ASDM يف نمآلا ليمعلا IKEv2/ASA نيوكت CERT ةقداصم ؛& AAA مادختساب

تايوتحملا

<u>ةمدقملا</u> <u>قىساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسملا تانوكملا</u> <u>ةكبشلل ىطىطختلا مسرلا</u> <u>تانىوكتلا</u> <u>ASDM يف نيوكتال</u> <u>VPN تاجلاعم حتف 1 ةوطخلا</u> <u>لاصتالا في عت فلم في عت 2 ةوطخلا</u> <u>VPN تالوكوتورب .3 ةوطخلا</u> <u>ليمعالا روص .4 ةوطخاا</u> <u>ققداصملا بيلاساً .5 قوطخلا</u> <u>SAML نېوكت .6 ةوطخلا</u> ليمعلا ناونع نييعت .7 ةوطخلا <u>تاكبش لا عامس ألى لحت مداوخ .8 ةوطخلا</u> <u>NAT ءافعا .9 ةوطخلا</u> <u>ءالمعلل نمآ رشن .10 ةوطخلا</u> <u>تادادعالا ظفح 11 ةوطخلا</u> <u>ەرىدصتو نمآلا لېمعلا فېرعت فلم دېكات .12 ةوطخلا</u> <u>نمآلا ليمعلا فيرعت فلم ليصافت ديكأت .13 ةوطخلا</u> <u>ASA CLI يف تادادعالا دېكأت .14 ةوطخلا</u> <u>رىڧشت قېمزراوخ ةڧاض| .15 قوطخل|</u> <u>Windows مداخ يف نيوكتا ا</u> <u>ISE يف نيوكتلا</u> <u>زامج ةفاض| .1 ةوطخلا</u> Active Directory ةفاضا. 2 ةوطخاا <u>قېوەلا ردصم قلسلس قفاضا .3 قوطخلا</u> <u>جەن ةعومجم ةفاض| .4 ةوطخل|</u> <u>ةقداصما اجهن ةفاضا .5 ةوطخاا</u> <u>ليوختارا جون ةفاضا .6 ةوطخارا</u> <u>قحصالا نم ققحتاا</u> <u>Win10 PC1 ىل نمآلا لىمعلا في عت فلم خسنا 1. قوطخلا</u> <u>VPN لاصتا ءدب .2 ةوطخلا</u> ASA <u>ىلع Syslog دىكأت .3 ةوطخلا</u> ASA يلع IPsec لمع ةس لج ديكأت .4 ةوطخلا Radius Live ل<u>جس ديكأت .5 ةوطخلا</u> <u>امحالصاو ءاطخألا فاشكتسا</u> <u>VPN لاصتا ءدب .1 ةوطخلا</u> <u>CLI يف Syslog دىكأت .2 ةوطخلا</u> عجرما

ةمدقملا

مادختساب ASA ىلع IKEv2 ربع نمآلا ليمعلا نيوكتل ةمزاللاا تاوطخلا دنتسملا اذه فصي ASDM مادختساب AAA مادختساب.

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- Cisco (ISE) نم ةيوهلا تامدخ كرحم نيوكت
- نم (ASAv) ةلدعملا ةيرهاظلا نامألا ةزهجأ نيوكت
- Cisco نم (ASDM) ةلدعملا نامألا ةزَّهجأ ريدم نيوكت •
- VPN ةقداصم قفدت •

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست

- حيحصتالا جمانرب Identity Services Engine Virtual 3.3 1
- 9.20(2)21 فيكتال لباقلا يُرهاظا نامأُلاً زاهج
- Adaptive Security Device Manager 7.20(2)
- Cisco Secure Client 5.1.3.62
- ليغشتلا ماظن Windows Server 2016
- Windows 10 ليغُشتلا مُاظن •

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

ةكبشلل يطيطختلا مسرلا

دنتسملا اذه لاثمل همادختسا متي يذلا ططخملا ةروصلا هذه ضرعت.

متي يذلاو ،ad.rem-system.com وه Windows Server 2016 ىلع ەنيوكت مت يذلا لاجملا مسا دنتسملا اذه يف لاثمك ەمادختسإ.



ةكبشلل يطيطختلا مسرلا

تانيوكتلا

ASDM يف نيوكتلا

VPN تاجلاعم حتف .1 ةوطخلا

.نمآلا ليمعلاب ةصاخلا VPN ةكبش جلاعم قوف رقنا ،VPN تاجلاعم < تاجلاعملا ىلإ لقتنا



(يلاتلا) Next قوف رقنا.

Secure Client VPN Conne	ction Setup Wizard	\times
VPN Wizard	Introduction Use this wizard to configure the ASA to accept VPN connections from the Secure VPN Clent. The connections will be protect when a VPN connection is established. VPN Remote Access Configure the Connection is established.	ed
	< Back Next > Riff Help	

يلاتلا رزلا قوف رقنا

لاصتالا فيرعت فلم فيرعت .2 ةوطخلا

لاصتالا فيرعت فلمل لاخدالا تامولعم. لاصتالا فيرعت فلم مسا: vpn-ips-tunnel-grp جراخ : VPN يلإ لوصولا ةمجاو

Secure Client VPN Conne	ction Setup Wizard	×
Secure Client VPN Connel Steps	ction Setup Wizard Connection Profile Identification This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN connections. Connection Profile Name: vpn-ipsec-tunnel-grp VPN Access Interface: outside v	×
10. Secure Client Deployme 11. Summary	< Back Mext > II:17 Help	,

