# **Configure and Deploy AnyConnect Web Security through ASA**

# Contents

Table of Contents
Introduction
Prerequisites
<u>Requirements</u>
Components used
Background Information
Configure
Anyconnect WebSecurity deployment through ASA
Verify
Upgrade/Downgrade Anyconnect version
Troubleshoot

### Introduction

This document describes the deploying of AnyConnect web security module for client based VPN terminating on Cisco Adaptive Security Appliances (ASA).

# Prerequisites

### Requirements

There are no specific requirements for this document.

### **Components used**

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## **Background Information**

• Upload the Anyconnect (recommend v4.1+) image on ASA



• Enable the VPN profile on ASA, as shown in the image

File View Tools Wizards Window He	elp					Type topic to search	Go	ahaha
Home 🖓 Configuration 🔯 Monitoring	Save	🚱 Refresh 🔇	Back OFForward	Help				cisco
Remote Access VPN	8 P P	Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles						
Introduction     Network (Client) Access     AnyConnect Connection Profiles     AnyConnect Customization/Localization     AnyConnect Client Profile     AnyConnect Client Software     Dynamic Access Policies     Group Policies     Group Policies     Disect(Kzv1) Connection Profiles	~	The security applia end-user administr Security (DTLS) tu Access Interfaces – Imable Cisco A SSL access must b	ance automatically depl ative rights. The Cisco nneling options. nyConnect VPN Client : e enabled if you allow /	oys the Cisco AnyConn AnyConnect VPN Client access on the interface AnyConnect client to be	ect VPN Client to remot supports IPsec (IKEv2 s selected in the table launched from a brow	te users upon connection. The initia 2) tunnel as well as SSL tunnel with below ser (Web Launch) .	il dient deploymen Datagram Transpi	t requires A
Secure Mobility Solution	=	Interface	SSL Access	[	IPsec (IKEv2) Acc	ess	Davice Co	rtificate
H → H Address Assignment		au desida	Allow Access	Enable DTLS	Allow Access	Enable Client Services	Device Ce	funcate
Advanced  Advan	~	outside inside Bypass interfa Access lists from g Login Page Setting - Allow user to s Shutdown port Connection Profiles Connection profile Connection profile Connection profile Connection profile	ce access lists for inbor roup policy and user pro- elect connection profile tal login page. t (tunnel group) specifi- here. t (incle group) Find:	und VPN sessions olicy always apply to the e on the login page.	e traffic.	eters. You can configure the mappi	Port Se	ttings ≣ e to
🛐 Firewall		Name	SSI. Enabled	IPsec Enabled	Aliases	Authentication Method	Group Poli	~
Remote Access VPN		DefaultRAGroup	✓		10000	AAA(LOCAL)	DfltGrpPoli	cy
Site-to-Site VPN		DefaultWEBVP	✓	✓		AAA(LOCAL)	DfltGrpPoli	У 🗸
Device Management		<						>
	>>				Apply Re:	set		

## Configure

### Anyconnect WebSecurity deployment through ASA

The steps involved in configuration are:

- Configure Anyconnect Websecurity client profile
- Edit Anyconnect VPN group policy
- Set split exclusion for Web Securityand select download Web Security client module
- Edit Anyconnect VPN group policy and select the Web Security client profile

#### Step 1. Configuring Anyconnect Websecurity Client profile

Navigate to Configuration >Remove Access VPN >Network (Client) Access >Anyconnect Client Profile, click on

**Note**: The Profile Name is hard-coded on the client side, so regardless of the name configured, the ASA always pushes out **Websecurity\_serviceprofile.wso** to the client.

**Note**: This is a default profile without authentication license key.

File View Tools Wizards Window Help							Туре
Home 🗞 Configuration 🔯 Monitoring 🔚 Save	e 💽 Refresh 🔇	Back 🔘 Fo	rward 🧖 Help				
Remote Access VPN 🗗 🖓	Configuration > R	Remote Acces	s VPN > Network	(Client) Access > AnyC	Connect Client Pro	<u>file</u>	
Introduction     Network (Client) Access     AnyConnect Connection Profiles     AnyConnect Customization/Localization     AnyConnect Client Profile     AnyConnect Client Software     Dynamic Access Policies     Group Policies     Dynamic Access	This panel is used 'Add' button to ad The profile Usage	to manage Any Id a new profile. field is introduc t	Connect Client Profi Pressing the Impor ed with the Secure I roup Policy	les and perform group assi t or Export button is for up Mobility Solution. This field ete The Import	ignment for AnyConn load and download o contains different pro t 🎒 Validate	ect version 2.5 or later.You c f dient profiles between local ffile usage in AnyConnect ver	an select a profile to machine and device. sion 3.0 and later.
B Secure Mobility Solution	Profile Name		Pr	ofile Usage		Group Policy	
Advanced	Pr Pr El au	rofile Name ( rofile Usage ) nter a device file utomatically created rofile Location (	Ac demo  Web Security Servic e path for an xml file ated if it does not ex disk0:/demo.wsp	d AnyConnect Clier e Profile ., ie. disk0:/ac_profile. The dist.	nt Profile	X Browse Flash Upload	
Device Setup     Device Setup     Firewall     Remote Access VPN	G	roup Policy	<unassigned></unassigned>	n VPN' for selected group			
Site-to-Site VPN			C	K Cancel	Help		

