Configurar a integração Duo com o Ative Diretory e o ISE para autenticação de dois fatores em clientes VPN Anyconnect/Acesso Remoto

Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Diagrama e cenário de rede
Processo de comunicação
Configurações do Active Directory
Configurações Duo
Configuração do proxy de autenticação Duo
Configurações do Cisco ISE
Configuração do Cisco ASA RADIUS/ISE
Configuração de VPN de acesso remoto do Cisco ASA
Teste
Troubleshooting
Depurações de trabalho

Introdução

Este documento descreve a integração por push do Duo com o AD e o ISE como autenticação de dois fatores para clientes AnyConnect conectados ao ASA.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de VPN RA no ASA
- Configuração RADIUS no ASA
- ISE
- Diretório ativo
- Aplicativos Duo

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft 2016 Server
- ASA 9.14(3)18
- Servidor ISE 3.0
- Servidor Duo
- Gerenciador de proxy de autenticação Duo

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento descreve como configurar a integração por envio do Duo com o Ative Diretory (AD) e o Cisco Identity Service Engine (ISE) como autenticação de dois fatores para clientes AnyConnect que se conectam ao Cisco Adaptive Security Appliance (ASA).

Diagrama e cenário de rede



Processo de comunicação

https://duo.com/docs/ciscoise-radius

- 1. Autenticação primária iniciada no Cisco ISE
- 2. O Cisco ISE envia a solicitação de autenticação para o proxy de autenticação Duo
- 3. A autenticação primária usa o Ative Diretory ou o RADIUS
- 4. Conexão de Proxy de Autenticação Duo estabelecida para Segurança Duo sobre a porta TCP 443
- 5. Autenticação secundária por meio do serviço Duo Security
- 6. O proxy de autenticação Duo recebe a resposta de autenticação
- 7. Acesso concedido ao Cisco ISE

Contas do usuário:

- Administrador do Ative Diretory: usado como a conta de diretório para permitir que o Proxy de Autenticação Duo se vincule ao servidor do Ative Diretory para autenticação primária.
- Usuário de teste do Ative Diretory
- Usuário de teste Duo para autenticação secundária

Configurações do Active Directory

O servidor Windows está pré-configurado com os serviços de domínio do Ative Diretory.

Nota:Se o RADIUS Duo Auth Proxy Manager for executado na mesma máquina host do Ative Diretory, as funções NPS (Servidor de Políticas de Rede) deverão ser desinstaladas/excluídas; se ambos os serviços RADIUS forem executados, eles poderão entrar em conflito e afetar o desempenho.

Para obter a configuração do AD para autenticação e identidade de usuário em usuários de VPN de acesso remoto, alguns valores são necessários.

Todos esses detalhes devem ser criados ou coletados no Microsoft Server para que a configuração possa ser feita no servidor proxy ASA e Duo Auth.

Os principais valores são:

- Nome de domínio. Este é o nome de domínio do servidor. Neste guia de configuração, agaricam.cisco é o nome de domínio.
- Endereço IP/FQDN do servidor. O endereço IP ou FQDN usado para acessar o Microsoft Server. Se um FQDN for usado, um servidor DNS deverá ser configurado no ASA e no proxy Duo Auth para resolver o FQDN.

Neste guia de configuração, esse valor é agaricam.cisco (que é resolvido como 10.28.17.107).

- Porta do servidor. A porta usada pelo serviço LDAP. Por padrão, LDAP e STARTTLS usam a porta TCP 389 para LDAP, e LDAP sobre SSL (LDAPS) usa a porta TCP 636.
- CA raiz. Se LDAPS ou STARTTLS for usado, a CA raiz usada para assinar o certificado SSL usado por LDAPS será necessária.

- Nome de usuário e senha do diretório. Essa é a conta usada pelo servidor proxy Duo Auth para vincular-se ao servidor LDAP e autenticar usuários e pesquisar usuários e grupos.
- Nome distinto (DN) de base e de grupo. O DN de base é o ponto de partida para o proxy de autenticação dupla e informa ao Ative Diretory para iniciar a pesquisa e autenticar usuários.

Neste guia de configuração, o domínio raiz agaricam.cisco é usado como DN base e DN de grupo é Duo-USERS.

1. Para adicionar um novo usuário do Duo, no Windows Server, navegue para o ícone do Windows na parte inferior esquerda e clique em Ferramentas Administrativas do Windows, conforme mostrado na imagem.

=	Recent	lly added	Windows Server		
		Notepad++			
	Z	PuTTYgen	L	Σ	2
		PSFTP	Server Manager	Windows PowerShell	Windows PowerShell ISE
	Expand	1 v			
	Most u	ised	Windows		
	240	Duo Authentication Proxy Manager	Administrativ	Task Manager	Control Panel
		Command Prompt			
	9	Snipping Tool	Remote	ė,	
	4	Wireshark	Desktop	Event Viewer	File Explorer
	Ń	Paint			
	9	Google Chrome			
	D				
		Duo Security V New			
8	G				
٢	9	Google Chrome New			
Φ	N				
		Notepad++			
-	Q	• 🤌 🥫 💆	🧧 🔼 🚦	•	

2. Na janela Ferramentas Administrativas do Windows, navegue até Usuários e Computadores do Ative Diretory.

No painel Usuários e computadores do Ative Diretory, expanda a opção de domínio e navegue até a pasta Usuários.

