使用ISE终端安全评估将Duo SAML SSO与 Anyconnect安全远程访问集成

目录			
<u>简介</u>			
<u>先决条件</u>			
<u>要求</u>			
<u>使用的组件</u>			
<u>配置</u>			
<u>网络图</u>			
<u>流量传输</u>			
<u>配置</u>			
<u>- Duo管理员门</u>	<u>户配置</u>		
<u>- Duo接入网关</u>	<u>(DAG)配置</u>		
<u>-ASA 配置</u>			
<u>-ISE 配置</u>			
<u>验证</u>			
<u>用户体验</u>			
<u>故障排除</u>			
<u>相关信息</u>			

简介

本文档介绍将Duo SAML SSO与利用思科ISE进行详细状态评估的自适应安全设备(ASA)Cisco AnyConnect安全移动客户端访问相集成的配置示例。双核SAML SSO使用双核接入网关(DAG)实施 ,该网关与Active Directory通信以进行初始用户身份验证,然后与双核安全(云)通信以进行多重 身份验证。思科ISE用作授权服务器,使用状况评估提供终端验证。

作者:Dinesh Moudgil和Pulkit Saxena, Cisco HTTS工程师。

先决条件

要求

本文档假设ASA完全运行且配置为允许思科自适应安全设备管理器(ASDM)或命令行界面(CLI)进行 配置更改。

Cisco 建议您了解以下主题:

- Duo接入网关和Duo安全基础知识
- ASA上远程访问VPN配置的基本知识
- ISE和状态服务基础知识

使用的组件

本文档中的信息基于以下软件版本:

- 思科自适应安全设备软件版本9.12(3)12
- Duo接入网关
- Duo安全
- 思科身份服务引擎2.6版及更高版本
- Microsoft Windows 10与AnyConnect版本4.8.03052

◆ 注意:此实施中使用的Anyconnect嵌入式浏览器要求每个版本的9.7(1)24、9.8(2)28、 9.9(2)1或更高版本以及AnyConnect版本4.6或更高版本ASA。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

配置

网络图



- 1. Anyconnect客户端发起到Cisco ASA的SSL VPN连接
- Cisco ASA配置为使用双协议访问网关(DAG)进行主要身份验证,将Anyconnect客户端中的嵌入式浏览器重定向到DAG进行SAML身份验证
- 3. Anyconnect客户端被重定向到Duo接入网关
- 4. AnyConnect客户端输入凭证后,会建立SAML身份验证请求,并从Cisco ASA发送到Duo访问 网关
- 5. Duo 接入网关利用与现场Active Directory的集成来执行Anyconnect客户端的主要身份验证
- 6. 主身份验证成功后,Duo接入网关向Duo Security over TCP端口443发送请求以开始双因素身 份验证
- 7. AnyConnect客户端已显示"Duo Interactive Prompt",用户使用其首选方法(推送或密码)完成双因素身份验证
- 8. Duo Security收到身份验证响应并将信息返回到Duo接入网关
- 9. Duo接入网关根据身份验证响应构建SAML身份验证响应,其中包含SAML断言并响应 Anyconnect客户端
- 10. Anyconnect客户端成功通过与Cisco ASA的SSL VPN连接的身份验证
- 11. 身份验证成功后,Cisco ASA向Cisco ISE发送授权请求

注意:Cisco ISE仅为授权配置,因为Duo Access Gateway提供必需的身份验证

- 12. 思科ISE处理授权请求,并且由于客户端状态未知,通过思科ASA有限访问Anyconnect客户端 返回状态重定向
- 13. 如果Anyconnect客户端没有合规性模块,系统会提示其下载以进行进一步的安全状态评估
- 14. 如果Anyconnect客户端具有合规性模块,则会与Cisco ASA建立TLS连接,并启动安全评估流 程
- 15. 根据ISE上配置的终端安全评估条件,完成终端安全评估检查,并将详细信息从Anyconnect客 户端发送到思科ISE
- 16. 如果客户端状态从Unknown更改为Compliant,则授权更改(CoA)请求从Cisco ISE发送到 Cisco ASA以授予客户端完全访问权限和VPN完全建立

配置

- Duo管理员门户配置

在本节中,在Duo Admin Portal上配置ASA应用。

1.登录"Duo Admin Portal"并导航至"Applications > Protect an Application",搜索保护类型为"2FA with Duo Access Gateway, self-hosted"的"ASA"。点击最右边的"保护"以配置Cisco ASA



2.为受保护的应用ASA在"服务提供商"下配置以下属性

基本URL	firebird.cisco.com	
隧道组	TG_SAML	
邮件属性	sAMAccountName,mail	

点击页面底部的"保存"

Device Insight Policies	Cisco ASA - Duo Access Gateway Authentication Log				
Applications Protect an Application	Configure Cisco ASA				
Single Sign-On Users	To set up this application, Next step: Download your	install the Duo Access Gateway and then configure your service provider. View Cisco ASA SAML SSO instructions ⊠ configuration file			
Groups Endpoints	Service Provider				
2FA Devices Administrators Reports	Base URL	firebird.cisco.com Enter the Cisco ASA Base URL.			
Settings Billing	Tunnel Group	TG_SAML Enter the Tunnel Group you are protecting with SSO.			
Need Help? Chat with Tech Support C Email Support Call us at 1-855-386-2884	Custom attributes	Use this setting if your Duo Access Gateway authentication source uses non-standard attribute names.			
Account ID 2010-1403-48	Mail attribute	sAMAccountName,mail			
Deployment ID DUO57 C		The attribute containing the email address of the user.			
Helpful Links Documentation 더		Save Configuration			

在本文档中,其余配置使用默认参数,但可以根据客户要求进行设置。

此时可以为新SAML应用调整其他设置,例如从默认值更改应用的名称、启用自助服务或分配组策 略。

3.单击"下载配置文件"链接获取Cisco ASA应用设置(作为JSON文件)。此文件将在后续步骤中上 传到Duo接入网关

Device Insight	Cisco ASA - Duo Access Gateway			
Policies	CISCO ASA - DUO ACCESS Galeway			
Applications	Configure Cisco ASA			
Protect an Application	g			
Single Sign-On	To set up this application, ins	stall the Duo Access Gateway and then configure your service provider. View Cisco ASA SAML SSO instructions		
Users	Next step: Download your co	onfiguration file		
Groups				
Endpoints	Service Provider			
2FA Devices				
Administrators	Base URL	firebird.cisco.com		
Reports		Enter the Cisco ASA Base URL.		
Settings				
Billing	Tunnel Group	TG_SAML		
		Enter the Tunnel Group you are protecting with SSO.		
Need Help?				
Email Support	Custom attributes	Use this setting if your Duo Access Gateway authentication source uses non-standard attribute names.		
Call us at 1-855-386-2884				
Account ID	Mail attribute	sAMAccountName,mail		
Deployment ID		The attribute containing the email address of the user.		
DU057 C				
Helpful Links		Ourse Operformation		
Documentation L3		Save configuration		

4.在Dashboard > Applications下,新创建的ASA应用如下图所示:

admin-77d04ebc.duosecurity.co	m/applications				☆		0
🗎 Cisco Study 🗎 Cisco Tools	Mix 🗃 SourceFire 🗎 VPN 🗎 AAA	🗎 ASA 📋 IFT 6.7					
DUO	 Search for users, groups, applications, 	or devices		O Cisco ID: 2010-1403-48	ciscoduoblr	~	
Dashboard	Dashboard > Applications						
Device Insight	Anneliantiana						
Policies	Applications			SSO Setup Guide Ľ Protect an	Application		
Applications							
Protect an Application				Export V Q Search			
Single Sign-On							
Users	Name 🔺	Туре	Application Policy	Group Policies			
Groups	Cisco ASA - Duo Access Gateway	Cisco ASA - Duo Access Gateway					
Endpoints							
2FA Devices	1 total						

5.导航至"用户>添加用户",如图所示:

创建名为"duouser"的用户以用于Anyconnect远程访问身份验证,并在最终用户设备上激活Duo Mobile

DII O	۹ Search for users, groups,	applications, or devices		
Dashboard	Dashboard > Users > Add Us	er		
Device Insight	Add User			
Policies	Adding Users			
Applications	Most applications allow us	sers to enroll themselves after they complete primary authentication.		
Users	Learn more about adding	users 🖸		
Add User				
Pending Enrollments				
Bulk Enroll Users	Username	duouser		
Directory Sync		Should match the primary authentication username.		
Bypass Codes				
Groups				
Endpoints		Add User		

要添加图中所示的电话号码,请选择"添加电话"选项。



为特定用户激活"Duo Mobile"

Device Info

Learn more about Activating Duo Mobile 1.