لاصتالا فيرعت فلم فيرعت

VPN تالوكوتورب .3 ةوطخلا

.ةديدج ايتاذ ةعقوم ةداهش ةفاضإل ةفاضإ رز قوف رقنا ،IPsec ددح

Secure Client VPN Conn	ection Setup Wizard	Manage Identity Certificates
Steps	VPN Protocols	Iccued To, Iccued By, Evniny Date, Accordiated Toutmainte, Ukane, Duble Key Tune, Add
1. Introduction	Secure Client can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to sumport.	Show Details
 Connection Profile Identification 	means and care contractions and an adaption of	Delate
3. VPN Protocols	59.	
 Client Images 	IPsec	Export
Authentication Methods	Device Certificate	Install
Client Address Assignme	Device certificate identifies the ASA to the remote access clients. Certain Secure Client Features (Always-On, IPsec/IKEv2) require that valid device certificate be	Re-Enroll
Network Name Resolutio	available on the ASA.	
Servers	Device Certificate: None V Manage	
0. Secure Client Deployme		
1. Summary		
		End: O O Match Case
		Certificate Expiration Alerts
		Send the first alert before : 60 (days) Set Default
	< gack Next > Ukin Help	Repeat Alert Interval : 7 (days)
		Weak Crypto Configurations
		Permit Weak key sizes and Hash Algorithms
		Public CA Enrolment
		Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust
		offers Cisco customers a special promotional price for certificates and trial certificates for testing.
		Enros ASA SSL certificate with Entrust
		Using a previously saved certificate signing request, <u>enrol with Entrust</u> ,
		ASDM Identity Certificate Wizard
		ASDM through launcher.
		Launch ASDM Identity Certificate Wizard
		OK. Cancel Help

ايتاذ ةعقوملا ةداەشلل تامولعم لاخدا.

مسا TrustPoint: vpn-ipsEc-TrustPoint

IPSec-KP : حيتافملا جوز

Ta Add Identity Certificate X	To Add Key Pair	×
Trustpoint Name: vpn-ipsec-trustpoint	Key Type: O RSA O ECDSA O EDDSA	
Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):		
Decryption Passphrase:	Name: Use default key pair name	
File to Import From: Browse	Enter new key pair name: lpsec-kp	
• Add a new identity certificate:	Size: 4096 V	
Key Pair: ipsec-kp	Usage: O General purpose O Special	
Certificate Subject DN: CN=ciscoasa Select		
Generate self-signed certificate Generate self-signed certificate Act as local certificate authority and issue dynamic certificates to TLS-Proxy	Generate Now Cancel Help	
Advanced		
C Enable CA flag in basic constraints extension		
Add Certificate Cancel Help		

ايتاذ ةعقوملا ةداهشلا ليصافت

رز كلذ دعب تقطقط ،VPN تالوكوتورب دادعإ ةيلمعلا تدكأ.

Secure Client VPN Conne	ction Setup Wizard	×
Steps 1. Introduction 2. Connection Profile Identification J. VPN Protocols 4. Client Images 5. Authentication Methods 6. SAML Configuration 7. Client Address Assignme 8. Network Name Resolutio Servers 9. NAT Exempt 10. Secure Client Deployme 11. Summary	VPN Protocols Secure Client can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols would like this connection profile to support. SSL Image: SSL Device Certificate Device Certificate identifies the ASA to the remote access clients. Certain Secure Client features (Always-On, IPsec/INEV2) require that valid device certificate be available on the ASA. Device Certificate I vpn-ipsec-trustpoint:unstructuredNam Manage	you
	< Back Next > It in Hel	P

VPN لوكوتورب تادادعإ ديكأت

ليمعلا روص .4 ةوطخلا

يلاتا رزلا قوف رقنا ،ةنمآ ليمع ةروص ةفاضإل رز ةفاضإ قوف رقنا.

Secure Client VPN Conne	ction Setup Wizard	×
Steps	Client Images	
1. Introduction	ASA can automatically upload the latest Secure Client package to	the client device when it accesses the enterprise network.
2. Connection Profile Identification	A regular expression can be used to match the user-agent of a br You can also minimize connection setup time by moving the image	owser to an image. used by the most commonly encountered operation system to
3. VPN Protocols	the top of the list.	
4. Client Images	A super sub the sub of the	
5. Authentication Methods	Add Keplace Delete 7 +	
6. SAML Configuration	Image	Regular expression to match user-agent
7. Client Address Assignme	disk0:/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg	
8. Network Name Resolutio Servers		
9. NAT Exempt		
10. Secure Client Deployme		
11. Summary		
	You can download Secure Client packages from Cisco by searchin	g 'Secure Mobility Client' or <u>click here</u> ,
	< gack Next >	Riff Help

ليمعلا روص

ةقداصملا بيلاسأ .5 ةوطخلا

.يلاتا رزلا قوف رقنا ،ديدج AAA مداخ ةفاضإل ديدج رز قوف رقنا

RADIUS-GRP : مداوخلا ةعومجم مسا

RADIUS :ةقداصملا لوكوتورب

1.x.x.191 :مداخلل IP ناونع

لخادلا : ةەجاولا

Secure Client VPN Conn	ection Setup Waard	a New Authentication Server Group	×	Secure Client VPN Conne	ction Setup Wizard
Para 1. District Conference on Conference Control Conference on Conference 2. Units Protocols 6. One of Longent Mathematic Conference Mathematics 1. Second Conference Second Co	Authoritosen Helhold Heli holg bis you avail heli holg authoritosten nerve- thor de néo nerve heli holg heli heli heli heli heli heli heli heli	Create a new authentication server group containing one authentication To add more servers to the group or change other AdA server resting Configuration D Device Management > Useral/AdA > AdA Server Group Server Group Name: Authentication Protocol: Server IP Address: Interface: Interface:	on server. 8, go to ps.	2945 1. Partodotton 2. Constituto Public Mathematical 3. WHP Instands 3. WHP Instands 3. Mathematical 5. Mathematical 5. Mathematical 5. Mathematical 5. Mathematical 10. Secure Clerk Diployme 11. Summay	Authentication Helholds This top lates you specify the function of the authentication server. Tou concludio tells Pass * National is could a series sorrer group. AAA forms' Grappi (make gg) Team AAA forms' Grappi Teal AAA forms' Grappi Teal AAA forms' Grappi Teal Series Teal
	(gal (gal) (Server Secret Key: Confirm Server Secret Key:			<pre>cpd (yet>)</pre>
		OK Cancel Help			

SAML نيوكت .6 ةوطخلا

رز كلذ دعب تقطقط.

