Troubleshooting Clientless SSL VPN

Troubleshooting Clientless SSL VPNs:
Identify and resolve the configuration issue

State the problem
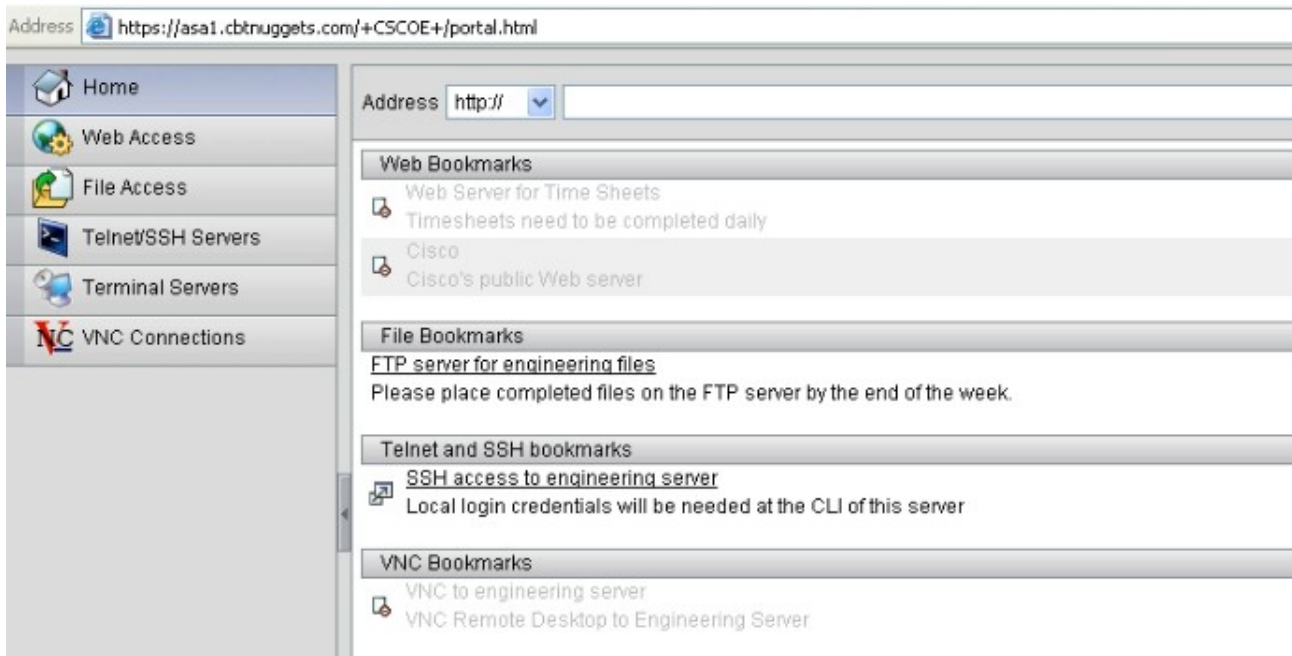Identify possibilities
Use the tools to isolate
Correct without causing harm

Connection profile: eng-con
Connection profile alias: eng-con-alias
User: eng-user
Group: eng-group

eng-user

ASA1

outside
192.168.1.171

inside
10.0.0.1

.5
Internal Networks

Internet

.1

.178

End user machine, located on a network somewhere on the outside (from the ASAs perspective.

Address https://asa1.cbtnuggets.com/+CSCOE+/portal.html

Home
Web Access
File Access
Telnet/SSH Servers
Terminal Servers
VNC Connections

Address http://

Web Bookmarks
Web Server for Time Sheets
Timesheets need to be completed daily
Cisco
Cisco's public Web server

File Bookmarks
FTP server for engineering files
Please place completed files on the FTP server by the end of the week.

Telnet and SSH bookmarks
SSH access to engineering server
Local login credentials will be needed at the CLI of this server