◆ 注:确保在最终用户设备上安装"Duo Mobile"。 <u>手动安装IOS设备Duo应用程序</u> <u>手动安装适用于Android设备的Duo应用程序</u>

选择"Generate Duo Mobile Activation Code",如图所示:

DU	Q Search for users, groups, applications, or devices ciscoduoblr v
Dashboard Device Insight Policies Applications	Dashboard > Phone: > Activate Duo Mobile Activate Duo Mobile Activate Duo Mobile This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.
Users Groups Endpoints 250 Devices	Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.
Phones Hardware Tokens WebAuthn & U2F	Expiration 24 hours v after generation
Administrators Reports Settings	Generate Duo Mobile Activation Code

选择"Send Instructions by SMS"(通过SMS发送说明),如图所示:

Dashboard	Dashboard > Phone: +91	> Activate Duo Mobile		
Device Insight	Activate Du	vo Mobilo		
Policies	Activate Duo Mobile			
Applications	A new Duo Mobile activation code has been generated, and any old credentials have been invalidated.			
Users		ie user by Sivis.		
Groups	Phone			
Endpoints				
2FA Devices	Installation instructions	Send installation instructions via SMS		
Phones		Welcome to Duo! Please install Duo Mobile from your app		
Hardware Tokens		store.		
WebAuthn & U2F				
Administrators		li li		
Reports				
Settings	Activation instructions	Send activation instructions via SMS		
Billing		To activate the app, tap and open this link with Duo Mobile: https://m-		
		77d04ebc.duosecurity.com/activate/YB5ucEisJAq1YIBN5ZrT		
Need Help?		4		
Email Support				
Call us at 1-855- <u>386-2884</u>		Send Instructions by SMS or skin this step		

点击SMS中的链接,Duo应用将链接到"设备信息"部分中的用户帐户,如图所示:



- Duo接入网关(DAG)配置
 - 1. 在网络中的服务器上部署Duo访问网关(DAG)

💊 注意:请遵循以下文档进行部署:

用于Linux的双核接入网关 https://duo.com/docs/dag-linux

用于Windows的双核接入网关 https://duo.com/docs/dag-windows

- 2. 在Duo Access Gateway主页上,导航至"Authentication Source"
- 3. 在"Configure Sources"下,输入您的Active Directory的以下属性,然后单击"Save Settings"

Configure Sources

Configure authentication	n source settings below. Changes made to non-active authentication sources will take effect when made active.
Source type	Active Directory Specify the authentication source to configure.
Status:	 LDAP Bind Succeeded Idap://10.197.243.110
Server	10.197. 389 Hostname and port of your Active Directory. The port is typically 389 for cleartext LDAP and STARTTLS, and 636 for LDAPS. Hostnames can be comma separated for failover functionality. For example: ad1.server.com, ad2.server.com, 10.1.10.150
Transport type	CLEAR LDAPS STARTTLS This setting controls whether the communication between Active Directory and the Duo Access Gateway is encrypted.
Attributes	SAMAccountName,mail Specify attributes to retrieve from the AD server. For example: sAMAccountName,mail.
Search base	CN=Users,DC=dmoudgil,DC=local The DNs which will be used as a base for the search. Enter one per line. They will be searched in the order given.
Search attributes	SAMAccountName Specify attributes the username should match against. For example: sAMAccountName,mail.
Search username	iseadmin The username of an account that has permission to read from your Active Directory. We recommend creating a service account that has read-only access.
Search password	The password corresponding to the search username specified above.
	Save Settings

4. 在"Set Active Source"下,选择源类型为"Active Directory",然后单击"Set Active Source"

S	Set Active Source		
Specify the source that end-users will use for primary authentication.			
Source type		Active Directory	
		Set Active Source	

5. 导航至"Applications",在"Add Application"子菜单下上传从"Configuration file"部分的Duo Admin Console下载的.json文件。相应的.json文件已在步骤3的Duo Admin Portal Configuration下下载

Applications

Add Application

Create a SAML application in the Duo Admin Panel. Then, download the provided configuration file and upload it here.			
Configuration file	Browse Cisco ASA - Duo Access Gateway.json		
	Upload		

6. 成功添加应用后,它将显示在"应用"(Applications)子菜单下

Applications					
Name	Туре	Logo			
Cisco ASA - Duo Access Gateway	Cisco ASA	dialo cisco	Delete		

- 7. 在"元数据"(Metadata)子菜单下,下载XML元数据和IdP证书,并记下随后在ASA上配置的以下 URL
 - 1. SSO URL
 - 2. 注销URL
 - 3. 实体Id
 - 4. 错误Url

Metadata		Recreate Certificate
Information for configuri	g applications with Duo Access Gateway. Download XML metadata.	
Certifica Expiratio SHA-1 Fingerpri SHA-256 Fingerpri	te /C=US/ST=MI/L=Ann Arbor/O=Duo Security, Inc. Download certificate	_
SSO UF Logout UF Entity Error UF	<pre>L https://explorer.cisco.com/dag/saml2/idp/SSOService.php L https://explorer.cisco.com/dag/saml2/idp/SingleLogoutSer D https://explorer.cisco.com/dag/saml2/idp/metadata.php L https://explorer.cisco.com/dag/module.php/duosecurity/du</pre>	

-ASA 配置

本节提供有关为SAML IDP身份验证和基本AnyConnect配置配置ASA的信息。本文档提供概述的 ASDM配置步骤和CLI运行配置。

1.上传Duo接入网关证书

A.导航到"Configuration > Device Management > Certificate Management > CA Certificates",然后 单击"Add"

B.在"安装证书页面"上,配置信任点名称:Duo_Access_Gateway

C.单击"浏览"选择与DAG证书关联的路径,选择后,单击"安装证书"

	Cisco ASDM 7.12	2(2) for ASA - 10.197.164.3		
Home 🚳 Configuration 📴 Monitoring	🔚 Save 🔇 Refresh 🔇 Bacl	k 🕐 Forward 🧳 Help Type topi	c Go	
O O Device Management	○ ○ ○ <u>Configuration > Devi</u>	ce Management > Certificate Man	agement > <u>CA Certificates</u>	
 Management Access Licensing System Image/Configuration High Availability and Scalability Logging Smart Call-Home Cloud Web Security Users/AAA Certificate Management Certificates CA Certificates CA Certificates DHCP DNS REST API Agent Advanced 	Trustpoint Name: Du Install from a file: //U Paste certificate in PEM	Install Certificate	Browse	uils RL
	Use SCEP: Specify source Interface SCEP URL: http:// Retry Period: Retry Count:	2: None 1 0	 minutes (Use 0 to indicate unlimited retries) 	
Device Setup Firewall			More Options	l
Remote Access VPN	Hel	p Cancel	Install Certificate	
Site-to-Site VPN				
Device <u>M</u> anagement		Reset Ap	ply	

2.为AnyConnect用户创建IP本地池

导航到"Configuration > Remote Access VPN > Network(Client)Access > Address Assignment > Address Pools",单击"Add"

