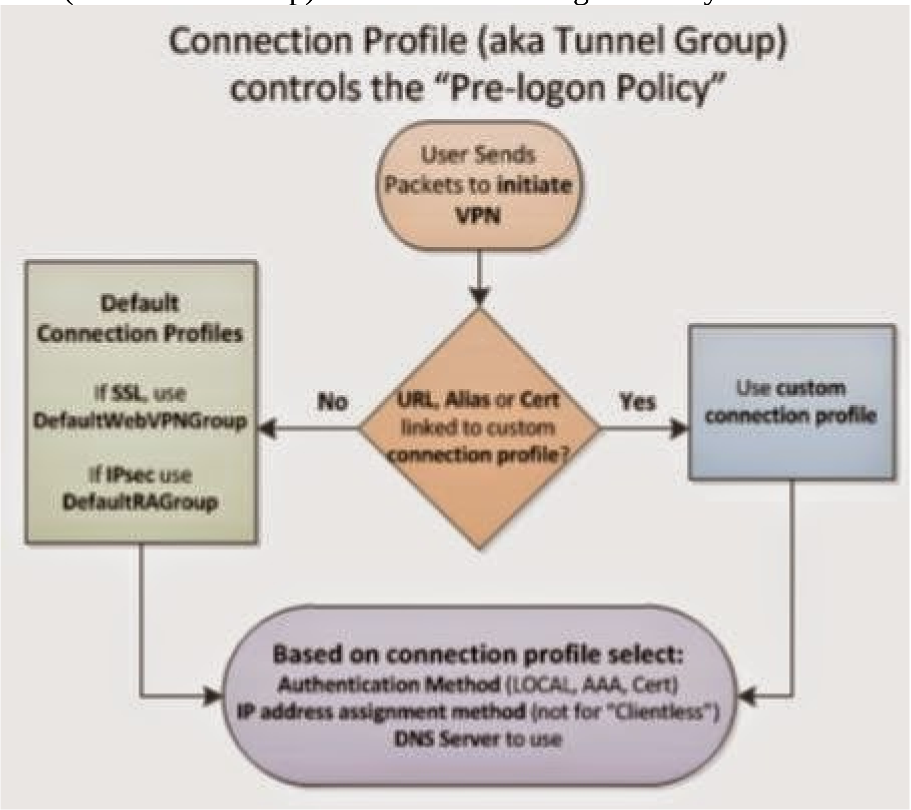
Add Delete (The table is in-line editable.)

URL	Enabled
https://192.168.1.171/custom-url	☑

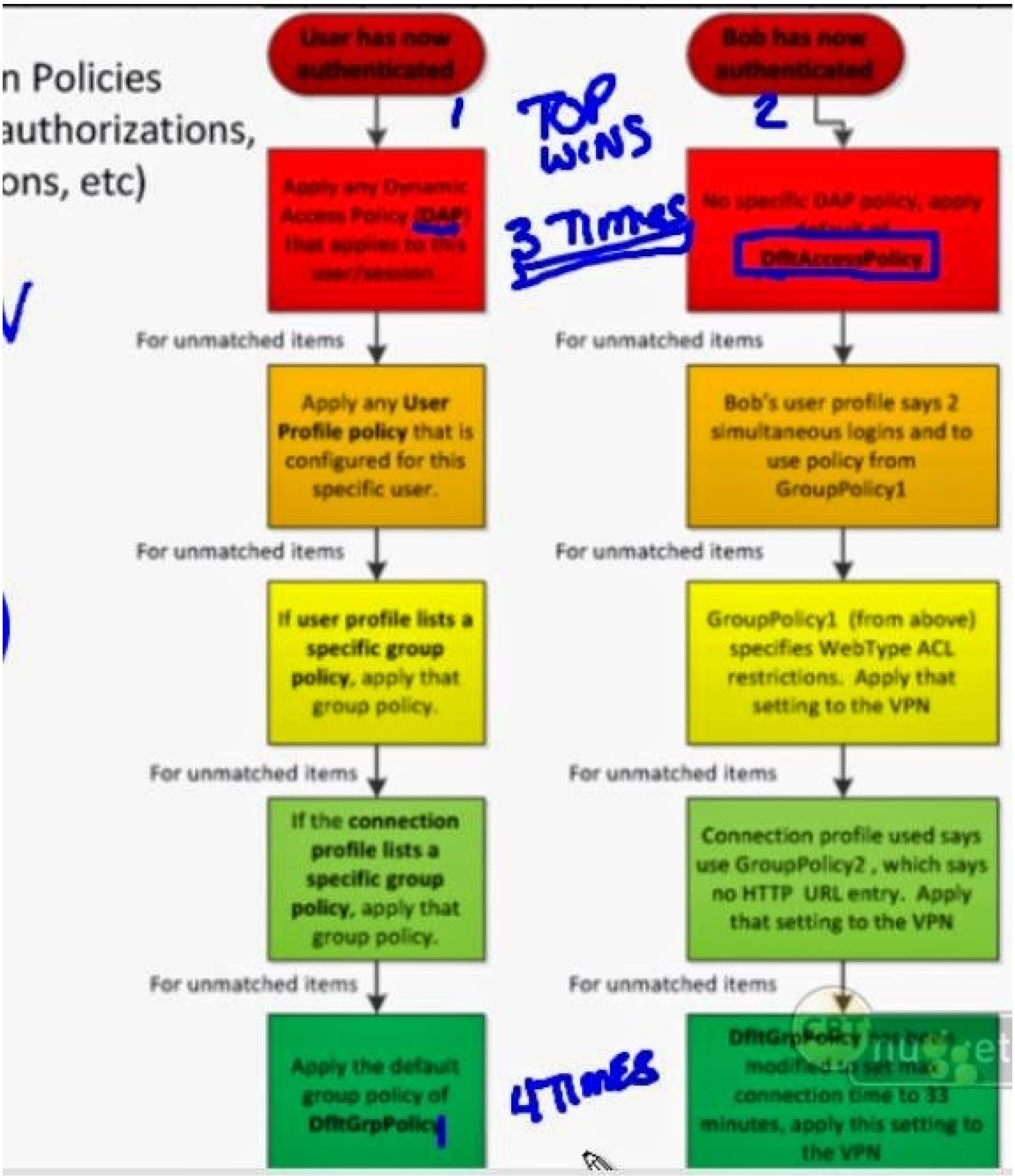
Three RA VPN methods:

Clientless
Anyconnect
Old IPSec cisco VPN client

VPN Profile and Policies
Connection Profile (aka Tunnel Group) controls the "Pre-logoin Policy":


Connection Profile (aka Tunnel Group) controls the "Pre-logon Policy"
User Sends Packets to initiate VPN
URL, Alias or Cert linked to custom connection profile?
No
Yes
Default Connection Profiles
If SSL, use DefaultWebVPNGroup
If IPsec use DefaultRAGroup
Use custom connection profile
Based on connection profile select:
Authentication Method (LOCAL, AAA, Cert)
IP address assignment method (not for "Clientless")
DNS Server to use

After login, ASA knows who the user is and post-login policies(permissions,authorizations,restrictions,etc) come. Top always win if there is conflict.



n Policies
authorizations,
ons, etc)

User has now authenticated

1

Apply any Dynamic Access Policy (DAP) that applies to this user/session.

For unmatched items

Apply any **User Profile policy** that is configured for this specific user.

For unmatched items

If **user profile lists a specific group policy**, apply that group policy.

For unmatched items

If the **connection profile lists a specific group policy**, apply that group policy.

