

VPN ليمع ب لاصت ال VPN 3000 زكرم نيوكت تاداهش ل ا مادخت ساب

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[شهادات مركز VPN 3000 لعملاء VPN](#)

[التحقق من الصحة](#)

[استكشاف الأخطاء وإصلاحها](#)

[معلومات ذات صلة](#)

[المقدمة](#)

يتضمن هذا المستند إرشادات خطوة بخطوة حول كيفية تكوين مركبات Cisco VPN 3000 Series مع عملاء VPN باستخدام الشهادات.

[المتطلبات الأساسية](#)

[المتطلبات](#)

لا توجد متطلبات خاصة لهذا المستند.

[المكونات المستخدمة](#)

تستند المعلومات الواردة في هذا المستند إلى برنامج Cisco VPN 3000 Concentrator نسخة 4.0.4a.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

[الاصطلاحات](#)

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

[شهادات مركز VPN 3000 لعملاء VPN](#)

أتمت هذا steps in order to شكلت VPN 3000 مركز شهادة ل VPN زبون.

1. يجب تكوين سياسة IKE لاستخدام الشهادات الموجودة على "مدير سلسلة مركز VPN 3000". لتكوين سياسة IKE، حدد التكوين < النظام > بروتوكولات الاتصال النفقي < IPsec > مقترحات IKE، ونقل CiscoVPNClient-3DES-MD5-RSA إلى الاقتراحات النشطة.

Configuration | System | Tunneling Protocols | IPsec | IKE Proposals Save Needed

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate. Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority. Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by [Security Associations](#) to specify IKE parameters.

Active Proposals	Actions	Inactive Proposals
CiscoVPNClient-3DES-MD5-RSA	<< Activate	IKE-3DES-SHA-DSA
CiscoVPNClient-3DES-MD5	Deactivate >>	IKE-3DES-MD5-RSA-DH1
IKE-3DES-MD5	Move Up	IKE-DES-MD5-DH7
IKE-3DES-MD5-DH1	Move Down	CiscoVPNClient-3DES-SHA-DSA
IKE-DES-MD5	Add	CiscoVPNClient-3DES-MD5-RSA-DH5
IKE-3DES-MD5-DH7	Modify	CiscoVPNClient-3DES-SHA-DSA-DH5
IKE-3DES-MD5-RSA	Copy	CiscoVPNClient-AES256-SHA
CiscoVPNClient-3DES-MD5-DH5	Delete	IKE-AES256-SHA
CiscoVPNClient-AES128-SHA		
IKE-AES128-SHA		

2. يجب أيضا تكوين نهج IPsec لاستخدام الشهادات. حدد تكوين < إدارة السياسة > إدارة حركة مرور البيانات < اقترانات الأمان، أبرز ESP-3DES-MD5 ثم انقر فوق تعديل لتكوين سياسة IPsec لتكوين سياسة IPsec.

Configuration | Policy Management | Traffic Management | Security Associations Save Needed

This section lets you add, configure, modify, and delete IPsec Security Associations (SAs). Security Associations use [IKE Proposals](#) to negotiate IKE parameters.

Click **Add** to add an SA, or select an SA and click **Modify** or **Delete**.

IPsec SAs	Actions
ESP-3DES-MD5	Add
ESP-3DES-MD5-DH5	Modify
ESP-3DES-MD5-DH7	Delete
ESP-3DES-NONE	
ESP-AES128-SHA	
ESP-DES-MD5	
ESP-L2TP-TRANSPORT	
ESP/IKE-3DES-MD5	

3. في نافذة "تعديل"، تحت "الشهادات الرقمية"، تأكد من تحديد شهادة هويتك المثبتة. تحت اقتراح IKE، حدد CiscoVPNClient-3DES-MD5-RSA وانقر فوق تطبيق.

Configuration | Policy Management | Traffic Management | Security Associations | Modify

Modify a configured Security Association.

SA Name Specify the name of this Security Association (SA).

Inheritance Select the granularity of this SA.