Neste exemplo de configuração, Duo-USERS é usado como o grupo de destino para a autenticação secundária.

→ ~ ↑ 檣 > Con	trol Panel > System and Security > Administra	tive Tools			Active Directory Users and Comp	outers		- 0	×
Converte access Quick access Desktop Dournloads P Dournloads P Dournloads P System32 This PC Desktop Dournloads Do	trol Panel > System and Security > Administra Name Attive Directory Administrative Center Active Directory Demains and Trusts Active Directory Obers and Trusts Active Directory Dess and Services Active Directory Uses and Computers Active Directory Descenters Active Descenters Active Directory De	ther Tools Date modified 7/16/2016 623 AM 7/16/2016 629 AM 7/16/2016 619 AM 7/16/2016 619 AM 7/16/2016 618 AM 7/16/2016 618 AM 7/16/2016 619 AM 7/16/2016 619 AM 7/16/2016 619 AM 7/16/2016 619 AM	Type File folder Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut	Size 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB	Active Unectory Users and Com File Action View Help the Action View Help Active Directory Users and Com Saved Queries Saved Queries Saved Queries Solutin Solu	Name Type Administrator User Administrator User Administrator User Administrator User Administrator User Administrator User Administrator User Administrator User Administrator User Administrator Security Group Consuble D. Security Group Consuble D. Security Group DonulodateP. Security Group DonulodateP. Security Group Donain Ad Security Group Donain Ac Security Group Donain Co Security Group Donain Co Security Group	Construction C	perform dynamic updates	* *
Pictures Videos Local Disk (C:) DVD Drive (D:) SSS_;	Group Policy Management Services (IIS) Manager isCSI Initiator Local Security Policy	7/16/2016 6:19 AM 7/16/2016 6:19 AM 7/16/2016 6:18 AM 7/16/2016 6:19 AM	Shortcut Shortcut Shortcut Shortcut	2 KB 2 KB 2 KB 2 KB		Domain Gue Security Group Domain Users Security Group DUO-USERS Security Group duo2 User Entroprise A Security Group	All domain guests All domain users Designated administrato		
network 🥏	Microsoft Azure Services ODBC Data Sources (32-bit) ODBC Data Sources (14)	7/16/2016 6:19 AM 7/16/2016 6:18 AM	Shortcut	2 KB 2 KB	< >>	Enterprise K Security Group Enterprise R Security Group	Members of this group Members of this group		~

3. Clique com o botão direito do mouse na pasta Users e selecione New > User, como mostrado na imagem.

Active Directory Users and Comp	outers			-	×
File Action View Help					
🗢 🔿 🙍 🚾 🛛 🛣 🖾] 🙆 🔒 🛛 🖬	n 🐮 🔌 în 🖷	r 🗾 🕱		
Active Directory Users and Com Saved Queries Saved Queries Save	Name Administrator agarciam alanad alanduo Allowed RO Cert Publish Cloneable D rol o D	Type User User User Security Group Security Group User Security Group	Description Built-in account for ad Members in this group c Members of this group Members of this group t A user account manage Members in this group c		^
New All Tasks View Refresh Export List Properties Help	> > Enterprise	Computer Contact Group InetOrgPerson msDS-KeyCreden msDS-ResourceP msDS-ShadowPri msImaging-PSPs MSMQ Queue Ali Printer	tial ropertyList ncipalContainer		~
Create a new object	and criter print	User 🔶			
		Shared Folder			

4. Na janela Novo Usuário de Objeto, especifique os atributos de identidade para este novo usuário e clique em Próximo, conforme mostrado na imagem.

New Object - User	×
Create in: agarciam.cisco/Users	on
First name: duovpn Initials:	
Last name:	
Full name: duovpn	s ir
	s o
User logon name:	s o
duovpn @agarciam.cisco	~ :cc
Liser logon name (pre-Windows 2000):	s ir
	nir
AGARCIAM	nts
	ed
	sta
< Back Next >	Cancel
	jin ain

5. Confirme a senha e clique em Avançar, em seguida, em Concluir quando as informações do usuário forem verificadas.

New Object - User	×
Create in: agarciam.cisco/Users	0
Password: Confirm password:	ac
 User must change password at next logon User cannot change password Password never expires Account is disabled 	s s c s n
< Back Next > C	ancel aii

6. Atribua o novo usuário a um grupo específico, clique com o botão direito do mouse nele e selecione Adicionar a um grupo, como mostrado na imagem.