For unmatched items

Apply the default group policy of **DfltGrpPolicy**

TOP WINS

3 Times

4 TIMES

Bob has now authenticated

2

No specific DAP policy, apply default of DfltAccessPolicy

For unmatched items

Bob's user profile says 2 simultaneous logins and to use policy from GroupPolicy1

For unmatched items

GroupPolicy1 (from above) specifies WebType ACL restrictions. Apply that setting to the VPN

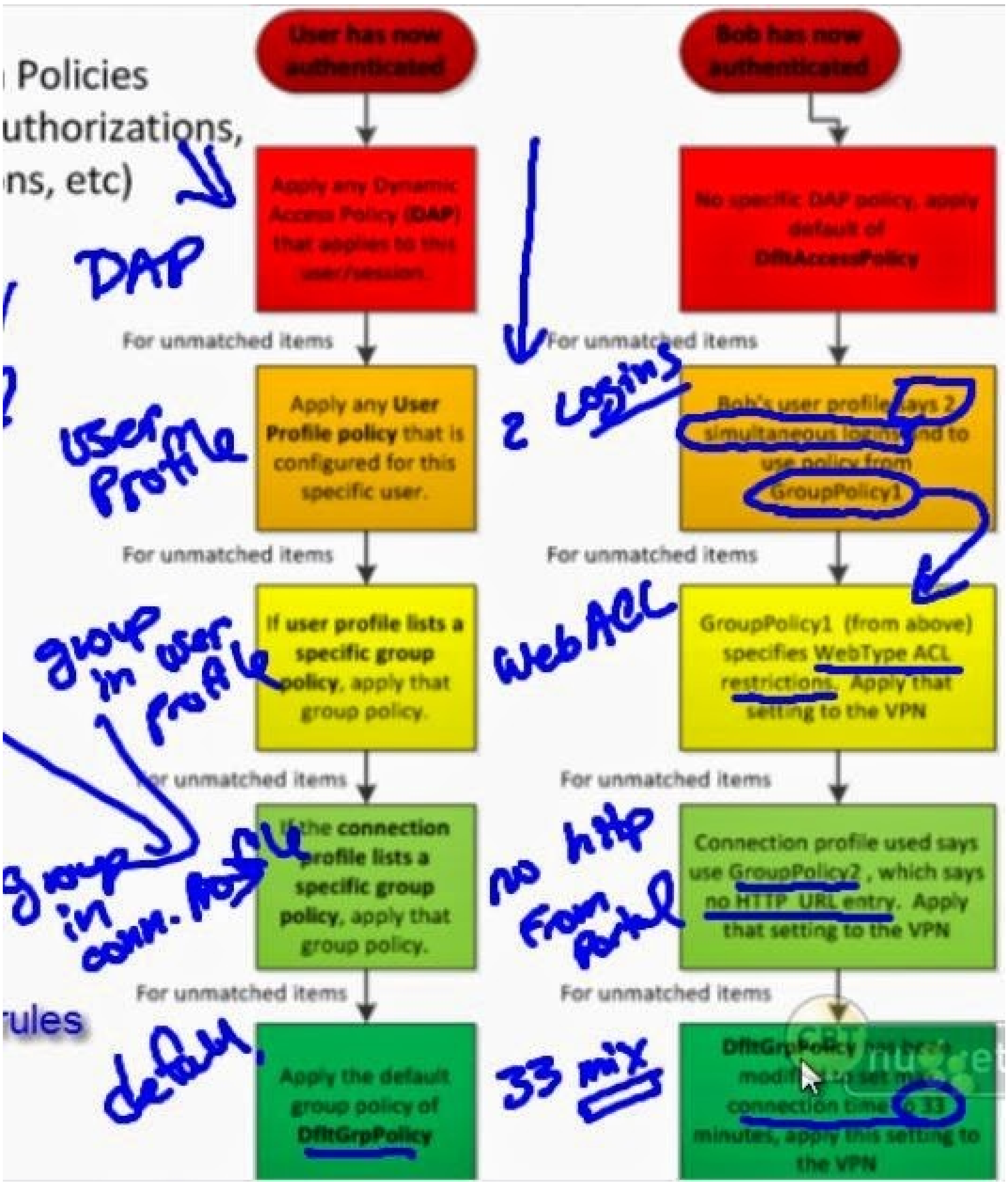
For unmatched items

Connection profile used says use GroupPolicy2 , which says no HTTP URL entry. Apply that setting to the VPN

For unmatched items

DfltGrpPolicy has been modified to set max connection time to 33 minutes, apply this setting to the VPN

Example Flow:



Policies
uthorizations,
ns, etc)

rules

User has now authenticated

Apply any Dynamic Access Policy (DAP) that applies to this user/session.

For unmatched items

Apply any User Profile policy that is configured for this specific user.

For unmatched items

If user profile lists a specific group policy, apply that group policy.

For unmatched items

If the connection profile lists a specific group policy, apply that group policy.

For unmatched items

Apply the default group policy of DfltGrpPolicy

Bob has now authenticated

No specific DAP policy, apply default of DfltAccessPolicy

For unmatched items

Bob's user profile says 2 simultaneous logins and to use policy from GroupPolicy1

For unmatched items

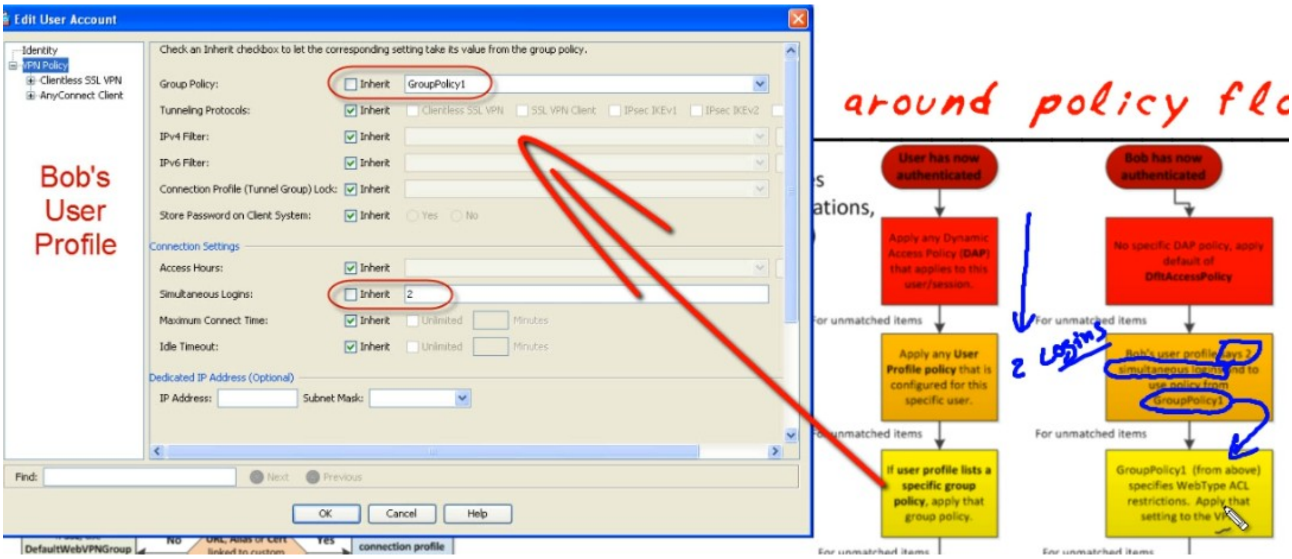
GroupPolicy1 (from above) specifies WebType ACL restrictions. Apply that setting to the VPN

For unmatched items

Connection profile used says use GroupPolicy2 , which says no HTTP URL entry. Apply that setting to the VPN

For unmatched items

DfltGrpPolicy has been modified to set max connection time to 33 minutes, apply this setting to the VPN



Edit User Account

Identity
VPN Policy
Clientless SSL VPN
AnyConnect Client

Bob's User Profile

Check an Inherit checkbox to let the corresponding setting take its value from the group policy.

Group Policy: □ Inherit GroupPolicy1

Tunneling Protocols: ☑ Inherit □ Clientless SSL VPN □ SSL VPN Client □ IPsec IKEv1 □ IPsec IKEv2

IPv4 Filter: ☑ Inherit

IPv6 Filter: ☑ Inherit

Connection Profile (Tunnel Group) Lock: ☑ Inherit

Store Password on Client System: ☑ Inherit ○ Yes ○ No

Connection Settings

Access Hours: ☑ Inherit

Simultaneous Logins: □ Inherit 2

Maximum Connect Time: ☑ Inherit □ Unlimited Minutes

Idle Timeout: ☑ Inherit □ Unlimited Minutes

Dedicated IP Address (Optional)

IP Address: Subnet Mask:

Find: Next Previous

User has now authenticated

Apply any Dynamic Access Policy (DAP) that applies to this user/session.

For unmatched items

Apply any User Profile policy that is configured for this specific user.

For unmatched items

If user profile lists a specific group policy, apply that group policy.