			Cisco ASDM 7.12(2) for ASA - 10.197.164.3	
	Home	Configuration 🧾 Monitoring 🖡] Save 🔇 Refresh 🔇 Back 🚫 Forward 🤗 Help Type topic Go	cisco
4	00	Remote Access VPN	CONTINUES ACCESS VPN > Network (Client) Access > Address Assignment	> <u>Address</u>
Bookmarks Device List		Remote Access VPN Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Client Software AnyConnect Client Software Dynamic Access Policies Group Policies IPsec(IKEv1) Connection Profiles IPsec(IKEv2) Connection Profiles Secure Mobility Solution Address Pools Advanced Clientless SSL VPN Access AAA/Local Users Secure Desktop Manager Certificate Management Load Balancing DHCP Server DNS	Configuration > Remote Access VPN > Network (Client) Access > Address Assignment Pools Configure named IP Address Pools. The IP Address Pools can be used in either a VPN IPsec(IKEv1) C Profiles, AnyConnect Connection Profiles, Group Policies configuration Add IPv4 Pool met Mask/Prefix L Starting IP Address: 10.197.164.6 Inding IP Address: 10.197.164.7 Subnet Mask: 255.255.0 VHE Help Cancel OK	> Address ionnection ength
		Device Management	Reset Apply	
		· ·		

3.配置AAA服务器组

A.在本节中,配置AAA服务器组并提供执行授权的特定AAA服务器的详细信息

B.导航到"Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups",点击 "Add"

) Home 🦓 Configuration 🧭 Monitoring	g 🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help Type topic Go	cisco
L.	O O O Remote Access VPN	○ ○ ⊖ Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups	
e Lis	? Introduction	AAA Server Groups	
evic	Network (Client) Access	Server Group Protocol Accounting Mode Reactivation Mode Dead Time Max Failed Attempts	Add
n		Add AAA Server Group	
arks	AAA Server Groups	AAA Server Group: ISE	Edit
okm	🚮 Local Users	Protocol: RADIUS 📀	
8	Gertificate Management	Accounting Mode: Simultaneous Single	
	Language Localization	Reactivation Mode: O Depletion Timed	
	P DHCP Server	Dead Time: 10 minutes	
	📲 DNS 🕨 🔯 Advanced	Max Failed Attempts: 3	
		Enable interim accounting update	
		Update Interval: 24 Hours	Add
		Enable Active Directory Agent mode	
		Enable Active Directory Agent mode	Edit
		ISE Policy Enforcement	Delete
		Enable dynamic authorization	
		Dynamic Authorization Port: 1700	Move Up
		Is authorization only mode (no common password configuration required)	Move Down
		Se autionzation only mode (no common password computation required)	Test
		VPN3K Compatibility Option ¥	Test
		Help Cancel OK	
	👫 Firewall		
	Remote Access VPN		
	Cal Site_to_Site VPN	Find: 💿 💿 Match Case	
		LDAP Attribute Map	*
	Device Management	Reset Apply	

C.在同一页的"Servers in the Selected group"部分下,点击"Add"并提供AAA服务器的IP地址详细信 息

Remote Access VPN		ation > Remot				ver Groups	ci
? Introduction	AAA Server Grou	ups		AA/LOCALOSCIS		ver droups	
Network (Client) Access AnyConnect Connection Profiles	Server Group	Protocol RADIUS	Accounting Mode Single	Reactivation Mode Depletion	Dead Time 10	Max Failed Attempts 3	Add
AnyConnect Customization/Localization/Loc	LOCAL	LOCAL					Edit
AnyConnect Client Software							Delete
Group Policies			Add AAA Serve	r			
IPsec(IKEv1) Connection Profiles IPsec(IKEv2) Connection Profiles	Server Group	: (SE				
Secure Mobility Solution Address Assignment	Interface Nan	ne:	outside ᅌ				
Assignment Policy	Server Name	or IP Address:	10.106.44.77				
 Address Pools Advanced 	Timeout:		10 seconds				
Clientless SSL VPN Access AAA/Local Users	RADIUS Parar	neters				(Add
AAA Server Groups	Server Auth	nentication Port	1645				Edit
Cocal Users	Server Acco	ounting Port:	1646				Delete
 Manager Certificate Management 	Retry Inter	val:	10 seconds				Move Up
Language Localization Load Balancing	Common P	et Ney.					Move Down
DHCP Server	ACL Netma	isk Convert:	Standard				Test
or DNS	Microsoft 0	CHAPv2 Capable	e: 🔽				rest
A Device Setup	SDI Messages	5					
🚯 Firewall	Message	Fable				*	
Remote Access VPN		Help	Cancel	ОК			
Site-to-Site VPN	LDAP Attribute	Мар					
🛺 Device <u>M</u> anagement							

4.映射AnyConnect客户端软件

A.映射用于WebVPN的Windows的AnyConnect客户端软件webdeploy映像4.8.03052

B.导航到"Configuration > Remote Access VPN > Network(Client)Access > AnyConnect Client Software",点击"Add"



5.配置由ISE推送的重定向ACL

A.导航到"Configuration > Firewall > Advanced > ACL Manager",点击Add以添加重定向ACL。配置后,条目如下所示:

•	•			_		Cisco ASDM 7.12(2)	or ASA - 10.	197.164.3			
6	Home	Configuration 🖉 Monitor	ing	📙 Sav	e 💽 R	efresh 🔇 Back 🔘	Forward	Help Type topic G	0		cisco
st	00	O Firewall		00	onfigur	ation > Firewall > A	dvanced > ,	ACL Manager			_
Ce Li		Access Rules	16	Add ·	- 🗹 Edi	t 📋 Delete 👌 🗲	አ 🖻 🛍	 Q Find 🔜 Export 	•		
Devi		Service Policy Rules	#		Enabled	Source	Se	. Destination	Security Group	Destination Service	Action
	l 🔐	AAA Rules	T T	redirec	t						
		Filter Rules		1	 Image: A start of the start of	🧼 any		any		👐 domain	Oeny
larks	•	Ethertype Rules		2		🧼 any		릨, 10.197.243.116		ır⊵ ip	3 Deny
ak k		Public Servers		3		🍑 any		🌍 any		🛃 icmp	3 Deny
B		URL Filtering Servers		4		🇳 any		any		<u></u> ₽> ip	✓ Permit
		Threat Detection		5	 Image: A start of the start of	🧼 any		🧼 any		😰 http	V Permit
	0	dentity Options									
		VM Attribute Agent									
	▶ 35	Botnet Traffic Filter									
	▶ 🐻	Objects									
	🕨 🔯	Unified Communications									
	V 🕲	Advanced									
		Anti-Spoofing									
		Certificate Management									
		P Audit									
		SUNRPC Server									
		TCP Options									
		🐯 Global Timeouts									
		P Virtual Access									
		ACL Manager									
		Standard ACL									
		Per-Session NAT Rules									
	<u>_</u>	Device Setup									
		F <u>i</u> rewall									
	a	Remote Access VPN									
		Site-to-Site VPN		Collan	se All	Expand All					
	1	Device <u>M</u> anagement		Sonap		espana / in					
		»						Reset Apply)		

6.验证现有组策略

A.此设置使用默认组策略,可以在以下位置查看:"Configuration > Remote Access VPN > Network(Client)Access > Group Policies"



7.配置连接配置文件

A.创建AnyConnect用户连接的新连接配置文件

B.导航到"Configuration > Remote Access VPN > Network(Client)Access > Anyconnect Connection Profiles",然后单击"Add"