Active Directory Users and Com	puters				-	×
File Action View Help						
🗢 🔿 🙋 📅 🖌 🖬 🗡 🕼	1 🖬 📑 🖬 🖬	1 🗏 🐮 🗊 🦷	1 🗾 🐍			
Active Directory Users and Com Saved Queries Saved Queries Builtin Builtin Computers Domain Controllers Sign ForeignSecurityPrincipal: Managed Service Accour Users	Name Administrator agarciam alanad alanduo Allowed RO Cert Publish Cert Publish Coneable D DefaultAcco DefaultAcco Donaid ROD Donaid ROD Donain Ad Domain Ad Domain Co Domain Co Domain Gue Domain Gue Domain Users duo2 DUO-USERS	Type User User User Security Group Security Group	Description Built-in a Members Members A user ac Members DNS Adm DNS clier Designato All works All doma All doma	on account for ad s in this group c s of this group s of this group t count manage s in this group c ninistrators Gro nts who are per ed administrato tations and ser in controllers i in guests in users		*
< >>	R Enterprise	Add to a group		of this group		 *
Allows you to add the selected object	ts to a group yo	Disable Account				

7. No painel Selecionar grupos, digite o nome do grupo desejado e clique em Verificar nomes.

Em seguida, selecione o nome que corresponde aos seus critérios e clique em Ok.



8. Este é o usuário usado neste documento como exemplo.

Configurações Duo

1. Faça login no portal do Administrador do Dudo.

Admin Login	
Enter your admin credentials	
Password Forgot password?	
Log in	
Confirm your identity	

2.No painel do lado esquerdo, navegue até Users, clique em Add User e digite o nome do usuário que corresponde ao seu nome de usuário do Ative Domain e clique em Add User.



3. No painel do novo usuário, preencha a lacuna com todas as informações necessárias.

Policies	Uasnboara > Users > duovpn		
Applications	duovpn		Logs Send Enrollment Email
Single Sign-On			
Users Add User Pending Enrollments Bulk Enroll Users	(i) This user has not end	olled yet. See our enrollment documentation [2] to learn more about enrolling users.	
Import Users Directory Sync Bypass Codes Groups	Username aliases	+ Add a username alias Users can have up to 8 aliases. Optionally, you may choose to reserve using an alias number for a specific alias	
Endpoints		(e.g., Username alias 1 should only be used for Employee ID).	
2FA Devices Trusted Endpoints	Full name	test <u>ypn</u> user	
Trust Monitor Reports	Email	com	
Settings	Status	Active	
Need Help? <u>Chat with Tech Support</u> C ⁴ <u>Email Support</u> Call us at 1-855-386-2884 Versioning Core Authentication Service: D235.6 Admin Panel: D235.6	Status	 Active Require multi-factor authentication (default). Bypass	authentication is not skipped.
<u>Read Release Notes</u> ದ Account ID 2910-6030-53	Groups	You don't have any editable groups. Add one. Groups can be used for management, reporting, and policy. Learn more about groups Ľ	
Deployment ID DUO63 ଫ Helpful Links Documentation ଫ User Guide ଫ Knowledge Base ଫ	Notes	For internal use.	

4. Em dispositivos do usuário, especifique o método de autenticação secundário.

Nota:Neste documento, é usado o método Duo push for mobile devices, de modo que é necessário adicionar um dispositivo telefônico.

Clique em Adicionar telefone.

You may rearrange the phones by dragging and dropping in the table. Learn more about activating a replacement phone [].	Add Phone
This user has no phones. Add one.	
Indpoints	
This user has no devices.	
Hardware Tokens	Add Hardware Token
This user has no hardware tokens. Add one.	
Bypass Codes	Add Bypass Code
This user has no bypass codes. Add one.	
NebAutha & 112E	Add Security Key

5. Digite o número de telefone do usuário e clique em Adicionar Telefone.

Dashboard > Users > duovpn > Add Phone

Add Phone



6. No painel Admin do Duo à esquerda, navegue até Usuários e clique no novo usuário.

Dashboard	Dashboard > Users						
Device Insight	Llooro			Director	Suna Import	Laoro Dulk Er	
Policies	Users			Director	y Sync 1 Import (USERS I DUIK ER	Add User
Applications	You have users where the series of the	ho have not activated Duo	Mobile. Click here to send them ad	ctivation links.			
Single Sign-On	Need to activate a	replacement phone? Lea	rn more about Reactivating Duo Mo	obile 🖸.			
Users ┥ ————							
Add User	5	0	2	1	0		0
Pending Enrollments	Total Users	Not Enrolled	Inactive Users	Trash	Bypass	Users	Locked Out
Bulk Enroll Users		_					
Import Users	Select (0) Y				Export ~	Q Search	
Directory Sync							
Bypass Codes	Username •	Name	Fmail	Phones	Tokens	Status	Last Login
Groups		Harre	Linus	Filones	TONOLIS	olatos	Last Login
Endpoints				1		Active	Mar 8, 2022 6:50 PM
2FA Devices				1		Active	Mar 5, 2022 7:04 PM
Trusted Endpoints							
Trust Monitor				1		Active	Never authenticated
Reports	duovpn		.com	1		Active	Never authenticated
Settings			e e.com	1		Active	Mar 5, 2022 7:16 PM
Need Help? Chat with Tech Support 다							

Nota:Caso não tenha acesso ao seu telefone no momento, você pode selecionar a opção de e-mail.