For unmatched items

Bob has now authenticated

No specific DAP policy, apply default of DfltAccessPolicy

For unmatched items

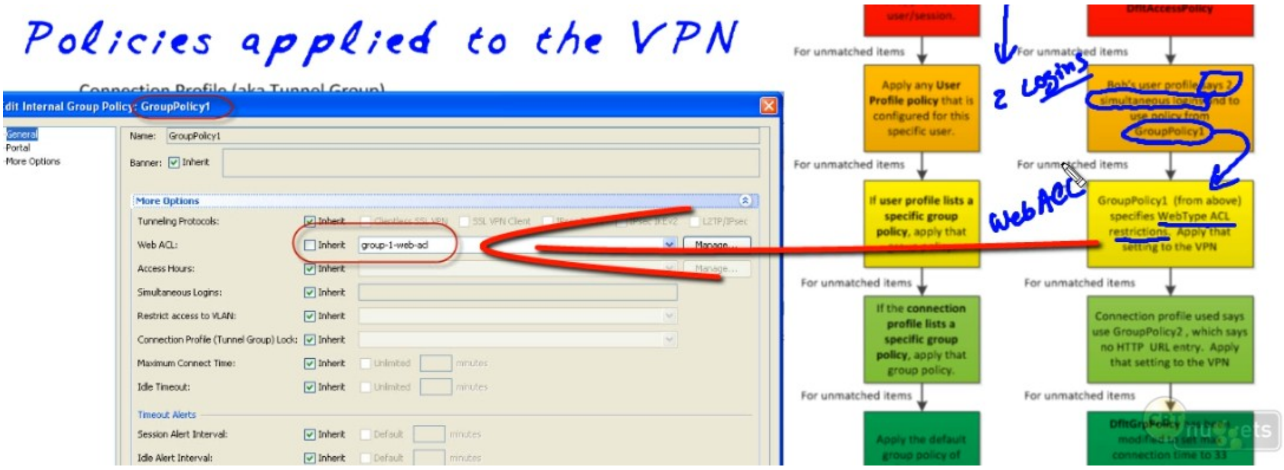
Bob's user profile says 2 simultaneous logins and to use policy from GroupPolicy1

For unmatched items

GroupPolicy1 (from above) specifies WebType ACL restrictions. Apply that setting to the VPN

For unmatched items

Policies applied to the VPN



Connection Profile (aka Tunnel Group)

dit Internal Group Policy: GroupPolicy1

General
Portal
More Options

Name: GroupPolicy1

Banner: ☑ Inherit

More Options

Tunneling Protocols:	☑ Inherit	□ Clientless SSL VPN □ SSL VPN Client □ IPsec IKEv1 □ IPsec IKEv2 □ L2TP/IPsec
Web ACL:	□ Inherit	group-1-web-acl
Access Hours:	☑ Inherit	
Simultaneous Logins:	☑ Inherit	
Restrict access to VLAN:	☑ Inherit	
Connection Profile (Tunnel Group) Lock:	☑ Inherit	
Maximum Connect Time:	☑ Inherit	□ Unlimited minutes
Idle Timeout:	☑ Inherit	□ Unlimited minutes

Timeout Alerts

Session Alert Interval:	☑ Inherit	□ Default minutes
Idle Alert Interval:	☑ Inherit	□ Default minutes

user/session.

For unmatched items

Apply any **User Profile policy** that is configured for this specific user.

For unmatched items

If **user profile lists a specific group policy**, apply that group policy.

For unmatched items

If the **connection profile lists a specific group policy**, apply that group policy.

For unmatched items

Apply the default group policy of

DfltAccessPolicy

For unmatched items

Bob's user profile says 2 simultaneous logins and to use policy from GroupPolicy1

For unmatched items

GroupPolicy1 (from above) specifies WebType ACL restrictions. Apply that setting to the VPN

For unmatched items

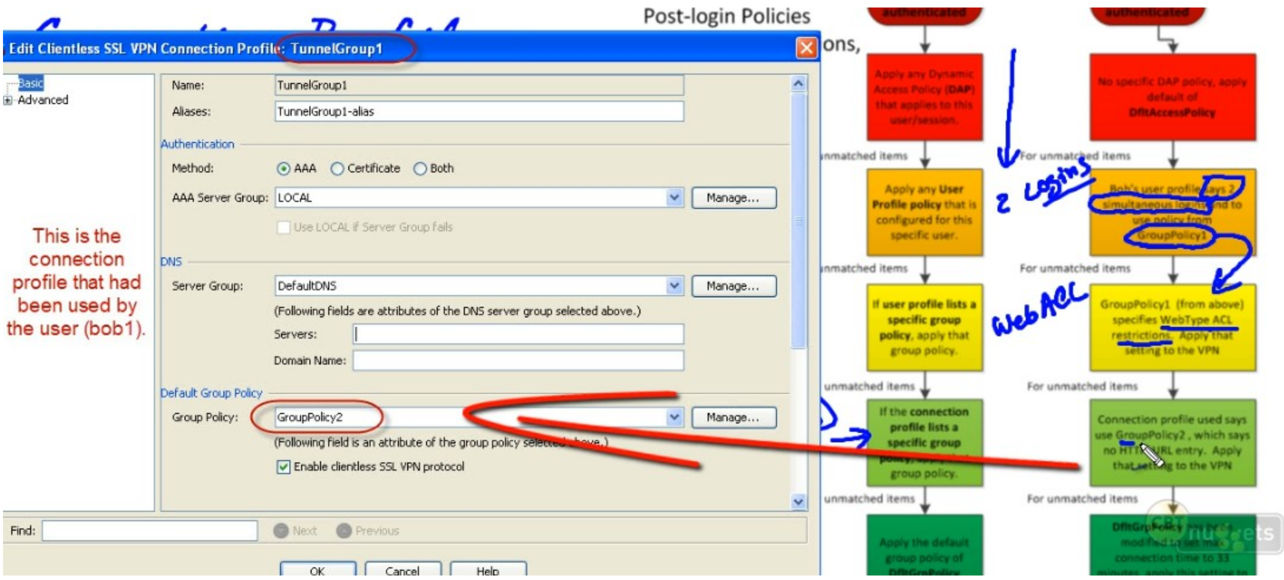
Connection profile used says use GroupPolicy2 , which says no HTTP URL entry. Apply that setting to the VPN

For unmatched items

DfltGrpPolicy has been modified to set max connection time to 33

2 Logins

WebACL



Post-login Policies

ons,

Edit Clientless SSL VPN Connection Profile: TunnelGroup1

Basic
Advanced

Name: TunnelGroup1

Aliases: TunnelGroup1-alias

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

DNS

Server Group: DefaultDNS

(Following fields are attributes of the DNS server group selected above.)

Servers:

Domain Name:

Default Group Policy

Group Policy: GroupPolicy2

(Following field is an attribute of the group policy selected above.)

☑ Enable clientless SSL VPN protocol

This is the connection profile that had been used by the user (bob1).

authenticated

Apply any Dynamic Access Policy (DAP) that applies to this user/session.

For unmatched items

Apply any User Profile policy that is configured for this specific user.

For unmatched items

If user profile lists a specific group policy, apply that group policy.

For unmatched items

If the connection profile lists a specific group policy, apply that group policy.

For unmatched items

Apply the default group policy of DfltGrpPolicy

authenticated

No specific DAP policy, apply default of DfltAccessPolicy

For unmatched items

Bob's user profile says 2 simultaneous logins and to use policy from GroupPolicy1

For unmatched items

GroupPolicy1 (from above) specifies WebType ACL restrictions. Apply that setting to the VPN

For unmatched items

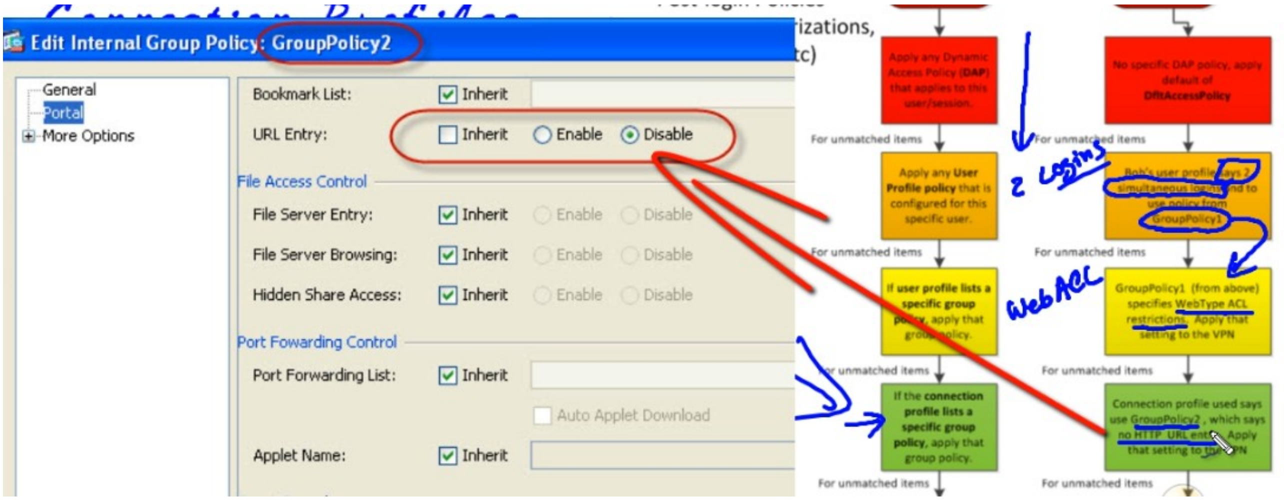
Connection profile used says use GroupPolicy2 , which says no HTTP URL entry. Apply that setting to the VPN