		Cisco ASDM 7.	12(2) for ASA - 10.	197.164.3		
Home 🖏 Configuration 🧾 Monitori	ng 릚 Save 🔇	Refresh 🔇 Ba	ck 💽 Forward	? Help Type topic	Go	CISC
O O Remote Access VPN	○ ○ ○ Configu	ration > Remo	te Access VPN > N	Network (Client) Acc	ess > AnyConnect Conne	ction Profiles
 Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Local AnyConnect Client Profile 	The security a initial client o tunnel as well Access Interface	appliance automa leployment requi l as SSL tunnel w	atically deploys the ires end-user admi rith Datagram Tran:	e Cisco AnyConnect \ inistrative rights. The sport Layer Security (/PN Client to remote users : Cisco AnyConnect VPN Cl DTLS) tunneling options.	upon connection. The ient supports IPsec (IK
AnyConnect Client Software	CI Enable Ci	sco AnyConnect	VPN Client access	on the interfaces sel	ected in the table below	Lever els)
Group Policies	SSL access m	ust be enabled if	you allow AnyCon	inect client to be laur	iched from a browser (Web	Launch) .
IPsec(IKEv1) Connection Profiles	Interface	Allow Access	Enable DTLS	Allow Access	Enable Client Services	
IPsec(IKEv2) Connection Profiles	outside					Device Certificate
Secure Mobility Solution		-	_			Port Settings
 Advanced 						
AAA/Local Users AAA/Local Users Secure Desktop Manager Certificate Management Language Localization Load Balancing DHCP Server DNS Advanced	Connection prof Connection prof	rom group policy ng r to select conne portal login pag files rofile (tunnel gro te to connection	ection profile on th ge. pup) specifies how profile <u>here</u> .	Iways apply to the transfer of	affic. I and other parameters. You	i can configure the ma
	Add 🖉	Edit 🔟 Delete	Find:		Match Case	
	Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
Setup	DefaultRAGr	· 🔽			AAA(LOCAL)	DfltGrpPolicy
	DefaultWEBV	. 🔽			AAA(LOCAL)	DfltGrpPolicy
Firewall	TG_SAML			SAML_Users	Saml	DfltGrpPolicy
Image: Site and S	Let group connectio	URL take preced on profile that m	dence if group URL atches the certifica	and certificate map r ate map will be used.	natch different connection	profiles. Otherwise, t
*				Reset Apply		

C.配置以下与连接配置文件相关的详细信息:

名称	TG_SAML
别名	SAML用户
方法	SAML
AAA 服务器组	本地
客户端地址池	AC_Pool
组策略	DfltGrpPolicy

Basic ▶ Advanced	Name:	TG_SAML	
	Aliases:	SAML_Users	
	Authentication		
	Method:	SAML	
	AAA Server Group:	LOCAL) Manage
		Use LOCAL if Server Group fails	
	SAML Identity Provider		
	SAML Server :	https://explorer.cisco.com/dag/saml2/idp/metadata.php	Manage
	Client Address Assignment		
	DHCP Servers:		
		None OHCP Link OHCP Subnet	
	• Client Address Pools:	AC_Pool	Select
	Client IPv6 Address Pools:		Select
	Default Group Policy		
	Group Policy:	DfltGrpPolicy	🗘 Manage
	(Following fields are linked	to attribute of the group policy selected above.)	
	Enable SSL VPN clien	t protocol	
	✓ Enable IPsec(IKEv2) c	lient protocol	
	DNS Servers:		
	WINS Servers:		
	Domain Name:		
Find:		Next Previous	
		Help Cancel OK	

d.在同一页面上,配置SAML身份提供程序详细信息,如下所示:

IDP实 体Id	https://explorer.cisco.com/dag/saml2/idp/metadata.php
登录 URL	https://explorer.cisco.com/dag/saml2/idp/SSOService.php
注销 URL	https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisc
基本 URL	https://firebird.cisco.com

E.点击"管理>添加"

• •	Add SSO Server
IDP Entity ID:	https://explorer.cisco.com/dag/saml2/idp/metadata.php
Settings	
Sign In URL:	https 📀 :// explorer.cisco.com/dag/saml2/idp/SSOService.php
Sign Out URL:	https 文 :// explorer.cisco.com/dag/saml2/idp/SingleLogoutSe
Base URL	https ᅌ :// firebird.cisco.com
Identity Provider Certificate	Duo_Access_Gateway:o=Duo Security Inc., I=Ann Ar ᅌ
Service Provider Certificate:	ID_CERT:cn=firebird.cisco.com:cn=SHERLOCK-CA, dc=c
Request Signature:	None 🗘
Request Timeout:	1200 seconds (1-7200)
Enable IdP only accessible on Internal Network	
Request IdP re-authentication at login	
Help	Cancel

F.在连接配置文件的Advanced部分下,定义用于授权的AAA服务器

导航到"Advanced > Authorization", 然后单击"Add"

e authorization database to connect
ıps
up to Interface
Manage

G.在"组别名"下,定义连接别名

导航到"Advanced > Group Alias/Group URL",然后单击"Add"

Edit AnyConnect Connection Profile: TG_SAML



H.这样,ASA配置即完成,如下面的命令行界面(CLI)所示

```
1
hostname firebird
domain-name cisco.com
1
1
name 10.197.164.7 explorer.cisco.com
name 10.197.164.3 firebird.cisco.com
1
   1 -
I
ip local pool AC_Pool 10.197.164.6-explorer.cisco.com mask 255.255.255.0
L
        ------Redirect Access-list-----
!
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.197.243.116
access-list redirect extended deny icmp any any
access-list redirect extended permit ip any any
access-list redirect extended permit tcp any any eq www
I
  -----AAA server configuration-----
1 -
I
aaa-server ISE protocol radius
authorize-only
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE (outside) host 10.106.44.77
key *****
I
!----Configure Trustpoint for Duo Access Gateway Certificate----
Т
crypto ca trustpoint Duo_Access_Gateway
enrollment terminal
crl configure
L
!-----Configure Trustpoint for ASA Identity Certificate-----
I
crypto ca trustpoint ID_CERT
 enrollment terminal
 fqdn firebird.cisco.com
 subject-name CN=firebird.cisco.com
```

```
ip-address 10.197.164.3
 keypair ID_RSA_KEYS
no ca-check
crl configure
I
!-----Enable AnyConnect and configuring SAML authentication-----
1
webvpn
 enable outside
hsts
 enable
 max-age 31536000
 include-sub-domains
 no preload
 anyconnect image disk0:/anyconnect-win-4.8.03052-webdeploy-k9.pkg 1
 anyconnect enable
 saml idp https://explorer.cisco.com/dag/saml2/idp/metadata.php
 url sign-in https://explorer.cisco.com/dag/sam12/idp/SSOService.php
 url sign-out https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explor
 base-url https://firebird.cisco.com
 trustpoint idp Duo_Access_Gateway
 trustpoint sp ID_CERT
 no signature
 no force re-authentication
 timeout assertion 1200
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
1
 -----Group Policy configuration------
I
ļ
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
ļ
    -----Tunnel-Group (Connection Profile) Configuraiton-----
Į.
T
tunnel-group TG_SAML type remote-access
tunnel-group TG_SAML general-attributes
address-pool AC_Pool
 authorization-server-group ISE
accounting-server-group ISE
tunnel-group TG_SAML webvpn-attributes
 authentication saml
group-alias SAML_Users enable
saml identity-provider https://explorer.cisco.com/dag/saml2/idp/metadata.php
i
```

```
-ISE 配置
```

1.添加Cisco ASA作为网络设备

在"Administration > Network Resources > Network Devices"下,单击"Add"。 配置网络设备的名称、关联的IP地址,并在"Radius身份验证设置"下配置"共享密钥"并单击"保存"