7.Navegue até a seção Telefones e clique em Ativate Duo Mobile.

Phones You may rearrange the phones by dragging and dropping in the table. Learn more about activating a replacement phone I.							
Alias	Device	Platform	Model	Security Warnings			
phone1	1000	Android 10	0.001 < 0.01	✓ No warnings	Activate Duo Mobile	Ê	

8. Clique em Gerar Código de Ativação Móvel Duo.



9. Selecione Email para receber as instruções por e-mail, digite seu endereço de e-mail e clique em Enviar Instruções por e-mail.

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allow: mobile device or authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the r

Phone	a di ka Wasaka
Send links via	SMS Email
Email	ay i mian ilin ven avan

10. Você receberá um e-mail com as instruções, conforme mostrado na imagem.



Don't have Duo Mobile yet? Install it first:

iPhone: https://itunes.apple.com/us/app/duo-mobile/id422663827

Android: https://play.google.com/store/apps/details?id=com.duosecurity.duomobile

11. Abra o Duo Mobile App a partir do seu dispositivo móvel e clique em Adicionar, selecione Usar código QR e digitalize o código a partir do e-mail de instruções.

12. O novo usuário é adicionado ao seu aplicativo móvel Duo.

Configuração do proxy de autenticação Duo

1.Baixe e instale o Duo Auth Proxy Manager em https://duo.com/docs/authproxy-reference.

Nota:Neste documento, o Duo Auth Proxy Manager está instalado no mesmo Windows Server que hospeda os serviços do Ative Diretory.

2.No Painel de administração do Duo, navegue para Aplicativos e clique em Proteger um aplicativo.



3. Na barra de pesquisa, procure por Cisco ISE Radius.

Protect an Application

0	Add an application that you'd like to protect with Duo two-factor authentication. You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the only one that will see it, until you decide to add others. Documentation: Getting Started C Choose an application below to get started.								
ise Applica	isel Application Protection Type								
(Akamal	Akamai Enterprise Application Access	2FA	Documentation 🗹 Protect						
alialia cisco	Cisco ISE RADIUS	2FA	Documentation D Protect						

4. Copie a Chave de integração, a Chave de segurança e o Nome de host da API. Essas informações são necessárias para a configuração do Proxy de autenticação Duo.

Successfully added Cisco ISE RADIUS to protected applications. Add another.

Dashboard > Applications > Cisco ISE RADIUS 1

Cisco ISE RADIUS 1

Follow the Cisco ISE RADIUS instructions ⊡.

Details

~

Integration key	5.00040a.00001/1012002447	Сору
Secret key	•••••W6ho	Сору
	Don't write down your secret key or share it with an	yone.
API hostname	(343,0700,022,022,024,074),0273	Сору

5. Execute o aplicativo Duo Authentication Proxy Manager e conclua a configuração do cliente do Ative Diretory e do ISE Radius Server e clique em Validate.

Observação: se a validação não for bem-sucedida, consulte a guia debug para obter detalhes e corrija-a de acordo.