VNC Bookmarks
VNC to engineering server
VNC Remote Desktop to Engineering Server

```
ASA1# show vpn-sessiondb webvpn

Session Type: WebVPN

Username       : eng-user              Index        : 15
Public IP      : 192.168.1.20
Protocol       : Clientless
License        : AnyConnect Premium
Encryption     : RC4                   Hashing      : SHA1
Bytes Tx       : 15208                 Bytes Rx     : 27231
Group Policy   : eng-group             Tunnel Group : eng-con
Login Time     : 11:45:00 PDT Wed Oct 17 2012
Duration       : 0h:06m:32s
Inactivity     : 0h:00m:00s
NAC Result     : Unknown
VLAN Mapping   : N/A                   VLAN         : none

ASA1#
```
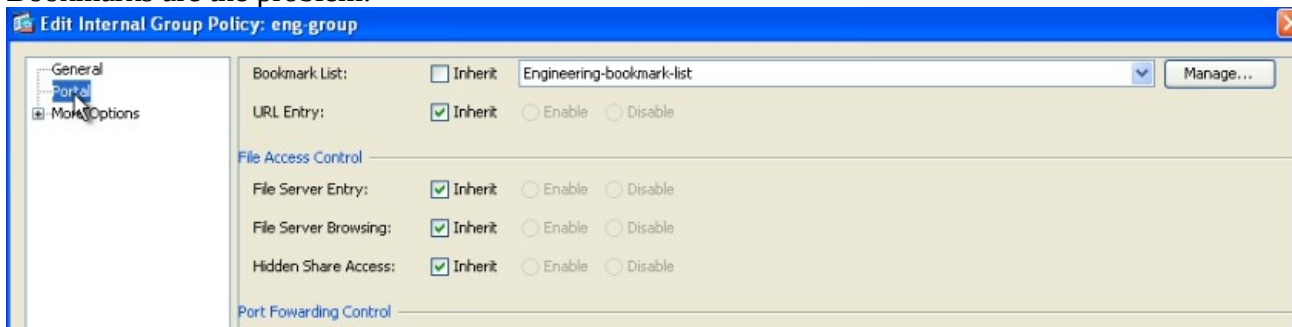
Check User, Tunnel Group (Connection profile) and Group Policy on ASDM.
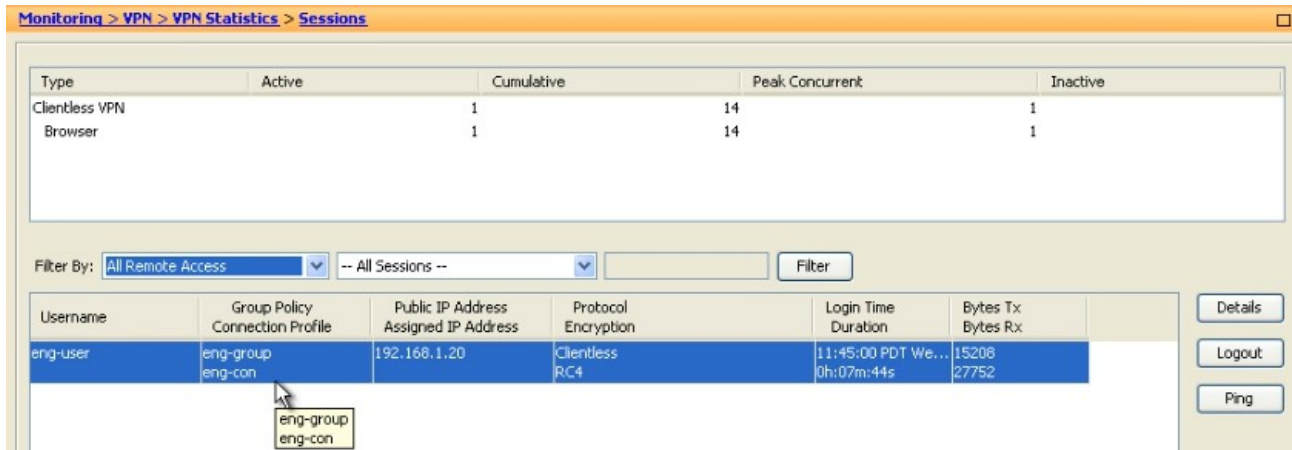
Bookmarks are the problem:

Home | Configuration | Monitoring | Save | Refresh | Back | Forward | Help

Remote Access VPN

- Introduction
- Network (Client) Access
- Clientless SSL VPN Access
  - Connection Profiles
  - Portal
    - Bookmarks
    - Client-Server Plug-ins
    - Customization
    - Help Customization
    - Portal Access Rules
    - Port Forwarding
    - Smart Tunnels
    - Web Contents
  - Group Policies
  - Dynamic Access Policies
  - Advanced
- AAA/Local Users
- Host Scan Image
- Secure Desktop Manager
- Certificate Management
- Language Localization
- DHCP Server
- DNS
- Advanced

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks

Configure Bookmark Lists that the security appliance displays on the SSL VPN portal page.