Notwor	A Devices	
Networ		
	IP Address • IP : 10.197.164.3	/ 32
	* Device Profile	
	Software Version	
	* Network Device Group	
	Location All Locations 📀 Set To Default	
	IPSEC No Set To Default	
	Device Type All Device Types 📀 Set To Default	
	RADIUS UDP Settings	
	Protocol	RADIUS
	* Shared Secret	••••• Show
	Use Second Shared Secret	
	Use Second Shared Secret	Show
	Use Second Shared Secret CoA Port	Image: Show Image: Show Image: Show Set To Default
	Use Second Shared Secret CoA Port RADIUS DTLS Settings (i)	Image: Show 1700 Set To Default
	Use Second Shared Secret CoA Port RADIUS DTLS Settings (i) DTLS Required Shared Secret	Image: Show Image: Show <t< th=""></t<>
	Use Second Shared Secret CoA Port RADIUS DTLS Settings (2) DTLS Required Shared Secret CoA Port	Image: Constraint of the second se
	Use Second Shared Secret CoA Port RADIUS DTLS Settings (i) DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA	Image: Show Image: Show </th
	Use Second Shared Secret CoA Port RADIUS DTLS Settings 7 DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name	Image: Show Image: Show </th
	Use Second Shared Secret CoA Port RADIUS DTLS Settings (i) DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name	Image: Show Image: Show Image: Image: Show Image: Image: Image: Show Image: Ima
	Use Second Shared Secret CoA Port RADIUS DTLS Settings (i) DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name General Settings	Image: Show Image: Show Image: Image: Show Image: Image: Show Image: Image: Show Image: Image: Image: Image: Image: Show Image: Im
	Use Second Shared Secret CoA Port RADIUS DTLS Settings (i) DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name General Settings Enable KeyWrap * Key Encryption Key	Image: Show 1700 Set To Default Image: Set To Default Image: Set To Default Select if required (optional)
	Use Second Shared Secret CoA Port RADIUS DTLS Settings () DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name General Settings Enable KeyWrap * Key Encryption Key * Message Authenticator Code Key	Image: Show Image: Image: Image: Show Image: Imag
	Use Second Shared Secret CoA Port RADIUS DTLS Settings () DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name General Settings Enable KeyWrap * Key Encryption Key * Message Authenticator Code Key Key Input Format	Image: Show Image: I
	Use Second Shared Secret CoA Port RADIUS DTLS Settings () DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name General Settings Enable KeyWrap * Key Encryption Key * Message Authenticator Code Key Key Input Format	Image: Constraint of the second s
	Use Second Shared Secret CoA Port RADIUS DTLS Settings () DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name General Settings Enable KeyWrap * Key Encryption Key * Message Authenticator Code Key Key Input Format	Image: Show Image: I
	Use Second Shared Secret CoA Port RADIUS DTLS Settings (i) DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name General Settings Enable KeyWrap * Key Encryption Key * Message Authenticator Code Key Key Input Format	Image: Show Image: Show </th
	Use Second Shared Secret CoA Port RADIUS DTLS Settings () DTLS Required Shared Secret CoA Port Issuer CA of ISE Certificates for CoA DNS Name General Settings Enable KeyWrap * Key Encryption Key * Message Authenticator Code Key Key Input Format • TACACS Authentication Settings • SNMP Settings	image: show 1700 Set To Default image: show Show Show ASCII HEXADECIMAL

2.安装最新的状态更新

导航至"管理>系统>设置>状态>更新"并单击"立即更新"

Posture Updates	
 Web 	Offline
* Update Feed URL	https://www.cisco.com/web/secure/spa/posture-update.xml Set to Default
Proxy Address	72.163.217.104
Proxy Port	80 HH MM SS
Automatically che	ck for updates starting from initial delay 06 - 00 - 18 - every 2 hours
Save	date Now Reset
▼ Update Inform	ation
Last successful upd	ate on 2020/05/07 15:15:05

	0
Last update status since ISE was started	No update since ISE was started.
Cisco conditions version	224069.0.0.0
Cisco AV/AS support chart version for windows	171.0.0.0
Cisco AV/AS support chart version for Mac OSX	91.0.0.0
Cisco supported OS version	41.0.0.0

3.上传ISE上的合规性模块和AnyConnect头端部署包

导航到"Policy > Policy Elements > Results > Client Provisioning > Resources"。点击"添加",然后 根据要从本地工作站还是思科站点获取文件,选择"从本地磁盘获取代理资源"或"从思科站点获取代 理资源"。

在这种情况下,要从"类别"下的本地工作站上传文件,请选择"思科提供的软件包",然后单击"浏览 ",选择所需的软件包,然后单击"提交"。

本文档使用"anyconnect-win-4.3.1012.6145-isecompliance-webdeploy-k9.pkg"作为合规性模块,使用"anyconnect-win-4.8.03052-webdeploy-k9.pkg"作为AnyConnect头端部署包。

Agent Resources From Local Disk > Agent Resources From Local Disk

Agent Resources From Local Disk

Category	Cisco Provided Packages Browse anyconnect-win-4.8.03	() 052-webdeploy-k9.pkg		
	 AnyConnect Uploaded Resource 	S		
	Name	Туре	Version	Description
	AnyConnectDesktopWindows 4.8.30	AnyConnectDesktopWindows	4.8.3052.0	AnyConnect Secure Mobility Clie

Submit Cancel

4.创建AnyConnect状态配置文件

A.导航到"策略>策略元素>结果>客户端调配>资源"。点击"Add"并选择"AnyConnect Posture Profile"

B.输入Anyconnect终端安全评估配置文件的名称,并在服务器名称规则下将服务器名称配置为 "*",然后点击"保存"

ISE Posture Agent Profile Settings > Anyconnect Posture Profile

* Name:	Anyconnect Posture Profile	
Description		
		11.

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	60 secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery host		IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	The server that the agent should connect to
• Server name rules	*	need to be blank by default to force admin to enter a value. *** means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. ".cisco.com"
Call Home List		List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

5.创建Anyconnect配置

A.导航到"策略>策略元素>结果>客户端调配>资源"。点击"添加"并选择"AnyConnect配置"

B.选择AnyConnect软件包,输入配置名称,选择所需的合规性模块

C.在"AnyConnect模块选择"下,选中"诊断和报告工具"

D.在"Profile Selection"下,选择Posture Profile并单击"Save"

AnyConnect Configuration > AnyConnect Configuration

* Select AnyConnect Package	AnyConnectDesktopWindows 4.8.3052.0	
* Configuration Name	AnyConnect Configuration	
Description:		
Description	Value Note	s
* Compliance Module	AnyConnectComplianceModuleWindows 4.3.1250.614	

AnyConnect Module Selection

Concollon
ISE Posture
VPN
Network Access Manager
Web Security
AMP Enabler
ASA Posture
Network Visibility
Umbrella Roaming Security
Start Before Logon
Diagnostic and Reporting Tool

Profile Selection

* ISE Posture	Anyconnect Posture Profile	D
VPN		
Network Access Manager		
Web Security		
AMP Enabler		
Network Visibility		
Umbrella Roaming Security		
Customer Feedback		

6.创建客户端调配策略

A.导航到"策略>客户端调配"。

B.点击"编辑",然后选择"在上面插入规则"