Authentication Proxy is running Up since: 3/5/2022, 9/23.04 AM	Duo Authentication Proxy Manager	- 🗆 X
Validation passed Configuration has passed validation and is ready to be saved Output 20 Configure: authproxycfg Unsaved Changes Output 21 in umber to the section name (e.g. [ad_client2]) Running The Duo Authentication Proxy Connectivity Tool. This may take several minutes 21 host=10.28.17.107 22 service_account_password= Maximistrator 23 service_account_password= Maximistrator 24 search_dn=DC=agarciam,DC=cisco 25 (radius_server_auto] 26 (radius_server_auto] 27 ikey=UTTC*UTE*Lt^fil*Lif*: 28 skey=UTTC*UTE*Lt^fil*Lif*: 29 api_host=api_mix*Lif*: 29 api_host=api_mix*Lif*: 29 api_host=api_mix*Lif*: 29 api_host=api_mix*Lif*: 29 api_host=api_mix*Lif*: 20 failmode=safe 38 client=ad_client 39 pit=1812 30 client=ad_client 30 client=ad_client 310 Testing section 'radius_server_auto' with configuration: 310 infoj Testing section 'radius_server_auto' with conf	Authentication Proxy is running Up since: 3/5/2022, 9:23:04 AM	Version: 5.6.0 Update your Authentication Proxy Stop Service
Configure: authproxy.cfgUnsaved ChangesOutput18; number to the section name (e.g. [ad_client2])Running The Duo Authentication Proxy Connectivity Tool. This may take several minutes20[ad_client]Running The Duo Authentication Proxy Connectivity Tool. This may take several minutes21host=10.28.17.10722service_account_username=Administrator23service_account_username=Administrator24search_dn=DC=agarciam,DC=cisco25	Validation passed Configuration has passed validation and is ready to be saved	
<pre>18 ; number to the section name (e.g. [ad_client2]) 19 19 19 19 19 20 [ad_client] 21 host=10.28.17.107 23 service_account_username=Administrator 23 service_account_password= PExtmn Lr1 24 search_dn=DC=agarciam,DC=cisco 25 26 27 27 28 29 29 29 29 29 20 20 20 20 20 20 20 20 20 20 20 20 20</pre>	Configure: authproxy.cfg Unsav	red Changes Output
Validate Save Learn how to configure the Authentication Provy	<pre>18 ; number to the section name (e.g. [ad_client2]) 19 20 [ad_client] 21 host=10.28.17.107 22 service_account_username=Administrator 23 service_account_password= HEAMTLAFI 24 search_dn=DC=agarciam,DC=cisco 25 26 [radius_server_auto] 27 ikey=UntolatelLAATMINAT 28 skey=X0+07x18jAZD*HTTpZ7i6AAF6xHn1V2papeWrCdp 29 api_host=api_uf704730.cluvet.urlty.tom 30 radius_ip_1=10.28.17.101 31 radius_secret_1=Wextph117! 32 failmode=safe 33 client=ad_client 34 port=1812 35 36 36 37 38 38 38 39 39 30 30 30 30 30 30 30 30 30 30 30 30 30</pre>	Running The Duo Authentication Proxy Connectivity Tool. This may take several minutes [info] Testing section 'main' with configuration: [info] ['debug': 'True', 'log_max_files': '10', 'log_max_files': '20971520', 'test_connectivity_on_startup': 'true'} [info] There are no configuration problems [info] Testing section 'ad_client' with configuration: [info] There are no configuration problems [info] There are no configuration problems [info] Testing section 'radius_server_auto' with configuration: [info] Testing section 'radius_server_auto' with configuration: [info] Testing section 'radius_server_auto' with configuration:

Configurações do Cisco ISE

1. Faça login no portal do administrador do ISE.

2.Expanda a guia Cisco ISE e navegue até Administration, clique em Network Resources e clique em External RADIUS Servers.

Cisco ISE -	Q What page are you looking for?				
Dashboard	Context Visibility	Operations	-Policy-	Administration	
Recent Pages External Identity Sources Policy Sets Network Device Profiles External RADIUS Servers RADIUS Server Sequences Live Logs	System Deployment Licensing Certificates Logging Maintenance Upgrade		Network Resources Network Devices Network Device Crow Network Device Prof External RADIUS Ser RADIUS Server Sequ NAC Managers	ins iles vers encs	
	Health Checks Backup & Restore		External MDM Location Services		

3. Na guia External Radius Servers, clique em Add.

■ Cisco ISE	Administration · Network Resources						
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences			
External R	ADIUS Servers		1				
	🗍 Duplicate 🌐 Delete						
Name Name:	Currently Sorted	Description					

4. Preencha a lacuna com a configuração RADIUS usada no Duo Authentication Proxy Manager e clique em Submit.

Network Devices Network	rk Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	More
* Name	DUO_NEW						
Description			Æ				
* Host IP	10.28.17.107						
* Shared Secret	········ -	Show					
Enable KeyWrap							
* Key Encryption Key		Show					
* Message Authenticator Code Key	(Show					
Key Input Format	o ascii 🔿 hexa	DECIMAL					
* Authentication Port	1812	(Valid Range 1 to 6	5535)				
* Accounting Port	1813	(Valid Range 1 to 6	5535)				
* Server Timeout	5	Seconds (Valid Ra	nge 1 to 120)				
* Connection Attempts	3	(Valid Range 1 to 9	9)				
Radius ProxyFailover Expiration	300	(valid Range 1	to 600)				
						Su	bmit

5. Navegue até a guia RADIUS Server Sequences e clique em Add.

■ Cisco ISE	Administration • Network Resources						
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences			
RADIUS Se		Î					

6. Especifique o nome da sequência e atribua o novo servidor Externo RADIUS, clique em Enviar.

RADIUS Server Sequences List > New RADIUS Server Sequence

RADIUS Server Sequence



✓ User Selected Service Type

Select the set of external RADIUS servers to use to process requests. Servers are accessed in sequence until a response is r



7. Navegue do menu Painel para Política e clique em Conjuntos de Políticas.



8. Atribua a Sequência RADIUS à política default.

Nota:Neste documento, a sequência Duo para todas as conexões é aplicada, de modo que a política Padrão é usada. A atribuição de políticas pode variar de acordo com os requisitos.

