Configure AnyConnect with LDAP Authentication on CSM

Contents

Introduction Prerequisites Requirements Components Used Configure Network Diagram Configurations Step 1. Configure the SSLVPN Access Step 2. Configure the Authentication Server Step 3. Configure the Connection Profile Step 4. Deploy Verify Troubleshoot

Introduction

This document describes how to configure AnyConnect with LDAP Authentication on CSM.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- CSM 4.23
- AnyConnect configuration
- SSL protocol

Components Used

The information in this document is based on these software and hardware versions:

- CSM 4.23
- ASA 5515
- AnyConnect 4.10.6090

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, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Configurations

Step 1. Configure the SSLVPN Access

Go to Policies > SSL VPN > Access:

Devices	• 9	Device: rtp-asa-csm.rtpvpn Policy Assigned: local			Polic) Assis	Access and Toplaced d	evice
Filter I none V		Torry Hong ton			i i i i i i i i i i i i i i i i i i i	ALCO TOT BOLIELS	ALMA .
(a) Department		Interface	Allow Access		Enable DTLS		Trustpoint
Location Construction Constr							
Policies							
Frewal Frewal Gate Rules (Unified) Gate Rules (Unified) Gate Rules (Unified)		ServerfiameIndication:		Add Access Interface		×	
Botnet Traffic Filter Rules		Domain Mask		Access Interface:*	outside Select		
Settings Transparent Rules				Trustpoint:	rtpvpnase Select		
Web Filter Rules NAT				Load Balancing Trustpoints	Select		
Site to Site WN					Allow Access		
- Configuration Wizard					C Enable Dita		
- 🗐 ASA Cluster Load Balance - 🗐 Connection Profiles					OK Cancel H	wb div	
Dynamic Access Gobal Settings							
🗐 Group Policies							
- I Trusted Pool							
Username From Cert Scripts		Port Number:*	443 Select				
B PSec VPN		DTLS Port Number:	443 Select				
		Falbeck Trustpoint:	Select				
Other Settings		Default Idle Timeout:*	1800 sec (60-	86-400)			
in the shared License		Max Session Limit:					

After configuring the Access Interface make sure you click Save:



Step 2. Configure the Authentication Server

Go to Policy **Object Manager > All Object Types > AAA Servers > Add**.

Configure the IP of the server, the source interface, Login Directory, Login Password, LDAP Hierarchy Location, LDAP Scope and LDAP Distinguished Name:

iii Edit A	AA Server			
Name:*	AD_rtp			
Description:				
Host:	v6 Address * 172.18.12	14.73 Select Interface:	outside	Select
O DNS Na	me (PIX7.2,ASA7.2)	Timeout:		
Drotocoli	ldan vi			
Protocol:	idap 🗸			
		Enable LDAP over SSL/Secure Communication	No Negotiation	
	Server Port:	389		Ldap-login-dn
	Login Directory:	CN=Administrator,CN=Users,DC=rtpvpn,DC=local		
	Login Password:	•••••		
		Encrypted (IOS)		
	LDAP Hierarchy Location:	DC=rtpvpn,DC=local		Ldap-base-dn
	PIX/ASA/FWSM IOS			
	LDAP Scope:	subtree	~	
	LDAP Distinguished Name:	sAMAccountName	>	Ldap-naming-a
		SASL MD5 Authentication		
		SASL Kerberos Authentication		
Category:	~			
			ОК	Cancel

Now add the AAA Server to **AAA Server Groups** > **Add**.

Edit AAA Server Group

Name:*	AD_LDAP
Description:	\$
Destaural	lden vi
Protocol:	idap 🗸
AAA Servers:	AD_rtp \$Select
	Make this Group the Default AAA Server Group (IOS)
	AD Agent Mode (ASA 8.4(2)+)
Dynamic Authorization Port:	1700 (1024-65535)
Interim Account Update Interval:	24 (1-120)
Authorize only	
Max Failed Attempts (PIX,ASA,FWSM):	3
Reactivation Mode (PIX7.x,ASA,FWSM):	depletion \checkmark
Reactivation Deadtime (PIX,ASA,FWSM):	10
Group Accounting Mode (PIX7.x,ASA,FWSM):	single \lor
Category	
catego y.	Allow Value Override per Device
	Overrides: None Edit
	OK Cancel Help
	Cancer Help

Step 3. Configure the Connection Profile

Go to **Policies > Connection Profiles > Add**.