C.输入Rule Name,选择所需的操作系统,然后在Results(在"Agent" > "Agent Configuration"中)下,选择在第5步中创建的"AnyConnect Configuration",然后单击"Save"

cisco Idei	ntity Service	s Engine	Home	• (Context Visibility	•	Operations	▼ Policy		Administration	Work Centers			License Warning 🔺	0	0 0	ø
Policy Sets	Profiling	Posture	Client Prov	isioning	 Policy Elem 	ients											
Client Prov Define the Cli For Agent Co	visioning P ient Provisionin nfiguration: ve	rolicy ng Policy to ersion of ag	o determine w	hat user sfile, age	s will receive upo	on logi odule	in and user sest	sion initiation	packa	1ge.							
- or Native St	applicant Conn	iguration: w	vizaro prome a	ind/or wi	zaro. Drag and o	rop n	ules to change t	te order.									
	Rule Na	me		Ide	ntity Groups		Operating Sys	lems		Other Conditions	3		Results				
	IOS			lf An	y i	and	Apple iOS All		and	Condition(s)		then	Cisco-ISE-NSP			Edit	÷
	Android			lf An	y i	and	Android		and	Condition(s)		then	Cisco-ISE-NSP			Edit	Ŧ
1	Windows_	10		lf An	y i	and	Windows 10 (All)	and	Condition(s)		then	AnyConnect Configuration			Edit	٣
	Windows			lf An	y :	and	Windows All		and	Condition(s)		then	CiscoTemporalAgentWi ndows 4.7.00135 And WinSPWizard 2.5.0.1 And Cisco-ISE-NSP			Edit	Ŧ
	MAC OS			lf An	y a	and	Mac OSX		and	Condition(s)		then	CiscoTemporalAgentOS X 4.7.00135 And MacOxXSPW2ard 2.10.42 And Cisco-ISE- NSP			Edit	÷
	Chromebo	ok		lf An	y i	and	Chrome OS A		and	Condition(s)		then	Cisco-ISE-Chrome-NSP			Edit	*
Save R	eset																

7.创建安全评估条件

A.导航至"策略>策略元素>条件>状态>文件条件"

B.单击"添加"并将条件名称"VPN_Posture_File_Check"、所需的操作系统为"Windows 10(All)"、文 件类型为"FileExistence"、文件路径为"ABSOLUTE_PATH"、完整路径和文件名配置为 "C:\custom.txt",选择文件操作符为"Exists"

C.此示例使用C:驱动器下名为"custom.txt"的文件作为文件条件

cisco Identity Services Engine	Home	Operations ▼Policy	Administration	Work Centers
Policy Sets Profiling Posture C	lient Provisioning Policy Element	s		
Dictionaries - Conditions - Result	ts			
C Library Conditions Smart Conditions Time and Date Profiling	File Conditions List > VPN_Postur File Condition * Name VPN_ Description	re_File_Check Posture_File_Check		
✓ Posture	* Operating System Wind	lows 10 (All) 🔶		
Anti-Malware Condition	Compliance Module Any ve * File Type FileE	rsion kistence		
Anti-Virus Condition	* File Path ABSO		C:\custom.txt	(i)
Compound Condition Disk Encryption Condition	Save Reset	<u> </u>		
File Condition				

8.创建状况补救操作

导航到"Policy > Policy Elements > Results > Posture > Remediation Actions"以创建对应的File Remediation Action。本文档使用"仅消息文本"作为下一步中配置的补救操作。

9.创建状况要求规则

A.导航至"策略>策略元素>结果>状态>要求"

B.单击"编辑",然后选择"插入新要求"

C.将条件名称"VPN_Posture_Requirement"、所需的操作系统配置为"Windows 10(All)"、合规性模 块配置为"4.x或更高版本"、安全评估类型配置为"Anyconnect"

D.条件为"VPN_Posture_File_Check"(在第7步中创建),在"Remediations Actions"下,选择 "Action"作为"Message Text Only",然后输入座席用户的自定义消息

cisco Identity Services Engine	Home Context Visibility Operations Poli	Administration			License Warning 🔺	Q 0 0
Policy Sets Profiling Posture Cl	ent Provisioning Policy Elements					
Dictionaries Conditions	<u>,</u>					
0					*	
Authentication	Requirements					
	Name Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions	
Authorization	Default_Hardware_Attributes_Re for Mac OSX quirement_Mac	using 4.x or later	using AnyConnect	met if Hardware_Attributes_Ch eck	then Select Remediations	Edit 🕶
Profiling	Default_Firewall_Requirement_W for Windows All in	using 4.x or later	using AnyConnect	met if Default_Firewall_Conditi on_Win	then Default_Firewall_Remedi ation_Win	Edit 🕶
• Posture	Default_Firewall_Requirement_M for Mac OSX ac	using 4.x or later	using AnyConnect	met if Default_Firewall_Conditi on_Mac	then Default_Firewall_Remedi ation_Mac	Edit 🕶
 Remediation Actions 	USB_Block_temporal for Windows All	using 4.x or later	using Temporal Agent	met if USB_Check	then Message Text Only	Edit 🕶
Requirements	Any_AM_Installation_Win_tempo for Windows All ral	using 4.x or later	using Temporal Agent	met if ANY_am_win_inst	then Message Text Only	Edit 🕶
Client Provisioning	Any_AM_Installation_Mac_tempo for Mac OSX ral	using 4.x or later	using Temporal Agent	met if ANY_am_mac_inst	then Message Text Only	Edit 🕶
	Default_AppVis_Requirement_Wi for Windows All n_temporal	using 4.x or later	using Temporal Agent	met if Default_AppVis_Conditio n_Win	then Select Remediations	Edit 🕶
	Default_AppVis_Requirement_M for Mac OSX ac_temporal	using 4.x or later	using Temporal Agent	met if Default_AppVis_Conditio n_Mac	then Select Remediations	Edit 🕶
	Default_Hardware_Attributes_Re for Windows All quirement_Win_temporal	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Ch eck	then Select Remediations	Edit 🕶
	Default_Hardware_Attributes_Re for Mac OSX quirement_Mac_temporal	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Ch eck	then Select Remediations	Edit 🕶
	Default_Firewall_Requirement_W for Windows All in_temporal	using 4.x or later	using Temporal Agent	met if Default_Firewall_Conditi on_Win	then Default_Firewall_Remedi ation_Win	Edit 🕶
	Default_Firewall_Requirement_M for Mac OSX ac_temporal	using 4.x or later	using Temporal Agent	met if Default_Firewall_Conditi on_Mac	then Default_Firewall_Remedi ation_Mac	Edit -
	VPN_Posture_Requirement for Windows 10	(All) using 4.x or later	using AnyConnect	met if VPN_Posture_File_Chec	then Message Text Only	Edit 🖛
	Note: Remediation Action is filtered based on the operating Remediation Actions are not applicable for Application	system and stealth mode selection. In Conditions (configured using the Provision E	By Category or Provision By Everything option	is), Hardware Conditions, and External Data	a source conditions.	

10.创建安全评估策略

A.导航到"策略>状态"

B.将规则名称配置为"VPN_Posture_Policy_Win",将所需的操作系统配置为"Windows 10(All)",将 合规性模块配置为"4.x或更高版本",将状态类型配置为"Anyconnect",将要求配置为 "VPN_Posture_Requirement"(如步骤9中所配置)

dentit	y Services Engin	e Home → Context Visit	bility		ation				License Warning 🔺	୍ ଡ୍ ୦
y Sets	Profiling Posture	Client Provisioning Policy	Elements							
ure Polic	v									
the Postu	re Policy by configu	ring rules based on operating syste	m and/or other conditio	ns.					*	
Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions		Requirements	
0	Policy Options	Default_AppVis_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then	Default_AppVis_Requir ement_Win	Edit
0	Policy Options	Default_AppVis_Policy_Win_te mporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then	Default_AppVis_Requir ement_Win_temporal	Edit
0	Policy Options	Default_Firewall_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then	Default_Firewall_Requir ement_Mac	Edit
0	Policy Options	Default_Firewall_Policy_Mac_t emporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then	Default_Firewall_Requir ement_Mac_temporal	Edit
0	Policy Options	Default_Firewall_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then	Default_Firewall_Requir ement_Win	Edit
0	Policy Options	Default_Firewall_Policy_Win_te mporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then	Default_Firewall_Requir ement_Win_temporal	Edit
0	Policy Options	Default_Hardware_Attributes_P olicy_Mac	lf Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then	Default_Hardware_Attri butes_Requirement_Ma c	Edit
0	Policy Options	Default_Hardware_Attributes_P olicy_Mac_temporal	lf Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then	Default_Hardware_Attri butes_Requirement_Ma c_temporal	Edit
0	Policy Options	Default_Hardware_Attributes_P olicy_Win	lf Any	and Windows All	and 4.x or later	and AnyConnect	and	then	Default_Hardware_Attri butes_Requirement_Wi n	Edit
0	Policy Options	Default_Hardware_Attributes_P olicy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then	Default_Hardware_Attri butes_Requirement_Wi n_temporal	Edit
0	Policy Options	Default_USB_Block_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then	USB_Block	Edit
0	Policy Options	Default_USB_Block_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then	USB_Block_temporal	Edit
° 🖌	Policy Options	VPN_Posture_Policy_Win	If Any	and Windows 10 (All)	and 4.x or later	and AnyConnect	and	then	VPN_Posture_Require	Edit