Step 2. Edit the newly created profile to add authentication license key and customize the configuration.



Cla Manu Tarah Minanda M	AnyConnect Client Profile Editor - demo	x
File View Tools Wizards W		
Home 🆓 Configuration	Profile: demo	About
Remote Access VPN	Web Security	
? Introduction	- Scanning Proxy Automatication	
Network (Client) Access	The Exceptions	~
AnyConnect Customization	Authentication Proxy Authentication License Key F90A686F696FF779CB758869F84A5688 ==	
AnyConnect Client Profile	Advanced Service Password unknown site	
AnyConnect Client Softwa	websecurry	
Group Policies	Enable Enterprise Domains     Use     Group Include List     V	
IPsec(IKEv1) Connection P	All Domains	
H- Address Assignment	Add	
🟦 🐻 Advanced	Add Delete	
Clientless SSL VPN Access     AAA/Local Users	Delete	
Host Scan Image		
Secure Desktop Manager		
- B Language Localization		_
Load Balancing		=
	Custom matching and reporting for machines not joined to domains	
⊞ - 🛃 Advanced	Computer Name	
	Computer Name	
	Custom Groups (optional)	
Cavica Catura	Add	
Device Setup	Delete	
Firewall		
Remote Access VPN		
🙀 Site-to-Site VPN	** change requires WebSecurity service restart	
Device Management		~
Device configuration loaded successfu	OK Cancel Help	



#### Step 3. Set split exclusion for Web Security and select download Web security client module

Edit Anyconnect VPN group policy, as shown in the image.



As shown in the image, set up split exclusion for Web Security.

<b>E</b>			Edit Internal Group Policy: DfltGrpPolicy
General	The VPN dient makes split tunneling decis	ions on the basis	s of a network list that can be specified below by providing the proper parameters to 'Policy
	DNS Names:		
Browser Proxy AnyConnect Client	Send All DNS Lookups Through Tunnel:	⊖Yes ●N	0
⊡ ·· IPsec(IKEv 1) Clien	t Policy:	Exclude Netwo	vrk List Below
	IPv6 Policy:	Exclude Netwo	vrk List Below
	Network List:	None	
	Pressing this button to set up split exlusion	on for Web Secu	rity proxies.
	Set up Split Exclusion for Web Securit	y	Web Security Proxies Exclusion
	Intercept DHCP Configuration Message	from Microsoft (	Enter a new or select an existing access list used for Web Security split exclusion. ASDM will set up the access list for use in the network list.         Access list name:       CWS-Tower         Create Access List       Update Access List       Cancel

6		Edit Internal Group Policy: DfltGrpPolicy
General Servers Advanced Split Tunneling Browser Proxy Browser Proxy Browser View (IKEv 1) Client	The VPN client makes split tunneling decises DNS Names: Send All DNS Lookups Through Tunnel: Policy: IPv6 Policy: Network List: Pressing this button to set up split exlusion Set up Split Exclusion for Web Securit Intercept DHCP Configuration Message	sions on the basis of a network list that can be specified below by providing the proper par Yes  No Exclude Network List Below Exclude Network List Below CWS-Tower on for Web Security proxies.

Select download Web Security client module, as shown in the image.