Policy Sets					Reset Policyset H	litcount
🕂 Status	Policy Set Name	Description	Co	nditions	Allowed Protocols / Server Sequence	e Hits
Q Search	(
٢	81.91W		Ŧ	Radius-User-Name EQUALS isevpn	Default Network Access	3
٢	18.1			Radius-NAS-Port-Type EQUALS Virtual	DUO_Sequence	22
٢	Default	Default policy set			Default Network Access $\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	0
	1 I				≣Q	•
	1				Allowed Protocols	eset
					Default Network Access Proxy Sequence	
					DUO_NEW	
					DUO Sequence	

Configuração do Cisco ASA RADIUS/ISE

1. Configure o ISE RADIUS Server em grupos de servidores AAA, navegue para Configuration, clique em Device Management e expanda a seção Users/AAA, selecione AAA Server Groups.

o t avi	Home Configuration Monitoring Save Device Lip Beokmarks Bookmarks bookmark a page, right-click on a node in the agation tree and select "Add to bookmarks". Go The Delete	Refresh Ba	ack () ation : ips Pro RA LO
0	O O Device Management		
>	Management Access		
>	8 Licensing		
>	System Image/Configuration		
>	High Availability and Scalability		
>		Find:	
	Smart Call-Home		
	Security	Servers in the Se	elected
	Service Module Settings	Server Name or IP	Addres
0		10 28 17 101	Addre:
	19 AAA Server Groups	10.20.17.101	
	Se I DAP Attribute Map		
	AAA Kerberos		
	Authentication Prompt		
	🗣 AAA Access		
	Dvnamic Access Policies		
	User Accounts		
	A Password Policy		
	G Change My Password		
	Login History		
5	Certificate Management		
>	P DHCP		
	B DNS		
Σ	UND TO THE REAL PROPERTY OF TH		

, selecione o nome da interface, especifique o endereço IP do ISE Server e digite a chave secreta RADIUS e clique em Ok.

Solution Proxy Manager.

• •	Edit AAA Server
Server Group: IS	SE outside
Server Name or IP Address:	10.28.17.101
Timeout:	10 seconds
RADIUS Parameters	
Server Authentication Port:	1645
Server Accounting Port:	1646
Retry Interval:	10 seconds
Server Secret Key:	•••••
Common Password:	
ACL Netmask Convert:	Standard 😌
Microsoft CHAPv2 Capable	: 🔽
SDI Messages	
Message Table	×
Help	Cancel OK

Configuração de CLI.

aaa-server ISE protocol radius
dynamic-authorization
aaa-server ISE (outside) host 10.28.17.101
key *****

Configuração de VPN de acesso remoto do Cisco ASA

ip local pool agarciam-pool 192.168.17.1-192.168.17.100 mask 255.255.255.0
group-policy DUO internal
group-policy DUO attributes
banner value This connection is for DUO authorized users only!
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split-agarciam
address-pools value agarciam-pool
tunnel-group ISE-users type remote-access
tunnel-group ISE-users general-attributes
address-pool agarciam-pool
authentication-server-group ISE
default-group-policy DUO
tunnel-group ISE-users webvpn-attributes
group-alias ISE enable

Teste

dns-group DNS-CISCO

1. Abra o aplicativo Anyconnect em seu dispositivo de PC. Especifique o nome de host do VPN ASA Headend e faça login com o usuário criado para a autenticação secundária Duo e clique em OK.

000	Sec	AnyConnect ure Mobility Client	cisco	
	VPN: Please enter yo	ur username and passw	ord.	
	Cisco A	nyConnect 192.168	3.100.100	
	Please enter your	username and passw	ord.	
	Group:	ISE	-	0
	msgstringESMEX	duovpn	-	
	MEX-PASS	••••		
			Cancel	

2. Você recebeu uma notificação por push Duo no dispositivo móvel Duo do usuário especificado.

3. Abra a notificação do aplicativo móvel Duo e clique em Aprovar.





4. Aceite o banner e a conexão será estabelecida.





Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

O Duo Authentication Proxy é fornecido com uma ferramenta de depuração que exibe os motivos

de erros e falhas.

Depurações de trabalho

Nota:As próximas informações são armazenadas em C:\Program Files\Duo Security Authentication Proxy\log\connectivity_tool.log.

Output	
Running	The Duo Authentication Proxy Connectivity Tool. This may take several minutes
[info]	Testing section 'main' with configuration:
[info]	{'debug': 'True',
	'log_max_files': '10',
	'log_max_size': '20971520',
	<pre>'test_connectivity_on_startup': 'true'}</pre>
[info]	There are no configuration problems
[info]	
[info]	Testing section 'ad_client' with configuration:
[info]	{'debug': 'True',
	'host': '10.28.17.107',
	'search_dn': 'DC=agarciam,DC=cisco',
	'service_account_password': '*****',
	'service_account_username': 'Administrator'}
[info]	There are no configuration problems

```
[info]
        Testing section 'radius_server_auto' with configuration:
[info]
        {'api_host': 'apl affect?'Laboratelly.com',
[info]
         'client': 'ad_client',
         'debug': 'True',
         'failmode': 'safe',
         'ikey': Lange Lot Manager ...
         'port': '1812',
         'radius_ip_1': '10.28.17.101',
         'radius_secret_1': '******',
         'skey': '********[40]'}
        There are no configuration problems
[info]
[info] Testing section 'main' with configuration:
[info] {'debug': 'True',
         'log_max_files': '10',
         'log_max_size': '20971520',
         'test_connectivity_on_startup': 'true'}
[info] There are no connectivity problems with the section.
```

```
[info] There are no connectivity problems with the section.
[info]
[info] Testing section 'ad_client' with configuration:
[info] {'debug': 'True',
         'host': '10.28.17.107',
         'search_dn': 'DC=agarciam,DC=cisco',
         'service_account_password': '******',
         'service_account_username': 'Administrator'}
       The LDAP Client section has no connectivity issues.
[info]
[info]
[info] Testing section 'radius_server_auto' with configuration:
[info] {'api_host': 'asi_adicate dissecurity.cmp',
         'client': 'ad_client',
         'debug': 'True',
         'failmode': 'safe',
         'ikey': ""There's Northern Science and the
         'port': '1812',
         'radius_ip_1': '10.28.17.101',
         'radius_secret_1': '******',
         'skey': '****** [40]'}
        The RADIUS Server has no connectivity problems.
[info]
[info]
[info] SUMMARY
[info] No issues detected
```