For unmatched items

DfltGrpPolicy has been modified to set max connection time to 33 minutes, apply this setting to the

2 Logins

WebACL



Post-login Policies

izations,
tc)

Edit Internal Group Policy: GroupPolicy2

General
Portal
More Options

Bookmark List:	☑ Inherit	
URL Entry:	□ Inherit	○ Enable ● Disable

File Access Control

File Server Entry:	☑ Inherit	○ Enable ○ Disable
File Server Browsing:	☑ Inherit	○ Enable ○ Disable
Hidden Share Access:	☑ Inherit	○ Enable ○ Disable

Port Fowarding Control

Port Forwarding List:	☑ Inherit	
		□ Auto Applet Download
Applet Name:	☑ Inherit	

Apply any Dynamic Access Policy (DAP) that applies to this user/session.

For unmatched items

Apply any User Profile policy that is configured for this specific user.

For unmatched items

If user profile lists a specific group policy, apply that group policy.

For unmatched items

If the connection profile lists a specific group policy, apply that group policy.

For unmatched items

No specific DAP policy, apply default of DfltAccessPolicy

For unmatched items

Bob's user profile says 2 simultaneous logins and to use policy from GroupPolicy1

For unmatched items

GroupPolicy1 (from above) specifies WebType ACL restrictions. Apply that setting to the VPN

For unmatched items

Connection profile used says use GroupPolicy2 , which says no HTTP URL entry. Apply that setting to the VPN

For unmatched items

2 Logins

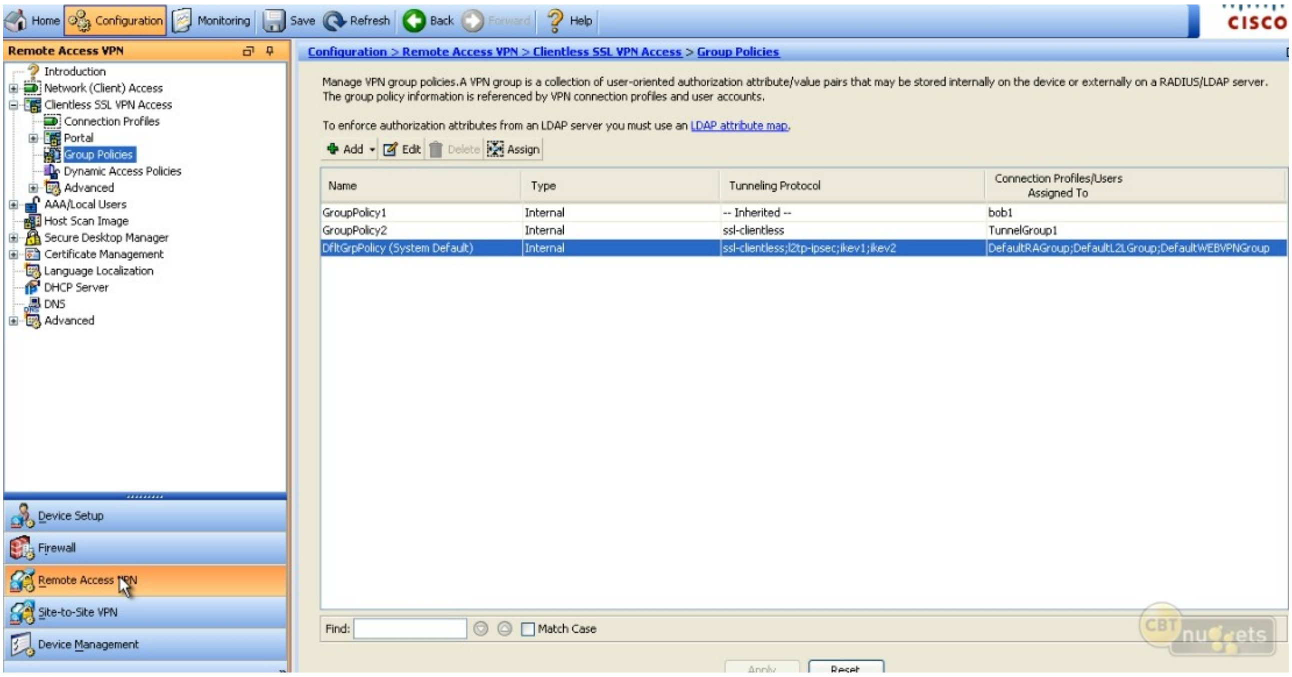
WebACL

VPN Profiles and Policies Flow (Top gets priority):

1.DAP rules (Dynamic Access Policy)(NAC)(e.g. if firewall present on client machine etc.)
2.User Profile rules (User Account)(e.g. Two simultanous logins)(tunnel group lock i.e. even if user chooses other tunnel group it will still be locked to a specific group)
3.User Profile Group rules (Group Policy attached to the User profile e.g. Sales group)(e.g. WebTypeACL e.g. Deny http://10.0.0.[7-8]/* and permit *)(e.g. custom bookmarks)
4.Connection Profile Group rules (selected at pre-login based on URL, Alias or Cert)(e.g. no http from portal)

DefaultWebVPNGroup
DefaultRAGroup
Custom connection profile

5.DfltGrpPolicy Group rules (e.g. connection time 33 mins)

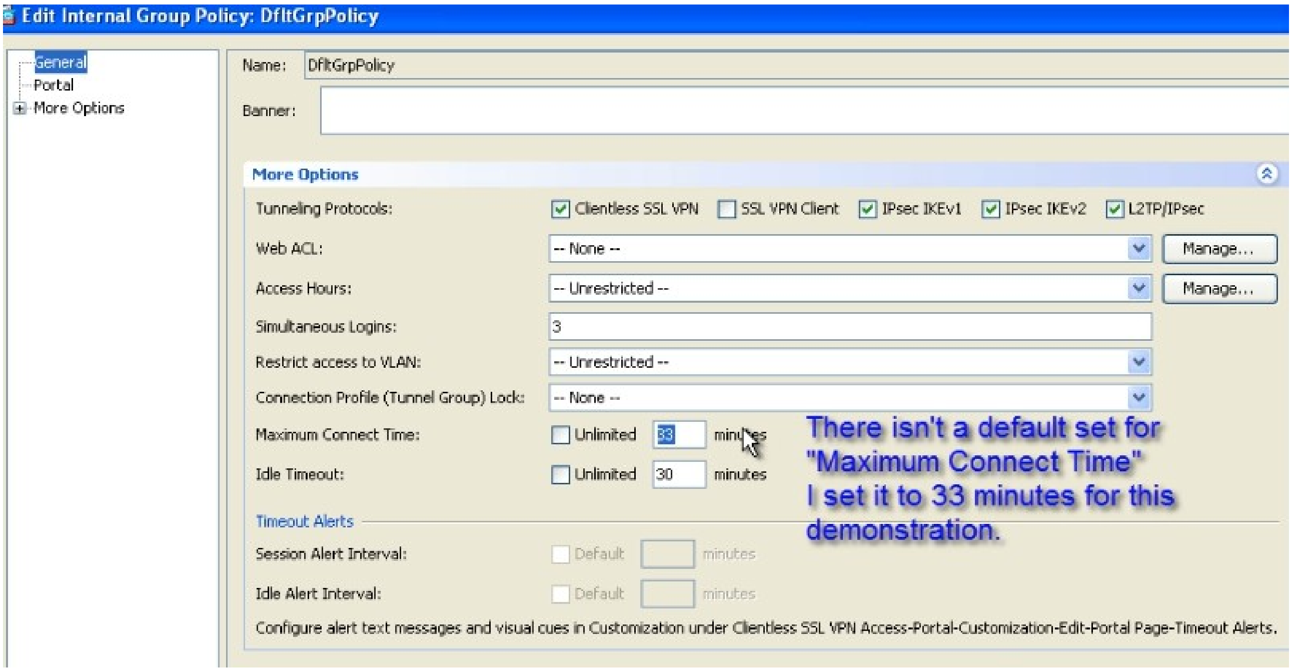


Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies

Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
GroupPolicy1	Internal	-- Inherited --	bob1
GroupPolicy2	Internal	ssl-clientless	TunnelGroup1
DfltGrpPolicy (System Default)	Internal	ssl-clientless;l2tp-ipsec;ikev1;ikev2	DefaultRAGroup;DefaultL2LGroup;DefaultWEBVPNGroup