Step 4. Download Web security client profile

Edit **Anyconnect VPN group policy > Client Profiles to Download > Add,** now choose the created Profile (as in Step 1)

General	Keep Installer on Client System:	Yes   No	
Servers	heep instance on electro jacom	0.00	
Advanced	Datagram Transport Layer Security (DTLS):	Enable      Disat	de la constante
-Split Tunneling			
-Browser Proxy	DTLS Compression:	Enable      Disat	ke la
AnyConnect Client Login Setting	SSL Compression:	○ Deflate ○ LZS	Oisable
- Client Firewall - Key Regeneration	Ignore Don't Fragment(DF) Bit:	○ Enable	le
-Dead Peer Detectio	Client Bypass Protocol:	🔿 Enable 💿 Disab	Ne la
	FQDN of This Device:		
IPsec(IKEv1) Client	MTU:	1406	
	Keepalive Messages:	Disable Interval	Select AnyConnect Client Profiles
	Optional Client Modules to Download:	websecurity	This panel is used to select existing AnyConnect profile for a group policy. To create or edit a profile, go to Remote
	Always-On VPN:	O Disable 💿 Use	Access VPN>Network (Client) Access>AnyConnect Client Profile.
			Select a profile name and the usage will be determined automatically. The 'View Profile' hutton will open the profile
	Client Profiles to Download:		viewer (no editing) if the AnyConnect 2.5 client or later is installed and if the profile usage is determined.
		💠 Add 🏢 Delete	Otherwise, it will show the profile content as XML text.
		Profile Name	Profile Name: demo
			Profile Usage: Web Security Service Profile V
			OK Cancel Help
		L	
<			
Find:	Next O Previous	;	
			OK Cancel Help

Click OK and apply the changes.

# Verify

When you connect to Anyconnect VPN, ASA will push the Anyconnect webscurity module through VPN as shown in the image.

S Cisco AnyConnect   10.106.36.30	S Cisco AnyConnect Secure Mobility Client ×
Username: user1 Password: *******	VPN:           Contacting 10.106.36.30.           10.106.36.30
OK Cancel	ijialbi Cisco



If you are already logged in, its recommended to log off and then log in back for the functionality to be enabled.

## **Upgrade/Downgrade Anyconnect version**

The deployment functionality remains unaltered if the version is upgraded. However, downgrade is not possible. So, with the current example of 4.1.x, it can be upgraded to version 4.2

The steps involved are as follows:

#### Step 1. Upload the latest Anyconnect package 4.2 to flash and replace 4.1 with latest file.

Under Anyconnect Client Software > Replace, and then choose the recent image file.

File       View       Tople       Type to         Image: Second process       Image: Second proces       Image: Second proces
Home Configuration Monitoring Save Refresh Sake Forward P Help
Remote Access VPN Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Software
<ul> <li>Introduction</li> <li>Network (Client) Access</li> <li>AnyConnect Connection Profiles</li> <li>AnyConnect Client Images</li> <li>Cisco AnyConnect Client packages can be downloaded from the Cisco Web using the search string 'AnyConnect Client Profile</li> <li>AnyConnect Client Profile</li> <li>AnyConnect Client Software</li> <li>Dynamic Access Policies</li> </ul>
Group Policies
IPsec(IKEv1) Connection Profiles
Secure Mobility Solution disk0:/anyconnect-win-4.1.08005-k9.pkg
Beplace AnyConnect Client Image
Advanced
Clientless SSL VPN Access
AAA/Local Users AnyConnect Image: disk0:/anyconnect-win-4.2.01035-K9.pkg Browse Hash
Host Scan Image
Brown Manager
Certificate Management Regular expression to match user-agent 😵
Ingliage Localization
Load Balancing OK Cancel Help
THE Perver
BNS Contraction of the second se

Step 2. When you re-connect to Anyconnect VPN, ASA will push the latest Anyconnect module through VPN with no alterations to the web security profile.

Cisco AnyConnect Secure Mobility Client
VPN:Exiting. Upgrade in progress.10.106.36.30Connect
Web Security: Enabled (India)
🗘 🛈
CISCO
AnyConnect Secure Mobility Client Downloader
The AnyConnect Downloader is installing AnyConnect Secure Mobility Client 4.2.01035. Please wait

**Note**: Downgrade is not supported.

### Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Using DART to Gather Troubleshooting Information:

DART is the AnyConnect Diagnostics and Reporting Tool that you can use to collect data useful for troubleshooting AnyConnect installation and connection problems. DART supports Windows 7, Windows

Vista, Windows XP, Mac version 10.5 and 10.6, and Linux Redhat. The DART wizard runs on the computer that runs AnyConnect. It assembles the logs, status, and diagnostic information for Cisco Technical Assistance Center (TAC) analysis and does not require administrator privileges.

Although DART does not rely on any component of the AnyConnect software to run, yet you can launch it from AnyConnect, it will collect the AnyConnect log file, if it is available. Currently, DART is available as a standalone installation, or the administrator can push this application to the client PC as part of the AnyConnect dynamic download infrastructure. Once installed, the end user can start the wizard from the Cisco folder available through the **Start** button.