1. Problemas de conectividade, IP incorreto, FQDN/Nome de Host não resolvível na configuração do Ative Diretory.

Output

'host': '10.28.17.106', 'search_dn': 'DC=agarciam,DC=cisco', 'service_account_password': '*****', 'service_account_username': 'Administrator'} [warn] The LDAP Client section has connectivity problems. [warn] The LDAP host clear connection to 10.28.17.106:389 has connectivity problems. [error] The Auth Proxy was not able to establish a connection to 10 .28.17.106:389.

2. Senha incorreta para usuário Administrador no Ative Diretory.



Debugs.

The Auth Proxy was able to establish a connection to 10.28.17
.107:389.
The Auth Proxy was able to establish an LDAP connection to 10
.28.17.107:389.
The Auth Proxy was unable to bind as Administrator.
Please ensure that the provided service account credentials
are correct.
Exception: invalidCredentials: 8009030C: LdapErr: DSID
-0C090516, comment: AcceptSecurityContext error, data 52e,
v3839 <mark>-</mark>
The Auth Proxy did not run the search check because of the
problem(s) with the bind check. Resolve that issue and rerun
the tester.

3. Domínio Base Incorreto.



Debugs.



4. Valor de RADIUS ikey errado.

[radius_server_auto]
ikey=U_NUL_LAHRNZ6EZ1
skey=Jackingen I findu. Die 1961 Juny: die status die state
api_host=apl = 🗖 📲 🖬 🖬 🖛 🖜 ity.com
radius_ip_1=10.28.17.101
<pre>radius_secret_1=!Mexvpn!17!</pre>
failmode=safe
client=ad_client
port=1812

Debugs

	and a summinely
[error]	The ikey value provided is invalid.
[info]	
[info]	SUMMARY
[warn]	Checks for external connectivity were not run. Please fix the
	configuration and try again.

5. Verifique se o Servidor ISE envia pacotes de Solicitação de Acesso.

*Ethernet0

File	e Edi	t View	Go	Capture	Analyze	Statistics	Telephony	Wireless	Tools I	Help			
1		. 💿		XC	٩ 👳 ه	e 🗟 🖗	£ 🗐 🔳	ଭ୍ର	Q. 🔢				
	radus												
No.		Time		Source	e		Destination		Protocol	Length	Info	<u> </u>	
	1511.	6020.	521457	10.2	8.17.101		10.28.17.10	37	RADIUS	877	Access-Reque	st 刘-31	
4	1513.	. 6024.	344735	10.2	8.17.107		10.28.17.10	91	RADIUS	191	Access Accep	t id=31	
>	Frame	151119	5: 877	bytes o	on wire (7016 bit	s), 877 byt	es captu	red (7016	5 bits)	on interface	\Device\NPF	{CA092CEE-5
>	Ether	net II,	Src:	Whene	b3:a4:21	(00:50:	56:b3:a4:2f), Dst:	Where_b	3:b4:3e	(00:50:56:b3	:b4:3e)	
>	Internet Protocol Version 4, Src: 10.28.17.101, Dst: 10.28.17.107												
>	User	Datagra	m Pro	tocol, S	Src Port:	42022,	Dst Port: 1	812					
~	RADIU	S Proto	col										
	Co	de: Acc	ess-R	equest ((1)								
	Pa	cket id	entif.	ier: 0x1	lf (31)								
	Le	ngth: 8	335										
	Au	thentic	ator:	38a28ca	3ca6bbc2	61819c53	84b1be6e3						
	11	he resp	onse	to this	request	is in fra	ame 151332]						
	✓ At	tribute	Valu	e Pairs									
	>	AVP: t	=User	-Name(1)	1=8 val	=duovpn	-						
	>	AVP: t	=User	-Passwor	d(2) 1=1	8 val=End	crypted						
	>	AVP: t	=NAS-1	IP-Addre	ss(4) 1=	6 val=192	2.168.100.1	99					
	>	AVP: t	=NAS-1	Port(5)	l=6 val=	344064							
	>	AVP: t	=Calle	ed-Stati	on-Id(30) 1=17 va	al=192.168.	100.100					
	>	AVP: t	=Call:	ing-Stat	ion-Id(3	1) 1=13 v	al M.H.C						
	>	AVP: t	=Proxy	y-State(33) 1=25	val=4669	97273745072	6f78793d	31302e323	82e3137	2e313031		
	2	AVP: t	=Prox	y-State(33) 1=76	val=4369	973636f2053	65637572	652041435	3373665	35323735612d	96362302d31	3165632d63
	>	AVP: t	=NAS-I	Port-Typ	e(61) 1=	6 val=Vir	rtual(5)						
	>	AVP: t	=Tunne	el-Clien	t-Endpoi	nt(66) l	13 val=10.	99.65.53					