11.创建动态ACL(DACL)

导航到Policy > Policy Elements > Results > Authorization > Downloadable ACL,并为不同的安全 评估状态创建DACL。

本文档使用以下DACL。

A.安全评估未知:允许流量到达DNS、PSN、HTTP和HTTPS流量

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	
Policy Sets Profiling Posture C	lient Provisioning Policy Elements	
Dictionaries	ts	
Authentication Authorization Authorization Profiles Downloadable ACLs Profiling Posture Client Provisioning	Downloadable ACL List > PostureUnknown Downloadable ACL * Name PostureUnknown Description IP version • IPv4 IP version • IPv6 Agnostic @ * DACL Content 1234567 permit udp any any eq domain 8910111 permit ip any host 10.106.44.77 2134145 permit tcp any any eq 80 1617181 permit tcp any any eq 443 9202122 2324252 6272829 3031323 3343556 > Check DACL Syntax	Ĩ
	Save Reset	

B.状态不兼容:拒绝访问私有子网并仅允许互联网流量

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture Clier	t Provisioning ▼Policy Elements
Dictionaries + Conditions - Results	
Authentication Authorization	Downloadable ACL List > PostureNonCompliant Downloadable ACL * Name PostureNonCompliant
Authorization Profiles	Description
Downloadable ACLs	
▶ Profiling	* DACL Content 1234567 deny ip any 10.0.0 255.0.0.0
→ Posture	8910111 deny ip any 172.16.00 255.240.00 2131415 deny ip any 192.168.00 255.255.0.0 1617181 permit ip any any
Client Provisioning	9202122 2324252 6272829 3031323 3343536 • Check DACL Syntax
	Save

C.安全评估合规性:允许安全评估合规性最终用户的所有流量

cisco Identity Services Engine	Home → Context Visibility → Operations → Policy → Administration → Work Centers	
Policy Sets Profiling Posture C	Client Provisioning Policy Elements	
Dictionaries	lts	
Authentication	Downloadable ACL List > PostureCompliant Downloadable ACL	
Authorization Authorization Profiles	* Name PostureCompliant Description	
Downloadable ACLs	IP version SIPv4 OPv6 Agnostic ()	
▶ Profiling	* DACL Content 1234567 (permit ip any any 891011)	
▶ Posture	2131415 1617181 9202122	
Client Provisioning	2324252 6272829 3031323 3343536	
	Check DACL Syntax	
	Save Reset	

12.创建授权配置文件

导航至"Policy > Policy Elements > Results > Authorization > Authorization Profiles"。

A.未知状态的授权配置文件

选择DACL"PostureUnknown",选中Web Redirection,选择Client Provisioning(Posture),配置 Redirect ACL名称"redirect"(要在ASA上配置),然后选择Client Provisioning门户(默认)

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺	् 🙆 o 🔅
Policy Sets Profiling Posture Cli	ent Provisioning Policy Elements		
Dictionaries + Conditions - Results	3		
0			
Authentication	Authorization Profile Authorization Profile		
- Authorization	Name Posture Redirect		
Authorization Profiles	Description		
Downloadable ACLs	* Access Type Access ACCEPT		
▶ Profiling	Network Device Profile 🛛 🟥 Cisco 🔻 🕀		
→ Posture	Service Template		
Client Provisioning	Track Movement		
	* Common Tasks		
	DACL Name RostureUnknown		
Client Provisioning	Web Redirection (CWA, MDM, NSP, CPP) ACL [redirect ©] Value Client Provisioning (Posture) • ACL [redirect ©]		
	▼ Advanced Attributes Settings		
	Select an item		
	Attributes Details Access Type = ACCESS_ACCEPT DACL = PostureUnknown disco-av-pair = urf-enderect-ad=redirect disco-av-pair = urf-redirect=https://ip.port/porta/gateway?session1d=Session1dValue&portal=27b1bc30-2e58-11e9-98/b-0050568775a3&action=cpp		te.

B.状态不合规的授权配置文件

选择DACL"PostureNonCompliant"以限制对网络的访问

dentity Services Engine	Home Context Visibility Operations Administration Work Centers	License Warning 🔺	९ 🕑	• •
Policy Sets Profiling Posture C	Ilent Provisioning Policy Elements			
Dictionaries + Conditions - Resul				
G				
Authentication	Authorization Profiles > Posture Non Compliant Authorization Profile			
- Authorization	* Name Posture Non Compliant			
Authorization Profiles	Description			
Downloadable ACLs	* Access Type Access Accept *			
▶ Profiling	Network Device Profile 📾 Clisco 💌 🕀			
+ Posture	Service Template			
Client Provisioning	Track Movement 🗇 🕖			
	Passive Identity Tracking 🔄 🕢			
	▼ Common Tasks			
	DACL Name PostureNonCompliant			
	▼ Attributes Details			
	Access Type = ACCESS_ACCEPT DACL = PostureNonCompliant	16.		
	Swe Reset			

C.安全评估合规性的授权配置文件

选择DACL"PostureCompliant"以允许对网络的完全访问

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺	۹ 🛛	o o
Policy Sets Profiling Posture C	Client Provisioning Policy Elements			
Dictionaries Conditions Resu	Its			
Authentication Authorization Authorization Profiles Descriptionship 401 p	Authorization Profile * Name Full Access Description * Access Type (arcress arcrept v)			
Profiling	Network Device Profile 💼 Cisco 🖡 🕀			
▶ Posture	Service Template			
Client Provisioning	Track Movement 0			
	✓ Common Tasks			
	▼ Attributes Details			
	Access Type = ACCESS_ACCEPT DACL = PERMIT_ALL_IPV4_TRAFFIC		14.	
	Save Reset			

12.配置授权策略

使用在上一步中配置的授权配置文件为安全评估合规性、安全评估不合规性和安全评估未知配置3个 授权策略。

通用条件"会话:状态状态"用于确定每个策略的结果

cisco Ide	entity Service	s Engine Home Conte	ext Visibility	y Operations	← Policy → Administration	Work Centers				License Warning	\$	0 0
Policy Se	Profiling	Posture Client Provisioning	 Policy El 	lements								
									_			
Policy S	Sets → De	fault								Reset Policyset Hitcoun	ts Res	et Save
	Status	Policy Set Name	Descrip	ption	Conditions					Allowed Protocols / Serv	er Sequenc	e Hits
Search												
	ø	Default	Default	policy set						Default Network Access	x - +	49
> Authe	entication Po	licy (3)										
> Autho	orization Poli	ou - Local Exceptions										
* Addie	012800111-01	cy - Eodal Exceptions										
> Autho	orization Poli	cy - Global Exceptions										
✓ Author	orization Poli	cy (15)										
							Poculte					
+	Status	Pulo Namo	Cond	itions			Profiles		Security Group		Lite	Actions
Conroh	Status	Nule Name	Cond	100113			101100		occurry oroup	_	riita	Actions
Search							(100				
	ø	Anyconnect Posture Compliant	£	Session PostureS	tatus EQUALS Compliant		× Full Access	+	Select from list	- +	6	¢
	ø	Anyconnect Posture Non Compliant	£	Session PostureS	tatus EQUALS NonCompliant		Posture Non Compliant	+	Select from list	× +	0	٥
	0	Anyconnect Posture Linknown		P Network	Access-Device IP Address EQUALS 1	0.197.164.3	× Posture Redirect	+	Select from list	· +	13	ò
	ľ	Paryounness - Solure Onkilowit	AND	E Session	PostureStatus EQUALS Unknown		(