Edit Internal Group Policy: DfltGrpPolicy

Name: DfltGrpPolicy

Banner:

More Options

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

Web ACL: -- None --

Access Hours: -- Unrestricted --

Simultaneous Logins: 3

Restrict access to VLAN: -- Unrestricted --

Connection Profile (Tunnel Group) Lock: -- None --

Maximum Connect Time: ☐ Unlimited 33 minutes

Idle Timeout: ☐ Unlimited 30 minutes

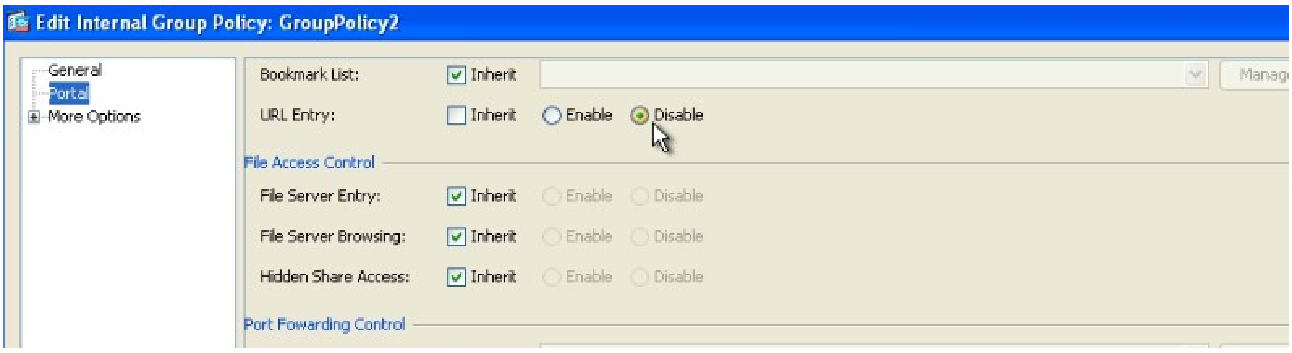
Timeout Alerts

Session Alert Interval: ☐ Default minutes

Idle Alert Interval: ☐ Default minutes

Configure alert text messages and visual cues in Customization under Clientless SSL VPN Access-Portal-Customization-Edit-Portal Page-Timeout Alerts.

There isn't a default set for "Maximum Connect Time"
I set it to 33 minutes for this demonstration.



Edit Internal Group Policy: GroupPolicy2

Bookmark List: ☑ Inherit

URL Entry: □ Inherit ○ Enable ● Disable

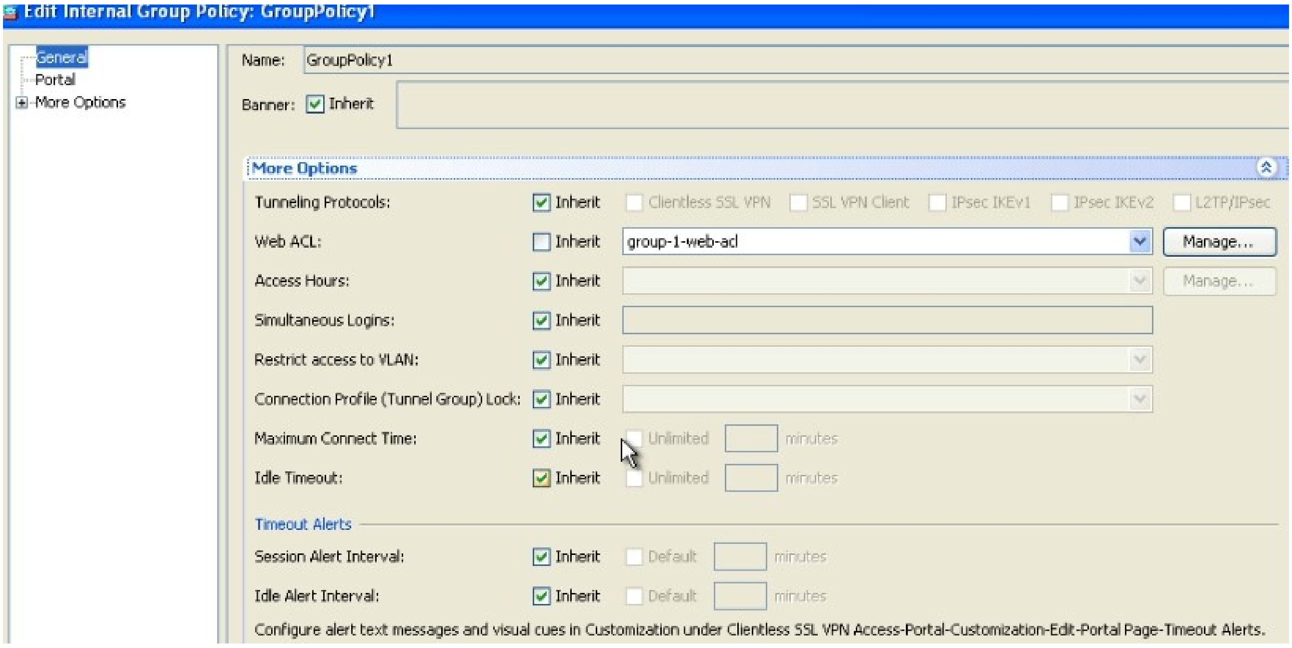
File Access Control

File Server Entry: ☑ Inherit ○ Enable ○ Disable

File Server Browsing: ☑ Inherit ○ Enable ○ Disable

Hidden Share Access: ☑ Inherit ○ Enable ○ Disable

Port Fowarding Control



Edit Internal Group Policy: GroupPolicy1

Name: GroupPolicy1

Banner: ☑ Inherit

More Options

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

Web ACL: □ Inherit group-1-web-acl Manage...

Access Hours: ☑ Inherit Manage...

Simultaneous Logins: ☑ Inherit

Restrict access to VLAN: ☑ Inherit

Connection Profile (Tunnel Group) Lock: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited minutes

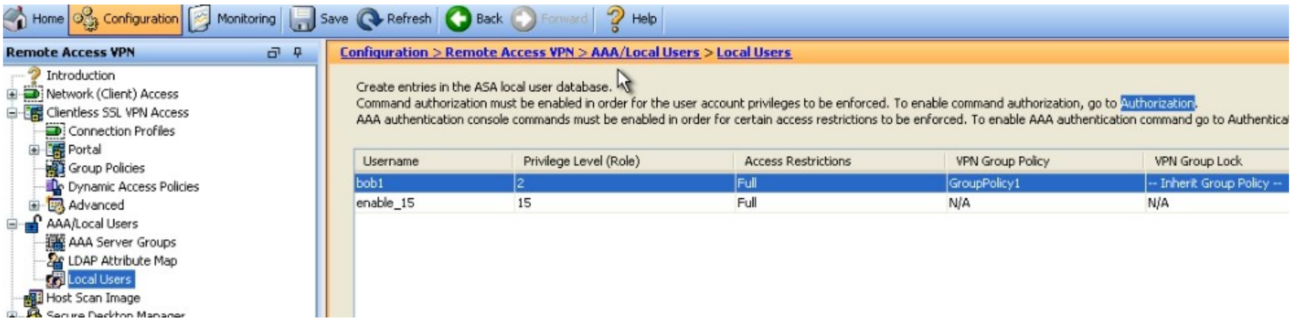
Idle Timeout: ☑ Inherit □ Unlimited minutes