Secure Client VPN Conne	ction Setup Wizard	×
Steps	SAML Configuration	
 Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods SAML Configuration Client Address Assignme Network Name Resolutio Servers NAT Exempt Secure Client Deployme Summary 	SAPE. Comparation This step allows you to configure a SAML and the authentication method. Authentication Method: AAA AAA Server Group: radus-grp Use LOCAL if Server Group fails SAML Identity Provider SAML Server : None Manage	
	< gack Next > Rifl H	alp

SAML نيوكت

ليمعلا ناونع نييعت .7 ةوطخلا

يلاتال رزلا قوف رقنا ،ديدج IPv4 عمجت ةفاضإل ديدج رز قوف رقنا.

vPN-IPSec-pool :مسال

172.16.1.20 :يلوألI IP ناونع

IP: 172.16.1.30 ناونع ةياەن

255.255.255.2 :ةيعرفلا ةكبشلا عانق

To Secure Client VPN Conne	ection Setup Wizard			×	Secure Client VPN Conne	nection Setup Wizard	×
Steps I. Introduction C. Connection Prolife Identification VPIP Protocols C. VPIP Protocols S. Authentication Methods S. Authentication Methods S. SAPL. Configuration C. Client. Address Assignment S. Horizon Klame Resolutio Servers N. NAT Exempt S. Secure Client Deployme S. Summary S. Summary I. Summary	Clerk Address Assignment This step allows you to create a new address pool or be assigned addresses from the pools when they cor IPV6 address pool is only supported for 55L connects IPV6 address Pool Address Pool Address Pool Details of the selected address pool	select an existing address nect. on. Add IPv4 Pool Name: Skarting IP Address Ending IP Address Submet Mask: OK	s pool for IPv4 and IPv6. The Secure Clents w vpri-ipsec-pool 172:16:1:20 172:16:1:30 255:255:255.01 Cancel Help	×	Skeps I. Untroduction C. Connection Profile Identification VHM Protocols S. Authentication Methods S. Authentication Methods G. SMML Configuration T. Client Address Assignments Nethods Reveal Nethods Reveal Nethods Reveal Nethods Reveal Nethods Reveal Nethods Reveal Secure Client Deployme S. Summary Secure Client Deployme Secure Client Secure Clien	Clerk Address Assignment This sites allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The Secure Clerks will be assigned address pool is only supported for SSL connection. IPv6 address Pool Address Pool Rating IP Address: Details of the selected address pool Rating IP Address: 172.16.1.30 - Subnet Mask: 255.255.0 -	ſ
	< Back Next >		Rtifl Help			<back next=""> 限闭 Help</back>	

ليمعلا ناونع نييعت

تاكبشلا ءامسأ ليلحت مداوخ .8 ةوطخلا

.يلاتال رزلا قوف رقنا ،لاجملاو DNS ل تامولعم لاخدا

DNS: 1.x.x.57 مداوخ

d.rem-system.com :لاجملا مسا

Steps Network Name Resolution Servers 1. Introduction This step lets you specify how domain names are resolved for the remote user when accessing the internal network. 2. Connection Profile Identification DNS Servers: 1.10200.57 3. VPN Protocols WINS Servers: 1.000000000000000000000000000000000000	Secure Client VPN Conn	ction Setup Wizard	×
1. Introduction This step lets you specify how domain names are resolved for the remote user when accessing the internal network. 2. Connection Profile Identification DNS Servers: 1.10200.57 3. VPN Protocols WINS Servers: 0 4. Client Images Domain Name: ad.rem-system.com	Steps	Network Name Resolution Servers	
5. Authentication Methods 6. SAML Configuration 7. Client Address Assignme 8. Network Name Resolution Servers 9. NAT Exempt 10. Secure Client Deployme 11. Summary	 Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods SAML Configuration Client Address Assignme Network Name Resolution Servers NAT Exempt Secure Client Deployme Summary 	This step lets you specify how domain names are resolved for the remote user when accessing the internal network. DNS Servers: UNS Servers: Domain Name: ad.rem-system.com	
< Back Next > 用的 Help		< gack Next > Rifl H	telp

تاكبشلا ءامسأ ليلحت مداوخ

NAT ءافعإ .9 ةوطخلا

رز كلذ دعب تقطقط.

Secure Client VPN Conne	ection Setup Wizard	×
Steps	NAT Exempt	
 Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods SAML Configuration Client Address Assignme 	If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.	
 Network Name Resolutio Servers NAT Exempt 		
 Secure Client Deployme Summary 		
	< gack Next > 取消	Help

NAT ءافعإ

ءالمعلل نمآ رشن .10 ةوطخلا

.يلاتلا رزلا قوف رقنا ،بيولا ليغشتب حامسلا ددح

Secure Client VPN Conne	ction Setup Wizard X
Steps	Secure Client Deployment
1. Introduction	Secure Client program can be installed to a client device by one of the following two methods:
2. Connection Profile Identification	 Web launch - On accessing the ASA using a Web Browser, the Secure Client package will be automatically installed; Pre-deployment - Manually install the Secure Client package.
3. VPN Protocols	
4. Client Images	
5. Authentication Methods	Allow Web Launch
6. SAML Configuration	Caution: Web launch is global setting, it affects all connections. Secure Client SSL connections and clientless SSL connections will
7. Client Address Assignme	NUT WORK # K IS CARRES OFF.
8. Network Name Resolutio Servers	For pre-deployment, please remember to include the client profile 'disk0:/vpn-ipsec-tunnel-grp_client_profile.xml' from the ASA
9. NAT Exempt	in your Secure Client package, otherwise IPsec connection will NOT work.
10. Secure Client Deployment	
11. Summary	
	< gack Next > 用的 Help

تادادعإلا ظفح .11 ةوطخلا

دادعإ ةيلمعلا ظفحو رز زاجنإ تقطقط.