6. Para confirmar o funcionamento do servidor de Proxy de Autenticação Duo, Duo fornece a ferramenta <u>NTRadPing</u> para simular pacotes de solicitação de acesso e resposta com Duo.

6.1 Instale o NTRadPing em um PC diferente e gere tráfego.

Nota:Neste exemplo, a máquina com Windows 10.28.17.3 é usada.

6.2 Configure com os atributos usados na configuração do ISE Radius.

INTRadPing Test Utility	– 🗆 X				
RADIUS Server/port 10.28.17.107	NTRadPing 1.5 - RADIUS Server Testing Tool © 1999-2003 Master Soft SpA - Italy - All rights reserved http://www.dialways.com/				
Reply timeout (sec.): 3 Retries: 6					
RADIUS Secret key: Harmy F i					
User-Name: duovpn					
Password: CHAP	MASTERSOFT DIALWAYS				
Request type: Authentication Request 💌 0	RADIUS Server reply:				
Additional RADIUS Attributes:	See Super-Stational and the second 22 2012 1022 Instantian a served work of the second 12 2012 1022 In a second second to the school area should (1) the second second second second (1) and we can even the school of 7000 - Bandward www.caref.color(second school) algorization to device of the school algorization to device of the				
Add Remove Clear list Load Save	Send Help Close				

6.3 Configure o Duo Authentication Proxy Manager da seguinte maneira:

[radius_server_auto]
ikey="Thereore "Isonne" and
skey=Jac3
api_host=ani=nd7c172n.dumnerinify.com
<pre>radius_ip_1=10.28.17.101</pre>
<pre>radius_secret_1=!Mex.um!17!</pre>
radius_ip_2=10.28.17.3
<pre>radius_secret_2=!Mexil 17!</pre>

6.4. Navegue até a ferramenta NTRadPing e clique em Send. Você recebe uma notificação por push Duo no dispositivo móvel atribuído.

INTRadPing Test	Utility		- 🗆 X
RADIUS Server/port:	10.28.17.107	1812	NTRadPing 1.5 - RADIUS Server Testing Tool © 1999-2003 Master Soft SpA - Italy - All rights reserved
Reply timeout (sec.):	3 Ret	ries: 6	http://www.dialways.com/
RADIUS Secret key:	!Mexvpn!17!		ms
User-Name:	duovpn		
Password:	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	CHAP	MASTERSOFT DIALWAYS
Request type:	Authentication Request 💌	0	RADIUS Server reply:
Additional RADIUS A	ttributes:		Sending authentication request to server 10.28.17.107:1812 Transmitting packet, code=1 id=12 length=46 no response from server (uned out), non-offerent (#1) received response from the server in 4000 milliseconds reply packet code=2 id=12 length=49 response: Access:Accept attribute dump Reply-Message=Success. Logging you in
Add Remove	e Clear list Load	Save	Send Help Close

	700 20.866684	10.28.17.3	10.28.17.107	RADIUS	88 Access-Request id=13,	, Duplicate Request	
ąL	737 22.184895	10.28.17.107	10.28.17.3	RADIUS	90 Access-Accept id=13	←	
>	Frame 700: 88 byte	s on wire (704 bit:	s), 88 bytes captured	(704 bits) on	interface \Device\NPF {CA	092CEE-5528-4E0A-9310-2D523160DD60	}, id 0
>	Ethernet II, Src:	VMware_b3:f2:72 (00	0:50:56:b3:f2:72), Dst	: VMware_b3:b	4:3e (00:50:56:b3:b4:3e)		
>	Internet Protocol	Version 4, Src: 10	.28.17.3, Dst: 10.28.1	7.107			
>	User Datagram Prot	cocol, Src Port: 51	188, Dst Port: 1812				
~	RADIUS Protocol						
	Code: Access-Re	quest (1)					
	Packet identifi	er: 0xd (13)					
	Length: 46						
	Authenticator:	2020202020203136343	36393335333230				
	[Duplicate Requ	est Frame Number: 5	532]				
	[The response t	to this request is i	in frame 737]				
	✓ Attribute Value	Pairs					
	> AVP: t=User-	Name(1) l=8 val=duc	ovpn				
	> AVP: t=User-	Password(2) l=18 va	al=Encrypted				
1							

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.