IPSec Parameters

Authentication Algorithm Select the packet authentication algorithm to use.

Encryption Algorithm Select the ESP encryption algorithm to use.

Encapsulation Mode Select the Encapsulation Mode for this SA.

Perfect Forward Secrecy Select the use of Perfect Forward Secrecy.

Lifetime Measurement Select the lifetime measurement of the IPSec keys.

Data Lifetime Specify the data lifetime in kilobytes (KB).

Time Lifetime Specify the time lifetime in seconds.

IKE Parameters

IKE Peer Specify the IKE Peer for a LAN-to-LAN IPSec connection.

Negotiation Mode Select the IKE Negotiation mode to use.

Digital Certificate Select the Digital Certificate to use.

Certificate Transmission Entire certificate chain
 Identity certificate only Choose how to send the digital certificate to the IKE peer.

IKE Proposal Select the IKE Proposal to use as IKE initiator.

4. من أجل تكوين مجموعة IPsec، حدد تكوين < إدارة المستخدم > مجموعات < إضافة >، وقم بإضافة مجموعة تسمى IPSECCERT (يتطابق اسم مجموعة IPSECCERT مع الوحدة التنظيمية (OU) في شهادة الهوية)، وحدد كلمة مرور. لا تستخدم كلمة المرور هذه في أي مكان إذا كنت تستخدم شهادات. في هذا مثال، "cisco123" هي كلمة المرور.

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

Identity Parameters

Attribute	Value	Description
Group Name	<input type="text" value="IPSECCERT"/>	Enter a unique name for the group.
Password	<input type="password" value=""/>	Enter the password for the group.
Verify	<input type="password" value=""/>	Verify the group's password.
Type	<input type="text" value="Internal"/>	<i>External groups</i> are configured on an external authentication server (e.g. RADIUS). <i>Internal groups</i> are configured on the VPN 3000 Concentrator's Internal Database.

5. في نفس الصفحة، انقر فوق علامة التبويب "عام" وتأكد من تحديد IPsec كبروتوكول الاتصال النفقي.

Identity General IPsec Client Config Client FW HW Client PPTP/L2TP			
General Parameters			
Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this group.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this group.
Filter	-None-	<input checked="" type="checkbox"/>	Enter the filter assigned to this group.
Primary DNS		<input checked="" type="checkbox"/>	Enter the IP address of the primary DNS server.
Secondary DNS		<input checked="" type="checkbox"/>	Enter the IP address of the secondary DNS server.
Primary WINS		<input checked="" type="checkbox"/>	Enter the IP address of the primary WINS server.
Secondary WINS		<input checked="" type="checkbox"/>	Enter the IP address of the secondary WINS server.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select the SEP cards this group can be assigned to.
Tunneling Protocols	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	<input type="checkbox"/>	Select the tunneling protocols this group can connect with.

6. انقر فوق علامة التبويب IPsec وتأكد من تحديد اقتران أمان (SA) IPsec الذي تم تكوينه ضمن IPsec وانقر فوق تطبيق.

Identity				General				IPSec				Client Config				Client FW				IHW Client				PPTP/L2TP			
IPSec Parameters																											
Attribute		Value				Inherit?		Description																			
IPSec SA		ESP-3DES-MD5				<input checked="" type="checkbox"/>		Select the group's IPSec Security Association.																			
IKE Peer Identity Validation		If supported by certificate				<input checked="" type="checkbox"/>		Select whether or not to validate the identity of the peer using the peer's certificate.																			
IKE Keepalives		<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>		Check to enable the use of IKE keepalives for members of this group.																			
Confidence Interval		300				<input checked="" type="checkbox"/>		(seconds) Enter how long a peer is permitted to idle before the VPN Concentrator checks to see if it is still connected.																			
Tunnel Type		Remote Access				<input checked="" type="checkbox"/>		Select the type of tunnel for this group. Update the Remote Access parameters below as needed.																			
Remote Access Parameters																											
Group Lock		<input type="checkbox"/>				<input checked="" type="checkbox"/>		Lock users into this group.																			
Authentication		Internal				<input type="checkbox"/>		Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication .																			
Authorization Type		None				<input checked="" type="checkbox"/>		If members of this group need authorization in addition to authentication, select an authorization method. If you configure this field, you must also configure an Authorization Server.																			
Authorization Required		<input type="checkbox"/>				<input checked="" type="checkbox"/>		Check to require successful authorization.																			
DN Field		CN otherwise OU				<input checked="" type="checkbox"/>		For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.																			
Authorization Required		<input type="checkbox"/>				<input checked="" type="checkbox"/>		Check to require successful authorization.																			
DN Field		CN otherwise OU				<input checked="" type="checkbox"/>		For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.																			
IPComp		None				<input checked="" type="checkbox"/>		Select the method of IP Compression for members of this group.																			
Reauthentication on Rekey		<input type="checkbox"/>				<input checked="" type="checkbox"/>		Check to reauthenticate the user on an IKE (Phase-1) rekey.																			
Mode Configuration		<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>		Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the Aliga/Cisco client is being used by members of this group.																			
Add				Cancel																							