Secure Client VPN Conn	ection Setup Wizard		× 🖾 Warning ×
VPN Wizard	Summary Here is the summary of the configuration.		ASDM received messages below when one or more of the commands below were sent to the ASA. [OK] means success, [ERROR] means failure, [INFO] means information and [WARNING] means warning [OK] in local and wro-inser-pool 122 16.1 20:122 16.1 30 mask 255 255 255 0.
	Name Summary Name/Alas of the Connection Profile WPI Access Interface Device Digital Certificate VPI Protocole Enabled Secure Client Images Authentication Server Group SAML Address Pool for the Client DNS Network Address Translation	Value vpn-ipsec-tunnel-grp outside vpn-ipsec-tunzbrintunstructuredName=ciscoasa, CN Piece only 1 package radus-grp Server: Authentication Method: asa 172:16.1.30 Server: Domain Name: The method is an e subjected to network address translation	[Ch] Witke Glenk profile Table 11:11:11:11:11:11:11:11:11:11:11:11:11:

تادادعإلا ظفح

ەريدصتو نمآلا ليمعلا فيرعت فلم ديكأت .12 ةوطخلا

ادعب نع لوصولا) Network (Client) Access

 (دعب نع لوصولا) Network (Client) Access
 (قكبشلا ىلإ لوصولا) .

Eile View Iools Wigards Window Help	ve 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help			Type topic to search Go	cisco		
Device List Bookmarks	Configuration > Remote Access VPN > Network (Client) Acce	ess > Secure Client Profile					
Boolmarks <u>a</u> Q X X To boolmark a page, right-click on a node in the navigation bree and select "Add to boolmarks". G G Delete	This panel is used to manage Secure Clent Profiles and perform group assignment for Secure Clent version 2.5 or later. You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for apland and download of clent profiles between local machine and device. The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in Secure Clent version 3.0 and later.						
Remote Access VPN 🗗 🖗	🗣 Ada 🕑 Edit 🔀 Change Group Policy 🃋 Delete 🛃 Impor	t 🖏 Export 🔊 Valdate					
Introduction Introduction	Profile Name Ison-psec-tunnel-grp_clent_profile	Profile Usage AnyConnect VMV Profile	Group Policy GroupPolicy_vpn-ipsec-tunnel-grp	Profile Location disk0:/vpn-ipsec-tunnel-grp_stent_profile.xml			

نمآ ليمع فيرعت فلم ريرحت

فيرعتلا فلم ليصافت ديكأت.

- CiscoASA (IPsec) IPv4 : (بولطم) ضرعلا مسا
- P: 192.168.1.1 ناونع وأ IP: 192.168.1.1
- IPsec :يساسألا لوكوتوربلا•

Secure Client Profile Editor - v	Secure Client Profile Editor - spe-ipsec-tunnel-grp_client_profile					Server List Entry					×
Profile: vpn-ipsec-tunne	el-grp_client_pr	ofile				Server Load Balancing Servers SCEP Mobile Certificate Pinning					
Vite Preferences (Part 1) Preferences (Part 2) References (Part 2)	Server List	Server List						(SCORER (Proc.) Prof.	Connection Information Primary Protocol	к v)	
Confracte Priving Confracte Priving Confracte Privilinent El Huble Polary Server Dat	Hostname Sectors (Short) 2	Host Address	User Group	Backup Server List	SCIP Mobile Se		QDN or IP Address 192:368.1.1 Josep URL	Uter Group	Auth Method During BLE Identity (305 ga	DE Negotiation [EAP-AnyConnect 🗸
	moon is a regres		aac one jorver pe	annei n's prine.	Add]	Backup 5 Host J	kvæs	Cancel	Add Plave Up Plave Down Delete	

نمآلا ليمعلا فيرعت فلم ديكأت

.يلحملا رتويبمكلا ىل فيصوتلا ريدصتل ريدصت رز ىلع رقنا



نمآلا ليمعلا فيرعت فلم ريدصت

نمآلا ليمعلا فيرعت فلم ليصافت ديكأت .13 ةوطخلا

يساسألا لوكوتوربلا نأ نم دكأتو ،ضرعتسملا ةطساوب "نمآلا ليمعلا فيرعت فلم" حتفا وه فيضملل IPsec.

نمآلا ليمعلا فيرعت فلم ليصافت

ASA CLI يف تادادعإلا ديكأت .14 ةوطخلا

.ASA ل (CLI) رماوألا رطس ةهجاو يف ASDM ةطساوب اهؤاشنإ مت يتلا IPsec تادادعإ ديكأت

// Defines a pool of addresses ip local pool vpn-ipsec-pool 172.16.1.20-172.16.1.30 mask 255.255.255.0 // Defines radius server aaa-server radius-grp protocol radius aaa-server radius-grp (inside) host 1.x.x.191 timeout 5 // Define the transform sets that IKEv2 can use crypto ipsec ikev2 ipsec-proposal AES256 protocol esp encryption aes-256 protocol esp integrity sha-256 sha-1 crypto ipsec ikev2 ipsec-proposal AES192 protocol esp encryption aes-192 protocol esp integrity sha-256 sha-1 crypto ipsec ikev2 ipsec-proposal AES protocol esp encryption aes protocol esp integrity sha-256 sha-1 crypto ipsec ikev2 ipsec-proposal 3DES protocol esp encryption aes protocol esp integrity sha-256 sha-1 crypto ipsec ikev2 ipsec-proposal DES protocol esp encryption aes protocol esp integrity sha-256 sha-1 // Configures the crypto map to use the IKEv2 transform-sets crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP crypto map outside_map interface outside // Defines trustpoint crypto ca trustpoint vpn-ipsec-trustpoint enrollment self subject-name CN=ciscoasa keypair ipsec-kp crl configure // Defines self-signed certificate crypto ca certificate chain vpn-ipsec-trustpoint certificate 6651a2a2 308204ed 308202d5 a0030201 02020466 51a2a230 0d06092a 864886f7 0d01010b ac76f984 efd41d13 073d0be6 f923a9c6 7b quit // IKEv2 Policies crypto ikev2 policy 1 encryption aes-256 integrity sha256 group 5 prf sha256 lifetime seconds 86400 crypto ikev2 policy 10