This parameter is enforced in either a VPN group policy, a dynamic access policy, or a user policy configuration. You can click on

Add | Edit | Delete | Import | Export | Assign

Bookmar...   the Bookmarks
Template
Bookmark
cl-bookm
Engineeri

Edit Bookmark List

Bookmark List Name: Engineering-bookmark-list

Bookmark Title	URL
Web Server for Time Sheets	http://10.0.0.5
SSH access to engineering server	ssh://10.0.0.5
FTP server for engineering files	ftp://10.0.0.5
VNC to engineering server	vnc://10.0.0.5
Cisco	http://www.cisco.com

Add
Edit
Delete
Move Up
Move Down

Find: [   ] ⊙ ⊙ ☐ Match Case

OK | Cancel | Help

Edit Internal Group Policy: eng-group

- General
- Portal
- More Options

Name: eng-group

Banner: ☑ Inherit [   ]

More Options

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

Web ACL: ☐ Inherit [eng-webtype-ACL ▼] Manage...

Access Hours: ☑ Inherit [▼] Manage...

Simultaneous Logins: ☑ Inherit [   ]

Restrict access to VLAN: ☑ Inherit [▼]

Connection Profile (Tunnel Group) Lock: ☑ Inherit [▼]
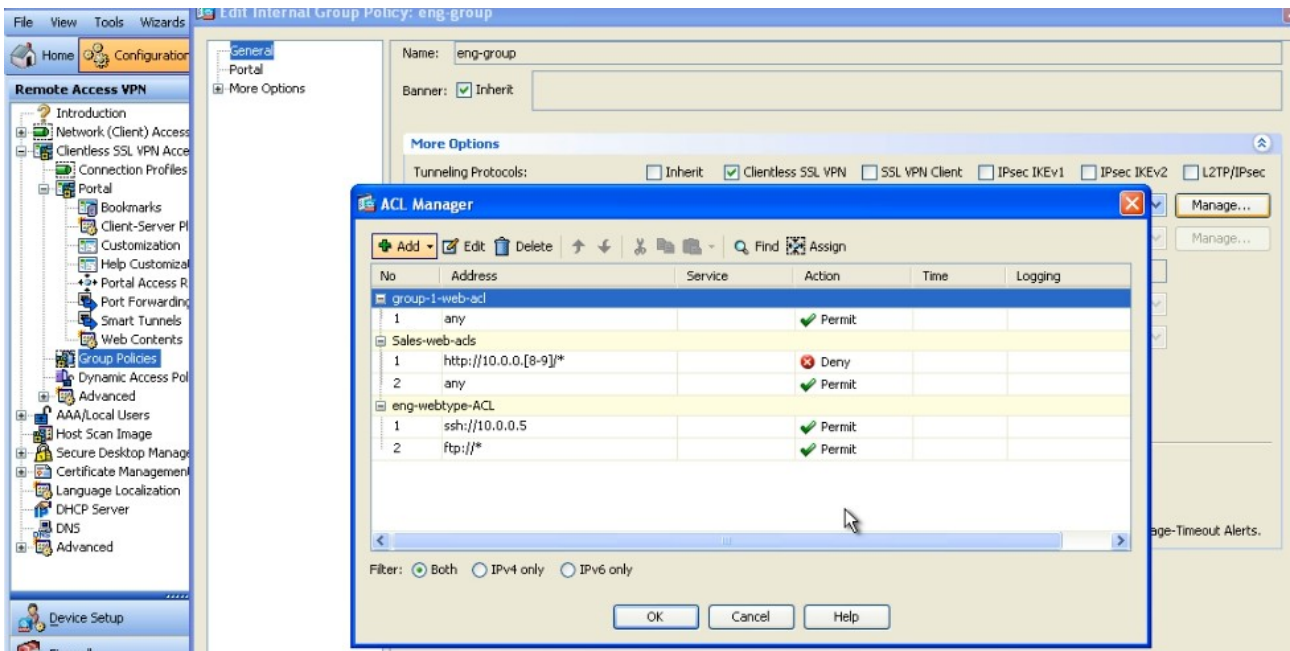
Maximum Connect Time: ☑ Inherit ☐ Unlimited [   ] minutes