Timeout Alerts

Session Alert Interval: ☑ Inherit □ Default minutes

Idle Alert Interval: ☑ Inherit □ Default minutes

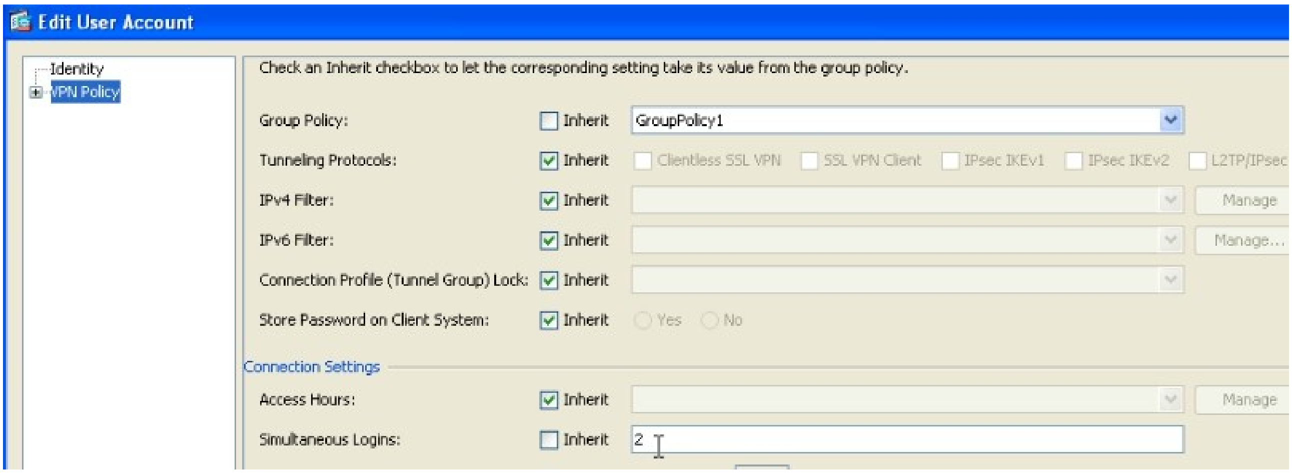
Configure alert text messages and visual cues in Customization under Clientless SSL VPN Access-Portal-Customization-Edit-Portal Page-Timeout Alerts.



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

Create entries in the ASA local user database.
Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to Authorization.
AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to Authentica

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock
bob1	2	Full	GroupPolicy1	-- Inherit Group Policy --
enable_15	15	Full	N/A	N/A



Edit User Account

Check an Inherit checkbox to let the corresponding setting take its value from the group policy.

Group Policy: □ Inherit GroupPolicy1

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

IPv4 Filter: ☑ Inherit Manage

IPv6 Filter: ☑ Inherit Manage...

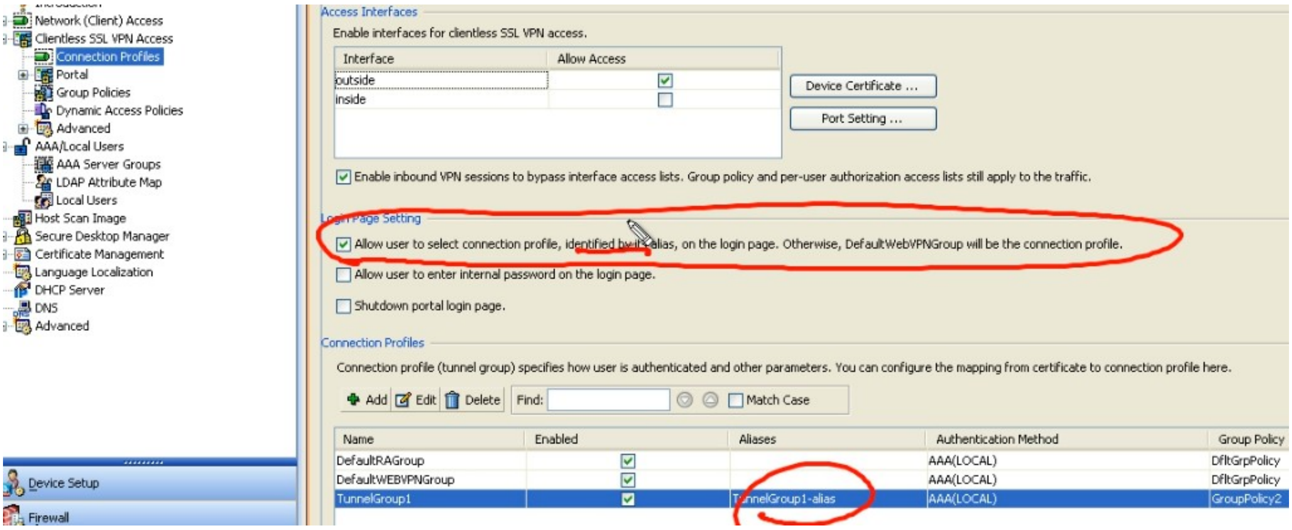
Connection Profile (Tunnel Group) Lock: ☑ Inherit

Store Password on Client System: ☑ Inherit ○ Yes ○ No

Connection Settings

Access Hours: ☑ Inherit Manage

Simultaneous Logins: □ Inherit 2



Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Portal
Group Policies
Dynamic Access Policies
Advanced
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
DHCP Server
DNS
Advanced

Device Setup
Firewall

Access Interfaces

Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	☑
inside	□

☑ Enable inbound VPN sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

Login Page Setting

☑ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.

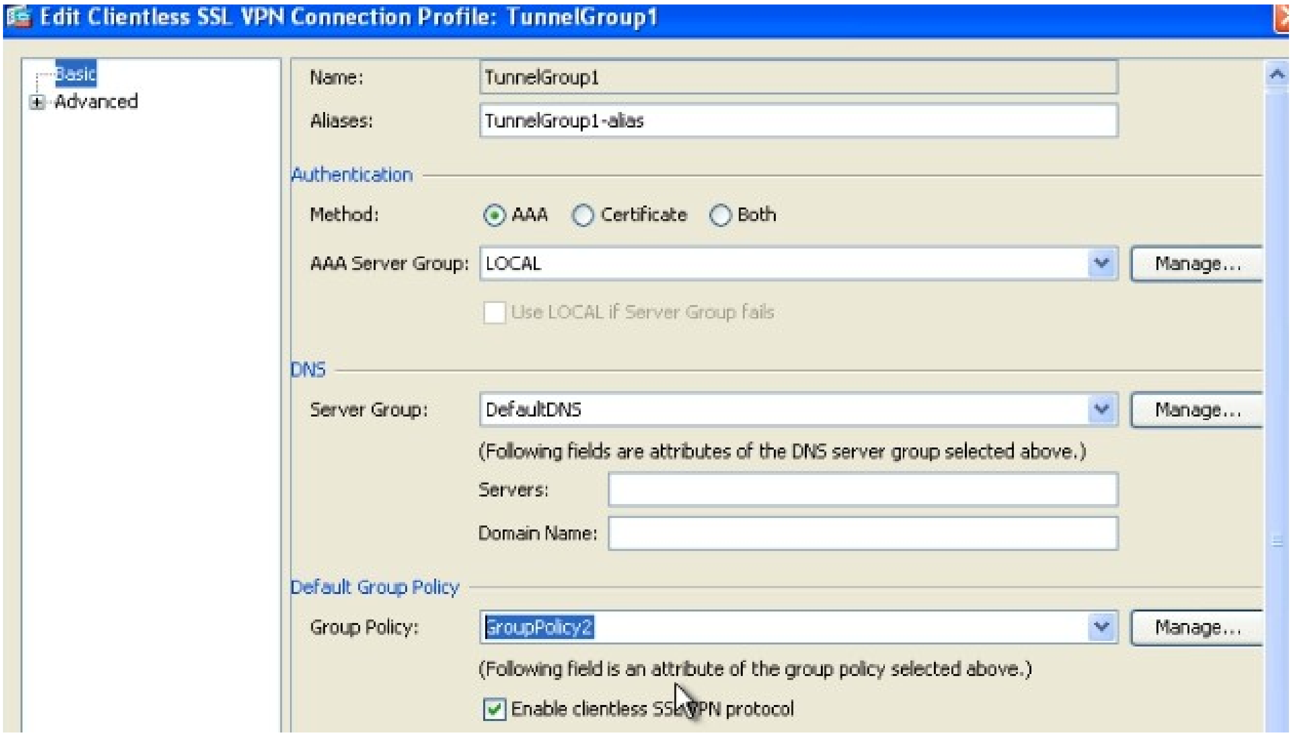
□ Allow user to enter internal password on the login page.

□ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.