encryption aes-192 integrity sha256 group 5 prf sha256 lifetime seconds 86400 crypto ikev2 policy 20 encryption aes integrity sha256 group 5 prf sha256 lifetime seconds 86400 crypto ikev2 policy 40 encryption aes integrity sha256 group 5 prf sha256 lifetime seconds 86400 // Enabling client-services on the outside interface crypto ikev2 enable outside client-services port 443 // Specifiies the certificate the ASA uses for IKEv2 crypto ikev2 remote-access trustpoint vpn-ipsec-trustpoint // Configures the ASA to allow Cisco Secure Client connections and the valid Cisco Secure Client images webvpn enable outside enable anyconnect image disk0:/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 anyconnect profiles vpn-ipsec-tunnel-grp_client_profile disk0:/vpn-ipsec-tunnel-grp_client_profile.xml anyconnect enable tunnel-group-list enable // Configures the group-policy to allow IKEv2 connections and defines which Cisco Secure Client profile group-policy GroupPolicy_vpn-ipsec-tunnel-grp internal group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes wins-server none dns-server value 1.x.x.57 vpn-tunnel-protocol ikev2 default-domain value ad.rem-system.com webvpn anyconnect profiles value vpn-ipsec-tunnel-grp_client_profile type user // Ties the pool of addressess to the vpn connection tunnel-group vpn-ipsec-tunnel-grp type remote-access tunnel-group vpn-ipsec-tunnel-grp general-attributes address-pool vpn-ipsec-pool authentication-server-group radius-grp default-group-policy GroupPolicy_vpn-ipsec-tunnel-grp tunnel-group vpn-ipsec-tunnel-grp webvpn-attributes group-alias vpn-ipsec-tunnel-grp enable

ريفشت ةيمزراوخ ةفاضإ .15 ةوطخلا

الجەن ىلإ 19 ةعومجملا فضأ ،ASA رماوأ رطس ةەجاو يف IKEv2.



تاعومجم معدت Cisco Secure Client دعت مل ،IKEv2/IPsec تالاصتال ةبسنلاب :ةظحالم رييغتلا اذه يدؤي دق .4.9.00086 رادصإلل اقفو 24 و 14 و 5 و 2 ماقرأ (DH) Diffie-Hellman (DH) ريفشتلا قيمزراوخ قباطت مدع ببسب لاصتالا يف لشف تالياح ثودح يلإ.

ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# group 19
ciscoasa(config-ikev2-policy)#

Windows مداخ يف نيوكتلا

لاصتال لمعتسم لاجم فيضي نأ جاتحت تنأ VPN. كاصتال لمعتسم لاجم فيضي نأ جاتحت تنأ Computers، لاجم مدختسمك vpnUser ةفاضإ.

Active Directory Users and Computers						
File Action View Help						
💠 🔶 🙍 📷 🥉 🛍 🗙 🖾 🧟 🙆 🔒 📓 📷 🕉 🔌 🛍 🔻 🛎	1 %					
Active Directory Users and Computers Saved Queres Saved Queres Saved Queres Saved Queres Saved Computers Domain Controllers Soft ForeignSecurityPrincipals Managed Service Accounts Users Users Domain Queres Saved Qu	tor DDC Passwor hers Domain Con ount DC Passwor i Proxy Imins Imputers introllers ters Admins Key Admins Read-only Du cy Creator O S Servers Domain Con I I I I I I I I I I I I I	roperties er Of DiaH e control Re Address Acco vpn user e: vpn e: user user ame: vpn us on:	n Environme mate Desktop Services unt Profile Tek	? ent Set forbie Grg nitale: Qther Other	X soons COM+ anization	t for administering the computer/domain s group can have their passwords replicated to s group that are domain controllers may be cl managed by the system. s group cannot have their passwords replicate tors Group o are permitted to perform dynamic updates o ninistrators of the domain trollers in the domain trollers in the domain sts s group can perform administrative actions on s group can perform administrative actions on s group are Read-Only Domain Controllers in t s group can modify group policy for the domain t for guest access to the computer/domain s group can perform administrative actions on s group can get for additional protections ag roup can access remote access properties of u s group are Read-Only Domain Controllers in t in s group are Read-Only Domain Controllers in t ninistrators of the schema

```
لاجم مدختسم ةفاضإ
```

لاجملا يمدختسمو لاجملا يلوؤسم وضع ىلإ لاجملا مدختسم ةفاضإ.

				?	×	vpn user Pr	roperties				?	>
Remote control	Remote [Desktop Servic	ces Profile	CO	M+	Remote control Remote Desktop Services Profile		CO	M+			
Member Of	Dial-in	Environ	ment	Sessio	ns	General	Address	Account	Profile	Telephones	Organia	zatio
General Address	Account	Profile 1	Telephones	Organi	zation	Memb	er Of	Dial-in	Env	vironment	Sessio	ns
User logon name:						Member	of:					
vpnuser		@ad.rem-s	ystem.com		\sim	Name		Active Direct	tory Domain	n Services Folder	r	
User logon name (pre-	Windows 200	0):				Domain	Admins	ad.rem-syste	m.com/Use	ers		
AD\	AD\ vpnuser					Domain	Users	ad.rem-syster	m.com/Use	ers		
User must chang User cannot cha Password never Store password	ge password a ange password expires using reversibl	t next logon d le encryption			^	A <u>d</u> d Primary g	I	Remove omain Users	to condite	ebaaa Dier		
User must chang User cannot cha Password never Store password Account expires Never End of:	ge password a ange password expires using reversibl Monday	t next logon d le encryption June 10,	2024		•	Add Primary g Set Pr	I	Remove omain Users There is r you have applicatio	no need to Macintosh ns.	change Primary n clients or POSI)	group unle K-complian	ess nt