Idle Timeout: ☑ Inherit ☐ Unlimited [   ] minutes

Timeout Alerts

Session Alert Interval: ☑ Inherit ☐ Default [   ] minutes
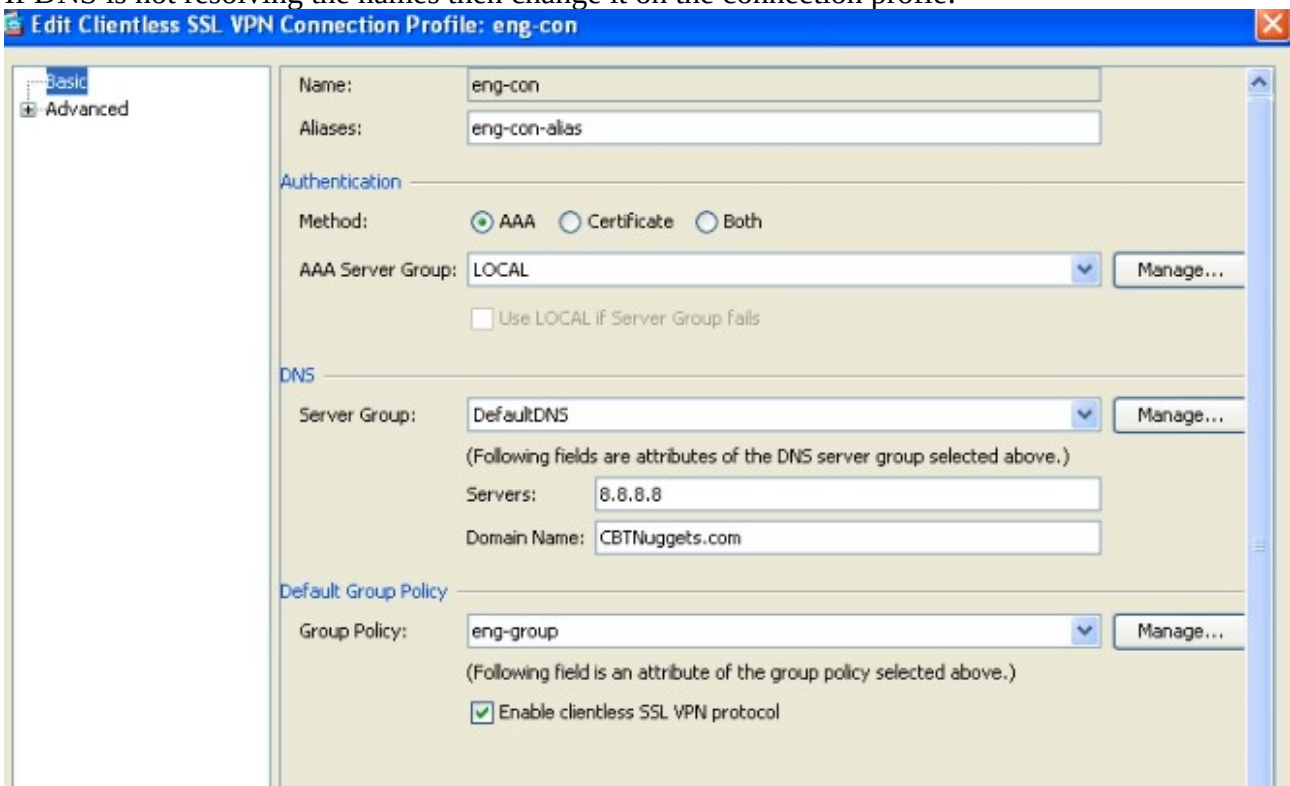
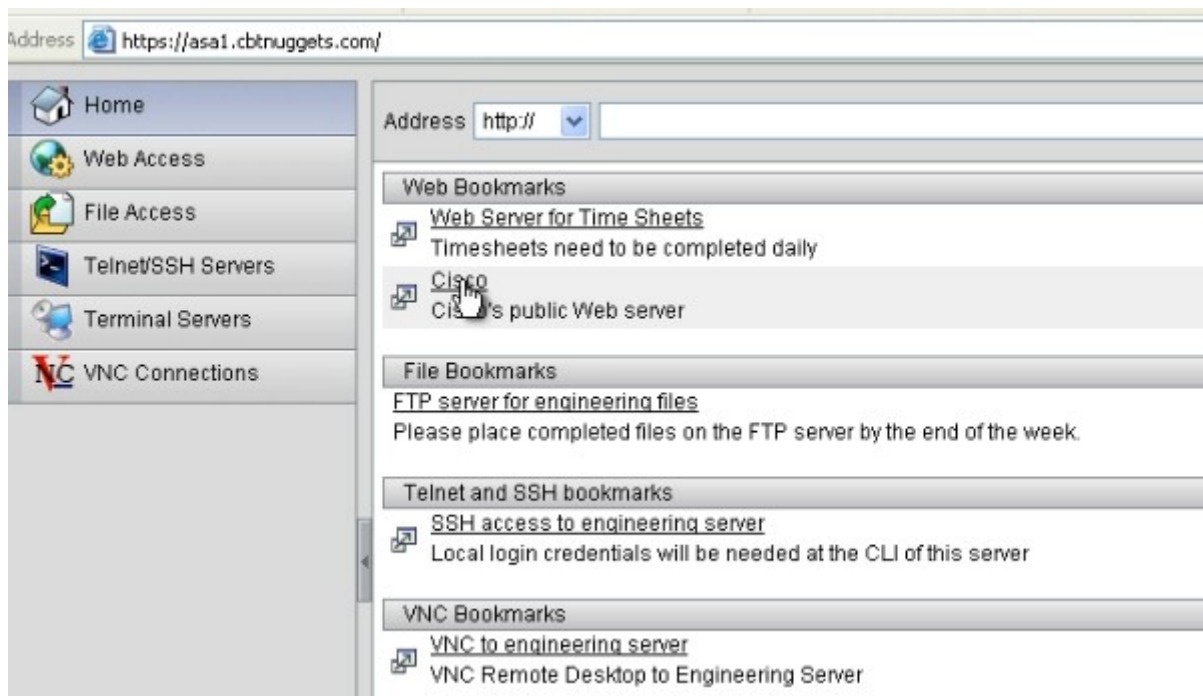Idle Alert Interval: ☑ Inherit ☐ Default [   ] minutes