7. in order to IPsec شملت مجموعة على ال VPN 3000 مركز، حددت تشكيل <مستعمل إدارة> <مستعمل> يضيف، يعين مستعمل إسم، كلمة، والمجموعة إسم، وبعد ذلك قطعة يضيف. في المثال، يتم استخدام هذه الحقول: إسم المستخدم = cert_user = كلمة المرور = Cisco123 التحقق من الصحة = Cisco123 المجموعة = IPSECCERT

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity | General | IPsec | PPTP/L2TP

Identity Parameters		
Attribute	Value	Description
Username	cert_user	Enter a unique username.
Password	*****	Enter the user's password. The password must satisfy the group password requirements.
Verify	*****	Verify the user's password.
Group	IPSECCERT	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Add Cancel

8. لتمكين تصحيح الأخطاء على VPN 3000 Concentrator تحديد تشكيل <نظام> أحداث <فئات> وأضفت هذه الفئات: فريق التحقيق 1-13 آيك 1-10-1 IKEDBG 6بروتوكول 1-6IPSECDBG 1-6IPSec

10

Configuration | System | Events | Classes

This section lets you configure special handling of specific event classes.

Click the **Add** button to add an event class, or select an event class and click **Modify** or **Delete**.

[Click here to configure general event parameters.](#)

Configured Event Classes	Actions
CERT	Add Modify Delete
IKE	
IKEDBG	
IPSEC	
IPSECDBG	
MIB2TRAP	

9. حدد مراقبة < سجل أحداث قابل للتصفية لعرض تصحيح الأخطاء.

Monitoring | Filterable Event Log

Select Filter Options

Event Class: All Classes (dropdown menu with options: AUTH, AUTHDBG, AUTHDECODE)

Severities: ALL (dropdown menu with options: 1, 2, 3)

Client IP Address: 0.0.0.0

Events/Page: 100

Group: -All-

Direction: Oldest to Newest

Buttons: <<<, <<, >>, >>>, Get Log, Save Log, Clear Log

Buttons: <<<, <<, >>, >>>

ملاحظة: إذا قررت تغيير عناوين IP، فيمكنك إجراء تسجيل لعناوين IP الجديدة وثبيت الشهادة التي تم إصدارها لاحقاً باستخدام هذه العناوين الجديدة.

[التحقق من الصحة](#)

لا يوجد حالياً إجراء للتحقق من صحة هذا التكوين.

[استكشاف الأخطاء وإصلاحها](#)

راجع [استكشاف أخطاء الاتصال وإصلاحها على مركز VPN 3000](#) للحصول على مزيد من المعلومات حول استكشاف الأخطاء وإصلاحها.

[معلومات ذات صلة](#)

- [مركزات Cisco VPN 3000 Series](#)
- [أجهزة Cisco VPN 3002 العملية](#)
- [مفاوضة IPsec/بروتوكولات IKE](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إلمءءاد ءوچرلاب ةصوء و تاملرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءنل دن تسمل