Here you have to configure the **IPv4 Global Address Pool** (**AnyConnect pool**), **Group Policy**, **AAA and Group Alias/URL**:

		-					
Devices	†		5	Connection Profiles			
Filter : none V			۳.	Connection Fromes			
			н	General AAA Secondar		C C C C C C C C C C C C C C C C C C C	
Department			н		y AAA P Sec	332	
			н	Connection Profile Name:* CS	SM_LDAP_SVC		
			н	Group Policy:	unic Dolicy	Calact	
Se character church			н	Group Policy.	asic_roncy	Secur	
Se i these carrier thin i			н	Client Address Assignment			
			н				
			н				
			н	DHCP Servers:			
			н				
			н				
Policies			н		anyconnect_p	loo	
		11	н	IPv4 Global Address Pool:			
-Firewal	^		н				
AAA Rules (Unified)			н				
Access Rules (Unified)			н				
-) Inspection Rules (Unified)			4	The of the ball to the second			
Bothet Tramc Hiter Rules			н	IPV6 Global Address Pool:			
H-settings		LP-					
Web Elter Dules			F				
		Ш.				-	
Gite to Site VPN		Ш.		Interface-Specific Address	Pools(IPv4/IPv	6)	
- Remote Access VPN		Ш.		Interface	IPv4	Address Pool	IPv6 Address
Configuration Wizard		Ш.					
ASA Cluster Load Balance		Ш.					
Connection Profiles		Ш.					
- J Dynamic Access							
- 🗐 Global Settings							
- Group Policies							
- 🗐 Trusted Pool							
- Subservame From Cert Scripts							
Certificate To Connection Profile Maps							
IPSec VPN							OK Car
SSL VPN							Cur
	~		1				

In order to select the AAA server, click on the **AAA** tab and select the server created on Step 2:

Connection Profiles	\times
General AAA Secondary AAA IPSec SSL	
Authentication Method: AAA	
Authentication Server Group: AD_LDAP Select	
Use LOCAL if Server Group Fails	
Authorization Server Group: Select	
Users must exist in the authorization database to connect	
Accounting Server Group: Select	
Strip Realm from Username	
Override Account-Disabled Indication from AAA Server ¹	
Enable Notification Upon Password Expiration to Allow User to Change Password ¹	
Enable Notification Prior to Expiration Notify Prior to Expiration:	days
Distinguished Name(DN) Authorization Settings	
Use the Entire DN as the Username	
Specify Individual DN Fields as the Username	
Primary DN Field: CN (Common Name) 🗸	
Secondary DN Field: OU (Organization Unit) $$	
Use script to select Username	
Select Script:	
Interface-Specific Authentication Server Groups	
Interface Server Group Use Fallback	
OK Cancel	Help

To configure a group alias/group url, dns or wins server in the connection profile, go to the SSL tab:

Connection Profiles

WINS Servers List: ONS Group: Portal Page Customization:	DefaultDNS	Select				
SAML Identity Provider:		Select				
	Override SVC	Download ¹ Message ¹				
Connection Aliases		Group URLs				
Alias	Status	URL	Status			
	• / =		+ / I			
	• / 9	Disable CSD ²	• 2 1			
Default Citrix Client Profil	 2 2 	Disable CSD ² Both Clientless and Anyco	mnect			
Default Citrix Client Profil	• 🖉 🖀	Disable CSD ² Both Clientless and Anyco Anyconnect only	mnect			
Default Citrix Client Profil	• 🖉 🖀	Disable CSD ² Both Clientless and Anyco Anyconnect only	mnect			
Default Citrix Client Profil		Disable CSD ² Both Clientless and Anyco Anyconnect only	mnect			

Step 4. Deploy

Click the deploy icon .

Verify

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

Accessing through CSM:

Open the Health and Performance Monitor > Tools > Device Selector > Select the ASA > Next > Select Remote Access Users

 \times

🐻 Cisco Security Manager - Health and Performance Monitor - admin Connected to '

File Launch Tools Help										
💽 Monitoring 🔔 Alerts 🍓 🍪	4 🛱 🍓 🗶 1 🕜									
Views-	Monitoring									
Views	👷 Priority Devices 🔒	Remote Access	Users ×							
Remote Access Users	Q- S	Q-S 🕐 Export -								
Site-to-Site Tunnels	Receive Time	User Name 🛛 🗸	User Group Policy \sim	Firewall Name 🛛 🗸	Assigned IP \sim	Public IP 🛛 🗸	Duration			
- B VPN Summary - Priority Devices	Tue Jul 25 00:12:10 EDT 2023	cisco	Basic_Policy	S rtpvpn∙asa	192.168.112.104		0h:02m:4			
- IPS Devices										
All Devices										

Note: The VPN user shows up based on the HPM refresh timer.

Through CLI:

```
ASA#show vpn-sessiondb anyconnect
Session Type: AnyConnect
Username : cisco
                                        Index : 23719
Assigned IP : 192.168.20.1
                                        Public IP : 209.165.201.25
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx : 15856
                                        Bytes Rx : 3545
Group Policy : Basic Policy
                                        Tunnel Group : CSM LDAP SVC
Login Time : 10:29:42 UTC Tue Jul 25 2023
Duration : 0h:010m:16s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                        VLAN : none
Audt Sess ID : 0e26864905ca700064bf3396
Security Grp : none
```

Troubleshoot

In order to check possible failures during the LDAP authentication or the anyconnect establishment you can execute the next commands on the CLI:

<#root> debug ldap 255 debug webvpn anyconnect 255