Configure alert text messages and visual cues in Customization under Clientless SSL VPN Access-Portal-Customization-Edit-Portal Page-Timeout Alerts.
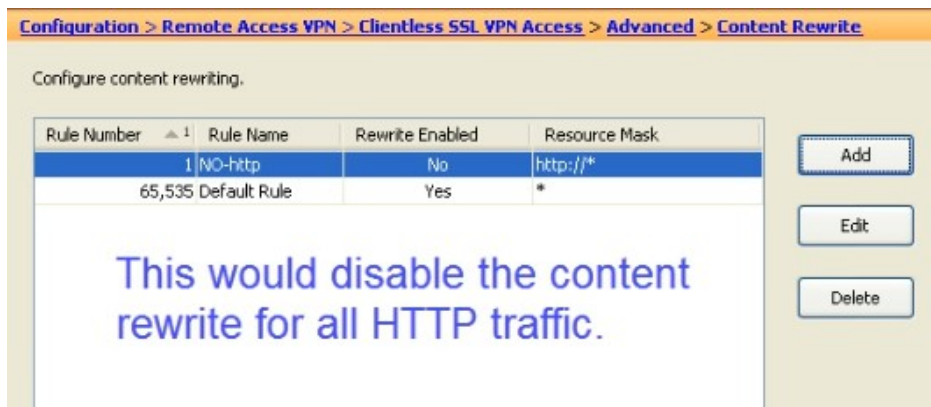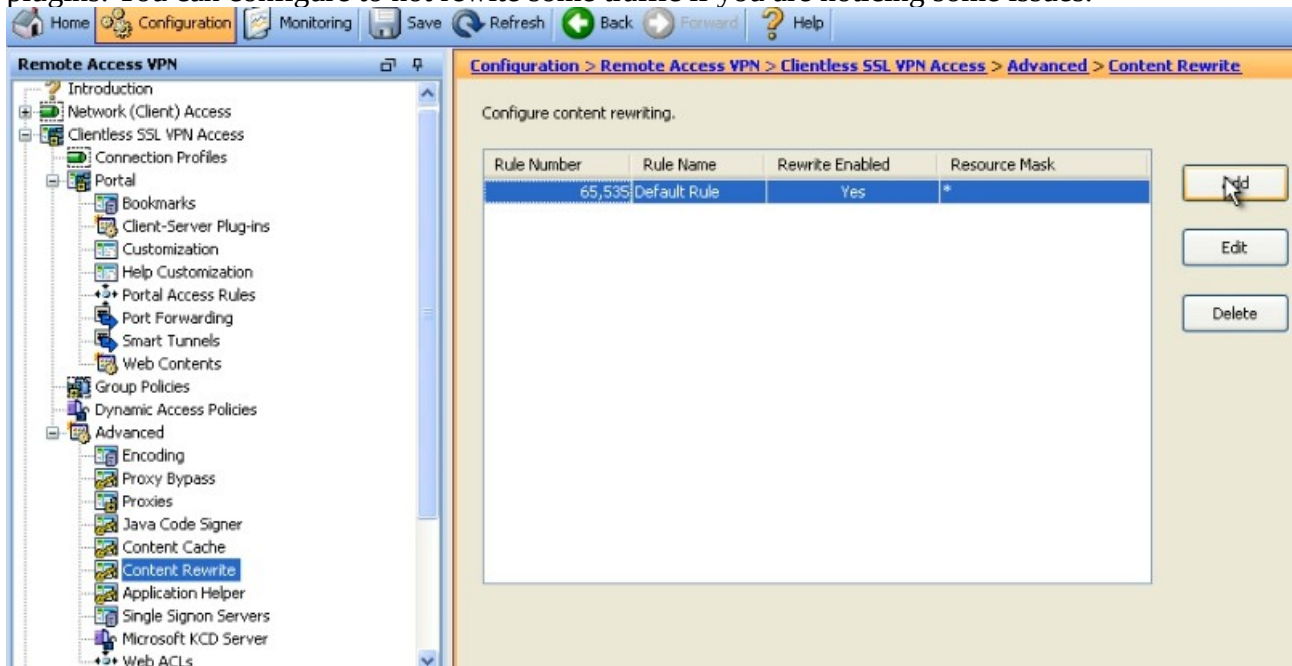
Remove WebType ACL and try it again.