Name	Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	☑		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPNGroup	☑		AAA(LOCAL)	DfltGrpPolicy
TunnelGroup1	☑	TunnelGroup1-alias	AAA(LOCAL)	GroupPolicy2



Edit Clientless SSL VPN Connection Profile: TunnelGroup1

Name: TunnelGroup1

Aliases: TunnelGroup1-alias

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

DNS

Server Group: DefaultDNS

(Following fields are attributes of the DNS server group selected above.)

Servers:

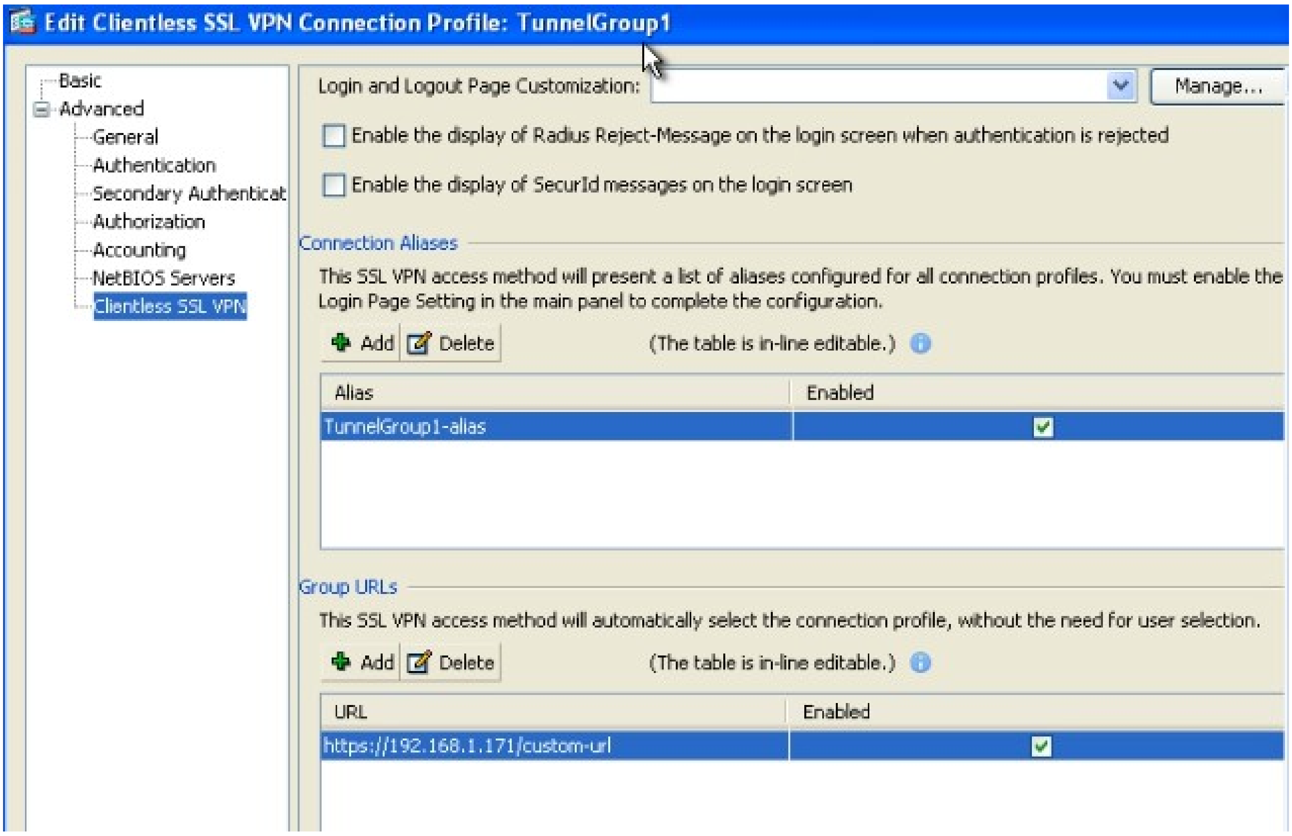
Domain Name:

Default Group Policy

Group Policy: GroupPolicy2

(Following field is an attribute of the group policy selected above.)

☑ Enable clientless SSL VPN protocol



Edit Clientless SSL VPN Connection Profile: TunnelGroup1

Login and Logout Page Customization:

☐ 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.

(The table is in-line editable.)

Alias	Enabled
TunnelGroup1-alias	☑

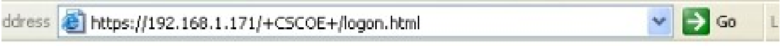
Group URLs

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

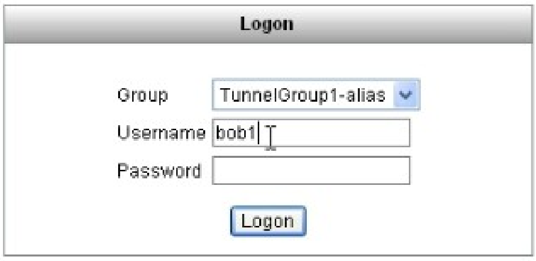
(The table is in-line editable.)

URL	Enabled
https://192.168.1.171/custom-url	☑

Option to select Tunnel Group/Connection Profile and associated Group Policy:



ddress https://192.168.1.171/+CSCOE+/logon.html



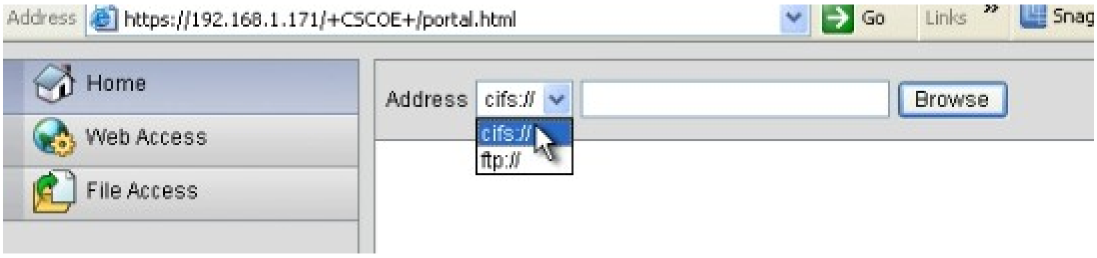
Logon

Group TunnelGroup1-alias

Username bob1

Password

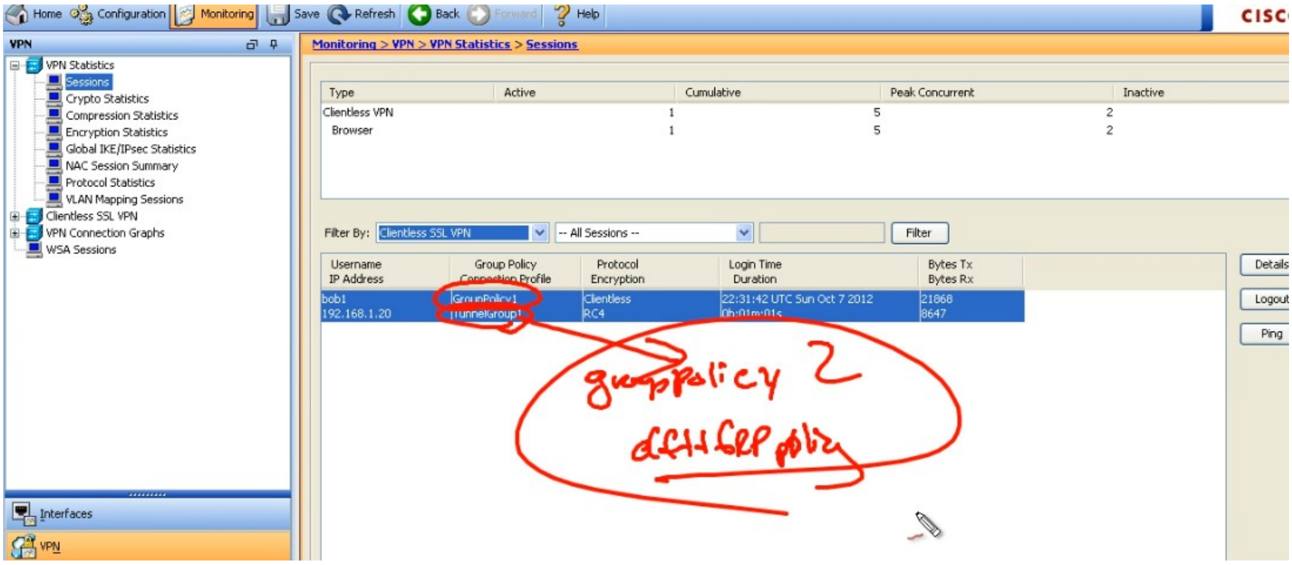
No http in the drop down as restricted by the connection profile group policy:



Address https://192.168.1.171/+CSCOE+/portal.html

Address cifs://

All these policies are assigned to this user:
1. Group Policy 1 for User Profile.
2. Group Policy 2 for Connection Profile (Tunnel group) selected by the User from the drop-down.
3. DfltGrpPolicy is the Default for all.