لاجملا ومدختسمو لاجملا ولوؤسم

ISE يف نيوكتلا

زاهج ةفاضإ .1 ةوطخلا

ASAv. زاهج ةفاضإل AddButton قوف رقنا ،ةكبشلا ةزهجأ < Administration ىلإ لقتنا

Network Devices	Network Device Groups	Network Device Profiles	External RADIUS	Servers RAD	IUS Server Sequences
Network Devices Default Device Device Security Settings	Network Devices Network Devices Name Description	ASAv			
	IP Addres	× ⁺ ™: 1.075,06	1 / 32 🚳		
	Device Profi	le 📫 Cisco	¥ (i)		
	Model Name		~		
	Software Ve	rsion	~		
	Network Dev	vice Group			
	Location	All Locations	~	Set To Default	
	IPSEC	No	~	Set To Default	
	Device Type	All Device Types	~	Set To Default	
		ADIUS Authentication	Settings		
	Prot	ocol RADIUS			
	Sha	red Secret cisco123		Hide	

زاهج ةفاضإ

Active Directory ةفاضإ .2 ةوطخلا

ىل لقتنا Administration < تي ما رداصم Administration > توف رقنا، ConnectTab المي القتنا مقاض المقو مقوا مقود ما مقود ما ما

- اطبرلا ةطقن مسا AD_JOIN_POINT
- الجم Active Directory: ad.rem-system.com



Active Directory ۃﻑﺍﺹﺍ

ةمئاقلا نمDirectory ةلدسنملا ةمئاقلا نم تاعومجم ددح ،تاعومجم بيوبتلا ةمالع ىلإ لقتنا ةلدسنملا.

≡	dentity Services	Engine Administration / Identity Management
Л	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
	Dashboard	
명	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
*	Operations	< 28
.0	Policy	Select Groups From Directory Select Groups From Directory Select Groups From Directory
20	Administration	Add Group Control Assist ad.rem-system.com/S-1-5-32-579

```
ليلدلا نم تاعومجم ددح
```

قلدسنملا قمئاقلا نم تاعومجملا دادرتسا قوف رقنا. Checkad.rem-system.com/Users/Domain Computersandad.rem-system.com/Users/Domain UserAnd clickOK.

=		Engine					×	🛦 tratas
	Restaurate	Identities Groups F	Sel	ect Directory Groups				
	Dookmarks		This di	alog is used to select groups from the Direct	ory.			
24	Dashboard	Active Directo	Do	main ad.rem-system.com				
16	Context Visibility	AD_Join_Poin	N	lame SID . Filter Filter	Type ALL Filter			
×	Operations	C LDAP		Retrieve Groups 9 Groups Retrieved	d.			
0	Policy	RADIUS Token						
20	Administration	C RSA SecuriD	0	Name ^	Group SID	Group Type		
-11	Work Centers	SAML Id Provide	-	ad rem-system.com/Users/Deal IndateProv	5-1-5-21-4193742415-4133520026-20462399.	CLOBAL	1	
_		C Social Login	-	ad rem-system.com/Users/Domain Admins	5-1-5-21-4193742415-4133520026-20462399	GLOBAL		
۲	Interactive Help			ad.rem-system.com/Users/Domain Computers	5-1-5-21-4193742415-4133520026-20462399.	GLOBAL		
			0	ad.rem+system.com/Users/Domain Controllers	5+1+5+21+4193742415+4133520026+20462399	GLOBAL		
			0	ad.rem-system.com/Users/Domain Guests	8-1-5-21-4190742415-4130520026-20462099	GLOBAL		
			•	ad.rem-system.com/Users/Domain Users	5-1-5-21-4193742415-4133520026-20462399	GLOBAL		
			0	ad.rem-system.com/Users/Enterprise Admins	5+1+5+21+4193742415+4133520026+20462399	UNIVERSAL	1	
				ad.rem-system.com/Users/Enterprise Key Admins	5-1-5-21-4193742415-4133520026-20462399.	UNIVERSAL		
				ad.rem-system.com/Users/Enterprise Read-only	5+1+5+21+4193742415+4133520026+20462399	UNIVERSAL		
				ad.rem-system.com/Users/Group Policy Creator .	. S+1+5+21+4193742415+4133520026+20462399.	GLOBAL		
			4					
						Cancel	ок	

نيمدختسملاو لاجملا رتويبمك ةزهجأ ةفاضإ

ةيوەلا ردصم ةلسلس ةفاضإ .3 ةوطخلا

ةيوه ردصم لسلست ةفاضإب مقو ،ةيوهلا ردصم تالسلست < ةرادإ ىلإ لقتنا.

- امسالا: Identity_AD
- المئاق AD_JOIN_POINT :ققداصملا نع ثحبالا قمئاق

≡	dials Identity Services E	Engine		Administration / Id	lentity Management
н	Bookmarks	Identities Groups	External Identity Sources	Identity Source Sequences	Settings
51	Dashboard	Martin Science Services	es Lie > Identity AD		
명	Context Visibility	Identity Source S	Sequence		
*	Operations				
U	Policy	✓ Identity Source	ce Sequence		
80	Administration	- Name	Identity_AD		
di.	Work Centers	Description			
(?)	Interactive Help	✓ Certificate B ☐ Select Centre	ased Authentication	~	
		✓ Authentication A set of identication	on Search List ntity sources that will be accessed	in sequence until first authentication s	ucceeds
		Available	0	Selected	
		Internal	Endpoints ^	AD_Join_Point ^	
		Internal	Users		
		All_AD_	Join_Points	E	
			>>>	E	
اض	صم تالسلست ةف	ةيوەلا رد			

جەن ةعومجم ةفاضإ .4 ةوطخلا

جەن ةعومجم ةفاضإل + قوف رقنا ،جەن تاعومجم < جەن ىلإ لقتنا.