If DNS is not resolving the names then change it on the connection profie:

Content Re-Write:
ASA is rewriting everything that goes through it for Clientless SSL which helps it to use the plugins. You can configure to not rewite some traffic if you are noticing some issues.

If random users are not able to connect to SSL VPN then you need to allow the algorithms. Keep it to default.
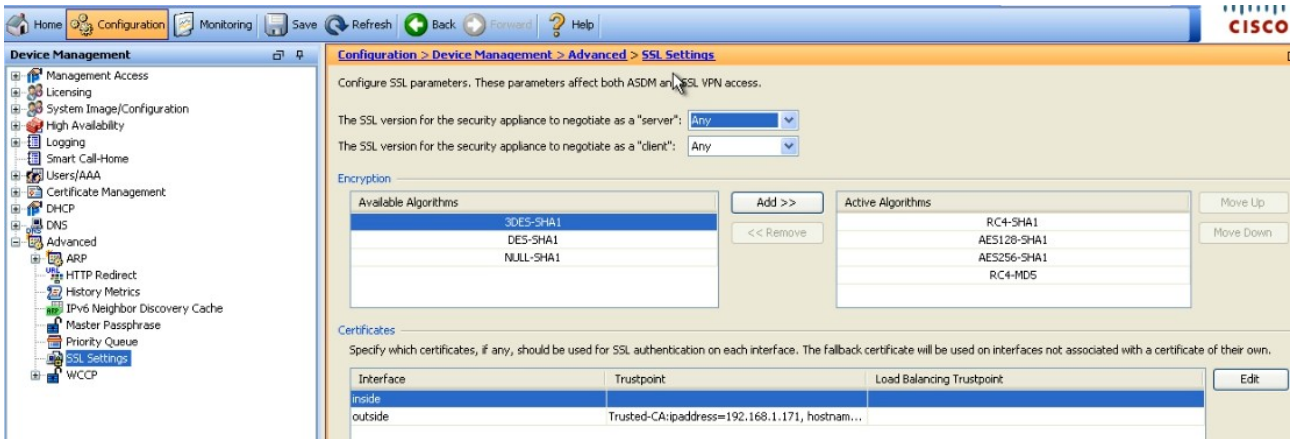
user will be associated it to its own group but the connection profile group policy inherited could cause problems, so we can lock it down to a specific connection profile.

Example using the wrong connection profile, and a valid username.

Edit User Account

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

Group Policy:	☐ Inherit	eng-group
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	eng-con
Store Password on Client System:	☑ Inherit	○ Yes ○ No

Connection Settings

Access Hours:	☑ Inherit	Manage
Simultaneous Logins:	☑ Inherit	
Maximum Connect Time:	☑ Inherit	☐ Unlimited ___ Minutes
Idle Timeout:	☑ Inherit	☐ Unlimited ___ Minutes

Dedicated IP Address (Optional)

IP Address: ___ Subnet Mask: ___

Always specify the right url:

Edit Clientless SSL VPN Connection Profile: eng-con

Login and Logout Page Customization: ___ Manage...

☐ 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
eng-con-alias	☑

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://asa1.cbtnuggets.com/engineering	☑

☐ 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.)