使用本部分可确认配置能否正常运行。

要验证用户是否成功通过身份验证,请在ASA上运行以下命令。

<#root>

firebird(config)#

show vpn-sess detail anyconnect

Session Type: AnyConnect Detailed : _585b5291f01484dfd16f394be7031d456d314e3e62 Username Index : 125 Assigned IP : explorer.cisco.com Public IP : 10.197.243.143 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 : 16404 Bytes Rx : 381 Bytes Tx Pkts Tx : 16 Pkts Rx : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : DfltGrpPolicy Tunnel Group : TG_SAML Login Time : 07:05:45 UTC Sun Jun 14 2020 : 0h:00m:16s Duration Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0ac5a4030007d0005ee5cc49 Security Grp : none AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 125.1 Public IP : 10.197.243.143 Encryption : none Hashing : none TCP Src Port : 57244 TCP Dst Port : 443 Auth Mode : SAML Idle TO Left : 29 Minutes Idle Time Out: 30 Minutes Client OS : win Client OS Ver: 10.0.15063 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052 Bvtes Tx : 7973 Bytes Rx : 0 Pkts Tx : 6 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 125.2 Public IP Assigned IP : explorer.cisco.com : 10.197.243.143 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384

Encapsulation: TLSv1.2 TCP Src Port : 57248 TCP Dst Port : 443 Auth Mode : SAML Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver: Cisco AnyConnect VPN Agent for Windows 4.8.03052Bytes Tx: 7973Bytes Tx: 6Pkts Tx: 6Pkts Rx: 0 Pkts Rx Drop : 0 Pkts Tx Drop : 0 Filter Name : #ACSACL#-IP-PostureUnknown-5ee45b05 DTLS-Tunnel: Tunnel ID : 125.3 Assigned IP : explorer.cisco.com Public IP : 10.197.243.143 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 49175 UDP Dst Port : 443 Auth Mode : SAML Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052 Bytes Tx : 458 Bytes Rx : 381 Pkts Tx : 4 Pkts Rx : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name :

#ACSACL#-IP-PostureUnknown-5ee45b05

ISE Posture: Redirect URL : https://ise261.pusaxena.local:8443/portal/gateway?sessionId=0ac5a4030007d0005ee5cc49&po Redirect ACL : redirect

状态评估完成后,用户访问将更改为完全访问,如字段"Filter Name"中推送的DACL中所示

<#root>

firebird(config)#

show vpn-sess detail anyconnect

Session Type: AnyConnect Detailed

Username	:	_585b5291f01484dfd16f394be7031d456d314e3e62
Index	:	125
Assigned IP	:	explorer.cisco.com Public IP : 10.197.243.143
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	:	16404 Bytes Rx : 381
Pkts Tx	:	16 Pkts Rx : 6
Pkts Tx Drop	:	0 Pkts Rx Drop : 0

Group Policy : DfltGrpPolicy Tunnel Group : TG_SAML Login Time : 07:05:45 UTC Sun Jun 14 2020 Duration : 0h:00m:36s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0ac5a4030007d0005ee5cc49 Security Grp : none AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 125.1 Public IP : 10.197.243.143 Encryption : none Hashing : none TCP Src Port : 57244 TCP Dst Port : 443 Auth Mode : SAML Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : win Client OS Ver: 10.0.15063 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052 Bytes Tx : 7973 Bytes Rx : 0 Pkts Tx : 6 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 125.2 Assigned IP : explorer.cisco.com Public IP : 10.197.243.143 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 57248 TCP Dst Port : 443 Auth Mode : SAML Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052 : 7973 Bytes Tx Bytes Rx : 0 Pkts Tx : 6 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name : #ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3 DTLS-Tunnel: Tunnel ID : 125.3 Assigned IP : explorer.cisco.com Public IP : 10.197.243.143 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 49175 UDP Dst Port : 443 Auth Mode : SAML Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052 Bytes Tx : 458 Bytes Rx : 381 Pkts Tx Pkts Rx : 4 : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name :

#ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

要验证是否在ISE上成功执行授权,请导航到"操作> RADIUS >实时日志"

此部分显示与授权用户相关的信息,例如身份、授权配置文件、授权策略和状态状态。

									Refresh	Never •	Show Latest 20	records • Within	La	st 24 hours •
S	C Refresh O Reset Repeat Counts 🕹 Export To 🗸													🔻 Filter 🕶 🗘 🗸
	Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P	Authenticat	Authorizati	Authorization Pro	Posture St	IP Address		Network Device
×		•			Identity	Endpoint ID	Endpoint Profi	Authentication	Authorization	Authorization Profiles	Posture Statu:	IP Address	•	Network Device
	Jun 14, 2020 07:44:59.975 AM	0	0	0	_585b5291f01484dfd1	00:50:56:A0:D6:97	Windows10	Default	Anyconnect	Full Access	Compliant	10.197.164.7		
	Jun 14, 2020 07:44:59.975 AM		0			10.197.243.143			Anyconnect	Full Access	Compliant			ASA
	Jun 14, 2020 07:44:59.975 AM		0		#ACSACL#-IP-PERMI									ASA
	Jun 14, 2020 07:44:34.963 AM		a		#ACSACL#-IP-Posture									ASA
	Jun 14, 2020 07:44:34.958 AM		0		_585b5291f01484dfd1	00:50:56:A0:D6:97	Windows10	Default	Default >> A	Posture Redirect	Pending			ASA

Selation S https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-iseposture-over-anyconnect-remote-acces.html#anc7

要验证Duo Admin Portal的身份验证状态,请点击Admin Panel左侧的"Reports", Admin Panel将显示Authentication Log。 更多详情:<u>https://duo.com/docs/administration#reports</u>

要查看Duo接入网关的调试日志记录,请使用以下链接: https://help.duo.com/s/article/1623?language=en_US

用户体验



故障排除

本节提供可用于对配置进行故障排除的信息。

💊 注意:使用<u>debug命令之前,请参</u>阅有关Debug命令的重要信息。

⚠ 注意:在ASA上,您可以设置各种调试级别;默认情况下,使用级别1。如果更改调试级别, ,调试的详细程度可能会增加。请谨慎执行此操作,尤其是在生产环境中。

大多数SAML故障排除都会涉及配置错误,通过检查SAML配置或运行调试可以发现该错误。

debug webvpn saml 255可用于排除大多数问题,但在此调试不提供有用信息的情况下,可以运行 其他调试: debug webvpn 255 debug webvpn anyconnect 255 debug webvpn session 255 debug webvpn request 255

要排除ASA上的身份验证和授权问题,请使用以下debug命令:

debug radius all debug aaa authentication debug aaa authorization To troubleshoot Posture related issues on ISE, set the following attributes to

posture (ise-psc.log)
portal (guest.log)
provisioning (ise-psc.log)
runtime-AAA (prrt-server.log)
nsf (ise-psc.log)
nsf-session (ise-psc.log)
swiss (ise-psc.log)

✤ 注意:有关详细的安全评估流程和AnyConnect和ISE故障排除,请参阅以下链接: <u>高级版和高级版2.2的ISE终端安全评估样式比较</u>

解释Duo接入网关调试日志并排除其故障 https://help.duo.com/s/article/5016?language=en_US

相关信息

https://www.youtube.com/watch?v=W6bE2GTU0Is& https://duo.com/docs/cisco#asa-ssl-vpn-using-saml https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-postureover-anyconnect-remote-acces.html#anc0

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。