- جەنلا ةعومجم مسا: VPN_TEST
- ةزهجألاا عاوناً عيمج يواسي زاهجلا عون :طورشلا
- ة فكبشلا يلاء عن الما المعالية عنه الما المالي المالي المالي المالي المالي المالي المالية المالية الم

$\equiv \frac{\mathrm{dtable}}{\mathrm{cisco}}$ Identity Services	Engine	Policy / Policy Sets	🔺 Evaluation Mode = Days Q 💩 💿 📮 Q
Bookmarks	Policy Sets		Reset Reset Policyset Hitcounts Save
Dashboard	+ Status Policy Set Name	Description Conditions	Allowed Protocols / Server Sequence Hits Actions View
I Context Visibility	Q Search		
× Operations	VPN Test	DEVICE Device Type EQUALS	All Default Network Access
Policy		Device Types	
جەن ةعومجم ةفاضإ			

ةقداصملا جەن ةفاضاٍ .5 ةوطخلا

.ةقداصم جەن ةفاضإل VPN_TEST قوف رقنا ،جەنلا تاعومجم ىلإ لقتنا

- اةدعاقلا مسا: VPN_AUTHENTICATION
- 1.x.x.61 يواسي ةكبشلا ىلإ لوصولا زامجل IP ناونع :طورشلا
- Identity_AD :مادختسالا

∨Auth	entication	Policy(2)				
÷	Status	Rule Name	Conditions	Use	Hits	Actions
C	Search					
				Identity_AD		
	۲	VPN_Authentication	Network Access-Device IP Address EQUALS 1.171.1.61	> Options	10	ŝ

ةقداصملا جەن ةڧاضإ

ليوختلا جەن ةفاضإ .6 ةوطخلا

ليوخت جەن ةفاضإل VPN_TEST قوف رقناو ،جەنلا تاعومجم ىلإ لقتنا.

- تدعاقلا مسا: VPN_AUTHORIZATION
- Network_ACCESS_AUTHENTICATION_PASS
- جئاتنلا: PermitAccess

∨Authorization Policy(2)					
		Results			
(+) Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Q Search					
VPN_Authorization	Network_Access_Authentication_Passed	PermitAccess		10	Ś

ليوختلا جهن ةفاضإ

ةحصلا نم ققحتلا

Win10 PC1 ىلإ نمآلا ليمعلا فيرعت فلم خسنا .1 ةوطخلا

ليلد ىلإ نمآلا ليمعلا فيرعت فلم خسنا C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile.



رتويبمكلا ىلإ فيرعتلا فلم خسن

VPN لاصتا ءدب .2 ةوطخلا

مث ،رورملا ةملكو مدختسملا مسا لخدأو Cisco Secure Client ليغشتب مق ،ةياەنلا ةطقن ىلع لاصتا ديكأتب مق Cisco Secure Client لاصتا ديكأتب مق.



لاصتالا حجن

ASA ىلع Syslog ديكأت .3 ةوطخلا

.IKEv2 لاصتا حاجن نم دكأت ،syslog يف

<#root>

May 28 20xx 08:xx:20: %ASA-5-750006: Local:192.168.1.1:4500 Remote:192.168.1.11:50982 Username:vpnuser New Connection Established

May 28 20xx 08:xx:20: %ASA-6-751026: Local:192.168.1.1:4500 Remote:192.168.1.11:50982 Username:vpnuser

ASA ىلع IPsec لمع ةسلج ديكأت .4 ةوطخلا

.ASA ىلع IKEv2/IPsec لمع ةسلج ديكأتل رمألا show vpn-sessiondb detail anyconnect ليغ شتب مق

<#root>

ciscoasa#

show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : vpnuser Index : 23 Assigned IP : 172.16.1.20 Public IP : 192.168.1.11 Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent License : AnyConnect Premium Encryption : IKEv2: (1)AES256 IPsecOverNatT: (1)AES256 AnyConnect-Parent: (1)none Hashing : IKEv2: (1)SHA256 IPsecOverNatT: (1)SHA256 AnyConnect-Parent: (1)none Bytes Tx : 840 Bytes Rx : 52408 Pkts Tx : 21 Pkts Rx : 307 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : GroupPolicy_vpn-ipsec-tunnel-grp Tunnel Group : vpn-ipsec-tunnel-grp Login Time : 08:13:20 UTC Tue May 28 2024 Duration : 0h:10m:10s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 01aa003d0001700066559220 Security Grp : none IKEv2 Tunnels: 1 IPsecOverNatT Tunnels: 1 AnyConnect-Parent Tunnels: 1 AnyConnect-Parent: Tunnel ID : 23.1 Public IP : 192.168.1.11 Encryption : none Hashing : none Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 19 Minutes Client OS : win Client OS Ver: 10.0.15063 Client Type : AnyConnect Client Ver : 5.1.3.62 IKEv2: Tunnel ID : 23.2 UDP Src Port : 50982 UDP Dst Port : 4500 Rem Auth Mode: userPassword Loc Auth Mode: rsaCertificate Encryption : AES256 Hashing : SHA256 Rekey Int (T): 86400 Seconds Rekey Left(T): 85790 Seconds PRF : SHA256 D/H Group : 19 Filter Name : Client OS : Windows Client Type : AnyConnect IPsecOverNatT: Tunnel ID : 23.3 Local Addr : 0.0.0.0/0.0.0.0/0/0 Remote Addr : 172.16.1.20/255.255.255.255/0/0 Encryption : AES256 Hashing : SHA256 Encapsulation: Tunnel Rekey Int (T): 28800 Seconds Rekey Left(T): 28190 Seconds Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Bytes Tx : 840 Bytes Rx : 52408 Pkts Tx : 21 Pkts Rx : 307

Radius Live لجس ديكأت .5 ةوطخلا

. VPN ةقداصمل ليغشتلا لجس دكأ ،LogISE ةرشابملا (GUI) ةيموسرلا مدختسملا ةهجاو < **RADIUS < ت***ايلمعل*ا يل إلقتنا