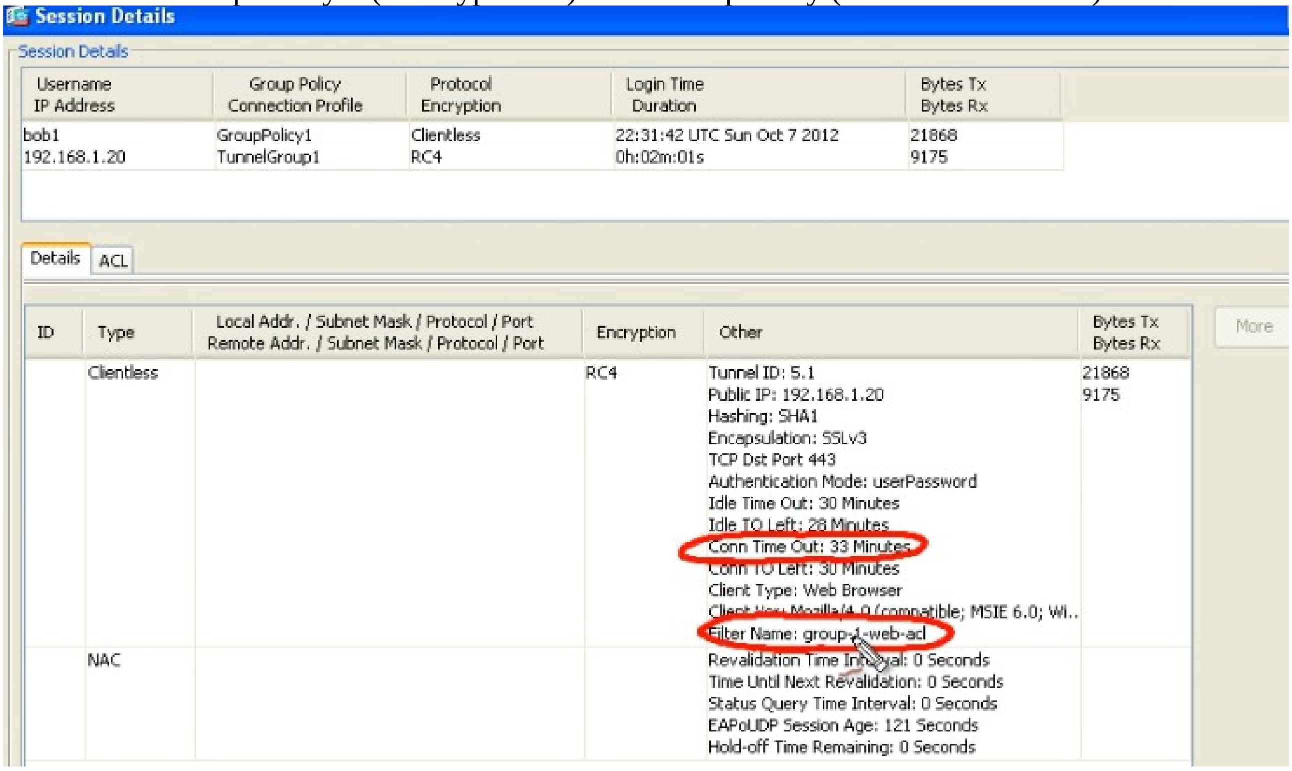
Monitoring > VPN > VPN Statistics > Sessions

Type	Active	Cumulative	Peak Concurrent	Inactive
Clientless VPN	1	5	2	
Browser	1	5	2	

Filter By: Clientless SSL VPN | -- All Sessions -- | Filter

Username IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
bob1 192.168.1.20	GroupPolicy1 TunnelGroup1	Clientless RC4	22:31:42 UTC Sun Oct 7 2012 0h:01m:01s	21868 8647

User Profile Group Policy 1 (WebTypeACL) and DfltGrpPoilcy (33 mins connection):

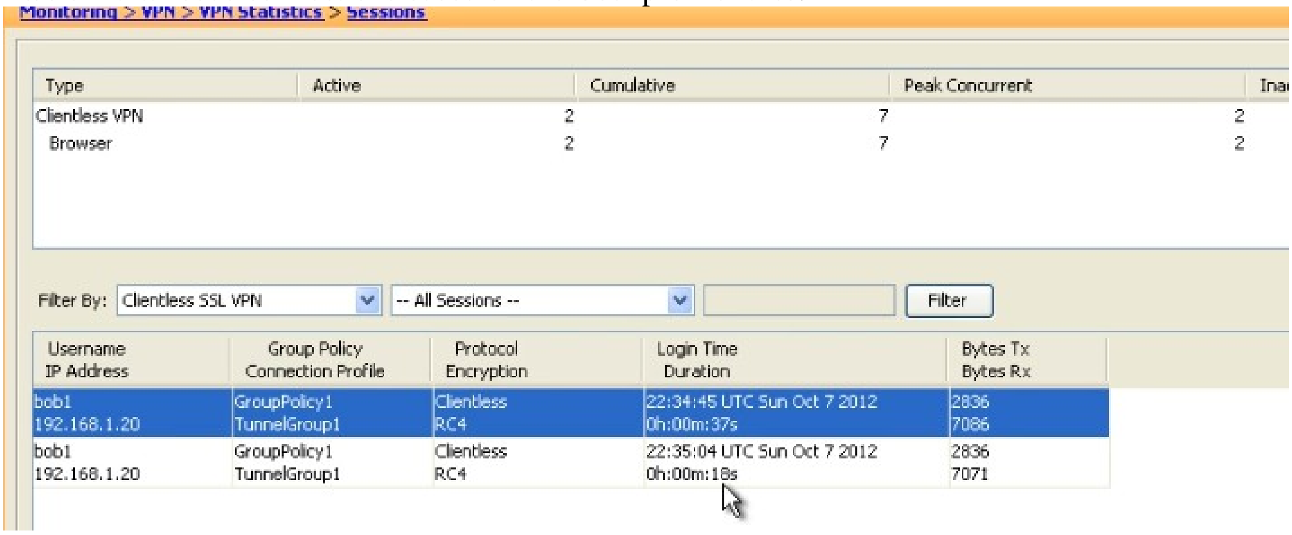


Session Details

Username IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
bob1 192.168.1.20	GroupPolicy1 TunnelGroup1	Clientless RC4	22:31:42 UTC Sun Oct 7 2012 0h:02m:01s	21868 9175

ID	Type	Local Addr. / Subnet Mask / Protocol / Port Remote Addr. / Subnet Mask / Protocol / Port	Encryption	Other	Bytes Tx Bytes Rx
	Clientless		RC4	Tunnel ID: 5.1 Public IP: 192.168.1.20 Hashing: SHA1 Encapsulation: SSLv3 TCP Dst Port 443 Authentication Mode: userPassword Idle Time Out: 30 Minutes Idle TO Left: 28 Minutes Conn Time Out: 33 Minutes Conn TO Left: 30 Minutes Client Type: Web Browser Client Ver: Mozilla/4.0 (compatible; MSIE 6.0; Wi.. Filter Name: group-1-web-acl	21868 9175
	NAC			Revalidation Time Interval: 0 Seconds Time Until Next Revalidation: 0 Seconds Status Query Time Interval: 0 Seconds EAPoUDP Session Age: 121 Seconds Hold-off Time Remaining: 0 Seconds	

Two simultaneous connections based on the User profile rules:



Monitoring > VPN > VPN Statistics > Sessions

Type	Active	Cumulative	Peak Concurrent	Ina
Clientless VPN	2	7	2	
Browser	2	7	2	

Filter By: Clientless SSL VPN -- All Sessions --

Username IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
bob1 192.168.1.20	GroupPolicy1 TunnelGroup1	Clientless RC4	22:34:45 UTC Sun Oct 7 2012 0h:00m:37s	2836 7086
bob1 192.168.1.20	GroupPolicy1 TunnelGroup1	Clientless RC4	22:35:04 UTC Sun Oct 7 2012 0h:00m:18s	2836 7071