=	dealer Identity Services	Engine						Operations / RADIL	JS			4.6	valuation Mode 🥅 Days	۵ ۵	•	0 Я
J.	Bookmarks	Live Logs Live Sessions														
	Dashboard															
R	Context Visibility	Misconfigured Supplicants		Misconfigured Network Devices 💿				RADIUS Drops		Client Stopped Responding 📀				Repeat Co	ounter 🕓	
*	Operations	0		0			0		0			0				
U	Policy											Defeeth	Show		Victor	
2	Administration											Never	V Latest 20 re	cords 🗸	Last 3 hou	irs v
6	Work Centers	😂 👘 Reset Repeat Counts	🕁 Export To	×											Filter 🖂	۰
		Time	Status	Details	Repeat	Endpoint	Identity	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization P	IP Address	Network De	Device Por	t Iden	tity Grou
0	Interactive Help	×	~			Endpoint ID	Identity	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profi	IP Address	V Network Devic	Device Port	Iden	sity Group
		May 28, 2024 05:13:42	•	0	0	00.50.5	vpruser	Windows10-Workstation	${\rm VPN}_{\rm o}{\rm Test} \gg {\rm VPN}_{\rm o}{\rm Authentication}$	${\rm VPN}_{\rm o}{\rm Test} \mapsto {\rm VPN}_{\rm o}{\rm Authorization}$	PermitAccess					
		May 28, 2024 05:13:42		ò		00:50:5	vpnuser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess		ASAu		Work	station

Radius Live لجس

.رشابملا ليغشتلا لجس ليصافت ديكأتل "ةلاح" قوف رقنا

	Cisco ISE				
6			1		
	Overview		Steps		
	Event	5200 Authentication succeeded	Step ID	Description	Latency (ms)
	Lycin	S200 Automication succeeded	11001	Received RADIUS Access-Request	
	Username	vpnuser	11017	RADIUS created a new session	1
	Endpoint Id	00:50:56:98:77:A4 ⊕	15049	Evaluating Policy Group	36
	Endpoint Profile	Windows10-Workstation	15008	Evaluating Service Selection Policy	1
			15048	Queried PIP - DEVICE.Device Type	6
	Authentication Policy	VPN_Test >> VPN_Authentication	15041	Evaluating Identity Policy	20
	Authorization Policy	VPN_Test >> VPN_Authorization	15048	Queried PIP - Network Access.Device IP Address	2
	Authorization Result	PermitAccess	22072	Selected identity source sequence - Identity_AD	6
			15013	Selected Identity Source - AD_Join_Point	1
			24430	Authenticating user against Active Directory - AD_Join_Point	4
	Authentication Details		24325	Resolving identity - vpnuser	38
	Source Timestamp	2024-05-28 17:13:42.897	24313	Search for matching accounts at join point - ad.rem- system.com	0
	Received Timestamp	2024-05-28 17:13:42.897	24319	Single matching account found in forest - ad.rem- system.com	0
	Policy Server	ise33-01	24323	Identity resolution detected single matching account	0
	Event	5200 Authentication succeeded	24343	RPC Logon request succeeded - vpnuser@ad.rem- system.com	23
	Username	vpnuser	24402	User authentication against Active Directory succeeded - AD_Join_Point	3
	Endpoint Id	00:50:56:98:77:A4	22037	Authentication Passed	1
	Calling Station Id	192.168.1.11	24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory	1
	Endpoint Profile	Windows10-Workstation	15036	Evaluating Authorization Policy	1
	Authentication Identity	AD_Join_Point	24209	Looking up Endpoint in Internal Endpoints IDStore - vpnuser	0
	Store		24211	Found Endpoint in Internal Endpoints IDStore	9
	Identity Group	Workstation	15048	Queried PIP - Network Access.AuthenticationStatus	2
	Audit Session Id	01aa003d0001700066559220	15016	Selected Authorization Profile - PermitAccess	7
	Authentication Method	PAP ASCIL	22081	Max sessions policy passed	6
	Potentiliteduori metriod		22080	New accounting session created in Session cache	0
	Authentication Protocol	PAP_ASCII	11002	Returned RADIUS Access-Accept	2
	Network Device	ASAv			

رشابملا لجسلا ليصافت

اهحالصإو ءاطخألا فاشكتسا

قباطت مدع ةلكشم ثدحت ىتم ىلع لاثم اذه .لاصتالا يف لشف تالاح ثودح ىلإ ريفشتلا تايمزراوخ قباطت مدع يدؤي دق قراطت مدع قلكشم ثدحت ىتم 15 قوطخلا ذيفنت .تايمزراوخلا ASDM يف مسقلا نيوكت نم 15 قوطخلا ذيفنت .تايمزراوخلا.

VPN لاصتا ءدب .1 ةوطخلا

. ريفشتلا تايمزراوخ قباطت مدع ببسب لاصتالا لشف نم دكأتو Cisco Secure Client ليغشتب مق ،ةياهنلا ةطقن ىلع

The cryptographic algorithms required by the secure gateway do not match those supported by AnyConnect.Please contact your network administrator.

S Cisco Secure Client		-		×	Cisco Secure Client		
AnyConnect VPN: Ready to connect. discoasa (IPsec) IPv4	~ Q		Connect		The cryptographic algorithms required by the secure gateway do not match those supported by Cisco Secure Client. Please contact your network administrator.		
					OK		

لاصتالا لشف

CLI يف Syslog ديكأت .2 ةوطخلا

يف syslog، تاضوافم لشف نم دكأت IKEv2.

<#root>

May 28 20xx 08:xx:29: %ASA-5-750002: Local:192.168.1.1:500 Remote:192.168.1.11:57711 Username:Unknown IKEv2 Received a IKE_INIT_SA requ May 28 20xx 08:xx:29: %ASA-4-750003: Local:192.168.1.1:500 Remote:192.168.1.11:57711 Username:Unknown IKEv2 Negotiation aborted due to ERI

Failed to find a matching policy

عجرملا

قدامشلا مقدام مادختس اب ASA مادختس اب IKEv2 ما المعام المعام المعام المعام المعام المعام المعام المعام المعام ا

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما