ASA 8.x/ASDM 6.x: ريظن تامولعم ةفاضإ ىلإ عقوم نم ةدوجوم VPN ةكبش يف ةديدج مادختساب عقوم

المحتويات

<u>المتطلبات الأساسية</u> <u>المتطلبات الأساسية</u> <u>المكونات المستخدمة</u> <u>الاصطلاحات</u> <u>معلومات خلفية</u> <u>معلومات خلفية</u> <u>تحرير تكوين NPN الموجود</u> <u>التحقق من الصحة</u> <u>استكشاف الأخطاء وإصلاحها</u> <u>تعذر على بادئ IKE العثور على النهج: INTF test_ext, SRC: 172.16.1.103, DST: 10.1.4.251 معلومات ذات صلة</u>

<u>المقدمة</u>

يقدم هذا المستند معلومات حول تغييرات التكوين التي يتم إجراؤها عند إضافة نظير شبكة VPN جديد إلى تكوين شبكة VPN الموجود من موقع إلى موقع باستخدام مدير أجهزة الأمان القابل للتكيف (ASDM). وهذا مطلوب في هذه السيناريوهات:

- تم تغيير موفر خدمة الإنترنت (ISP) ويتم إستخدام مجموعة جديدة من نطاق IP العام.
 - إعادة تصميم كاملة للشبكة في موقع ما.

• يتم ترحيل الجهاز المستخدم كبوابة VPN في موقع ما إلى جهاز جديد باستخدام عنوان IP عام مختلف. يفترض هذا المستند أن شبكة VPN من الموقع إلى الموقع تم تكوينها بالفعل بشكل صحيح وتعمل بشكل صحيح. يزود هذا وثيقة ال steps أن يتبع in order to غيرت VPN نظير معلومة في ال L2L VPN تشكيل.

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

cisco يوصي أن يتلقى أنت معرفة من هذا موضوع:

• <u>مثال تكوين VPN من موقع ASA إلى موقع</u>

<u>المكونات المستخدمة</u>

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- سلسلة أجهزة الأمان المعدلة Cisco 5500 مع إصدار البرنامج 8.2 والإصدارات الأحدث
- مدير أجهزة حلول الأمان المعدلة من Cisco مع الإصدار 6.3 من البرنامج والإصدارات الأحدث

<u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

معلومات خلفية

تعمل الشبكة الخاصة الظاهرية (VPN) من موقع إلى موقع بشكل جيد بين الحقاصة والبقاصة. بافتراض أن BKASA لديه إعادة تصميم شبكة كاملة وتم تعديل مخطط IP على مستوى ISP، ولكن تبقى جميع تفاصيل الشبكة الفرعية الداخلية كما هي.

يستخدم نموذج التكوين هذا عناوين IP التالية:

- BKASA موجود خارج عنوان 1P 200.200.200.200
 - BKASA جديد خارج عنوان IP 209.165.201.2

ملاحظة: هنا، سيتم تعديل معلومات النظير فقط. نظرا لعدم وجود تغيير آخر في الشبكة الفرعية الداخلية، تظل قوائم الوصول الخاصة بالشفرة كما هي.

<u>تكوين ASDM</u>

يوفر هذا القسم معلومات حول الطرق المحتملة المستخدمة لتغيير معلومات نظير VPN على HKASA باستخدام ASDM.

إنشاء ملف تعريف اتصال جديد

يمكن أن يكون هذا هو الطريقة الأسهل لأنه لا يزعج تكوين VPN الموجود ويمكن أن يخلق ملف تعريف اتصال جديد باستخدام المعلومات الجديدة ذات الصلة بنظير VPN.

1. انتقل إلى *التكوين > VPN من موقع إلى موقع > ملفات تعريف الاتصال* وانقر فوق *إضافة* ضمن منطقة ملفات تعريف

nable interfaces for IPs	ec access.				
Interface	Allow Acce	ss -			
utside		V			
dma					
nside					
naction Dealling					
nection Profiles				and the second second second	. 54 m.
mection Profiles onnection profile identi	ies the peer of a site-to-sit	e connection. It specifies what data traffic	is to be encrypted, how the data traffic	is to be encrypted, and other para	aneters.
nnection Profiles Connection profile identi	ies the peer of a site-to-site	e connection. It specifies what data traffic	is to be encrypted, how the data traffic	is to be encrypted, and other para	ameters.
nnection Profiles Connection profile identi Add	ies the peer of a site-to-site viote	e connection. It specifies what data traffic	s to be encrypted, how the data traffic	is to be encrypted, and other para	ameters.
nnection Profiles Connection profile identi Add 2 Edit 1 C Name	les the peer of a site-to-site ploto	e connection. It specifies what data traffic Local Network	s to be encrypted, how the data traffic Remote Network	is to be encrypted, and other para	ameters. Group Policy

يظهر إطار *إضافة ملف تعريف اتصال من موقع إلى موقع IPSec*.

2. تحتّ عُلامةُ التبويب "أساسي"، قم بتوفيرٌ تفاصيلُ *عنوانٌ IP للنظير والمفتاح المشترك مسبقا والشبكات المحمية.* استعملت كل ال نفسه معلم بما أن ال VPN موجود، ماعدا النظير معلومة. وانقر فوق

nced	Peer IP Address: 🗹 Static	209.165.201.2	
	Connection Name: 🔽 Same as IP Address	209.165.201.2	
	Interface: outside	×	
	JKE Authentication		
	Pre-shared Key:		
	Identity Certificate: None	×	Manage
	Protected Networks		
	Local Network: inside-network/24		
	Remote Network: 192.168.25.0/24	-	
	Encryption Algorithms		
	IKE Proposal: pre-share-des-sha, p	re-share-3des-sha	Manage.
	IPsec Proposal: S-256-MDS, ESP-3DE	S-SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5	Select

3. تحت قائمة متقدمة، انقر فوق *إدخال خريطة التشفير*. ارجع إلى علامة التبويب *الأولوية*. هذه الأولوية مساوية للرقم التسلسلي في تكوين CLI المكافئ الخاص بها. عند تعيين رقم أقل من إدخال خريطة التشفير الحالي، يتم تنفيذ ملف التعريف الجديد هذا أولا. كلما زاد رقم الأولوية، كلما قلت القيمة. يستخدم هذا لتغيير ترتيب التسلسل الذي سيتم تنفيذ خريطة تشفير معينة به. انقر على *موافق* لإكمال إنشاء توصيف توصيل

Basic	Priority:	20	
Advanced Crypto Map Entry	Perfect Forward Secrecy:	⊙ Disable ◯ Enable	
-Tunnel group		Diffie-Helman Group:	~
	NAT-T:	Enable	
	Reverse Route Injection:	Enable	
	Security Association Lifetime	e 	
	Time:	8 : 0 : 0	hh:mm:s
	Traffic Volume:	4608000	KBytes
	Static Crypto Map Entry Par	ameters	
	Connection Type:	bidirectional	~
	CA Certificate:	None	~
		Send CA Certificate Chain	
	IKE Negotiation Mode:	Main Aggresive	
		Dffle-Helman Group;	
ndi (A Designed	

يؤدي هذا تلقائيا إلى إنشاء مجموعة نفق جديدة مع خريطة تشفير مقترنة. تأكد من إمكانية الوصول إلى BKASA باستخدام عنوان IP الجديد قبل إستخدام ملف تعريف الاتصال الجديد هذا.

<u>تحرير تكوين VPN الموجود</u>

هناك طريقة أخرى لإضافة نظير جديد وهي تعديل التكوين الموجود. لا يمكن تحرير ملف تعريف الاتصال الموجود لمعلومات النظير الجديدة لأنه مرتبط بنظير معين. in order to حررت التشكيل حالي، أنت تحتاج أن ينجز هذا steps:

- 1. إنشاء مجموعة نفق جديدة
- 2. تحرير خريطة التشفير الموجودة

<u>إنشاء مجموعة نفق جديدة</u>

انتقل إلى *التكوين > VPN من موقع إلى موقع > متقدم > مجموعات النفق* وانقر فوق *إضافة* لإنشاء مجموعة نفق جديدة تحتوي على معلومات نظير VPN الجديدة. حدد حقلي *الاس*م والمفتاح *المشترك مسبقا*، ثم انقر على *موافق*.

🖆 Add IPsec Site-to-	site Tunnel (Group			
Name:	209.165.201.2	1			
IKE Authentication					_
Pre-shared Key:	•••••				
Identity Certificate:	None			~	Manage
Send Certicate Chain:	Enable				
IKE Peer ID Validation:	Required			~	
IKE Keepalive Disable keepalives Monitor keepalives Confidence Intervo Retry Interval O Headend will never	initiate keepaliv	seconds seconds e monitoring			
Group Policy:	DfltGrpPolicy			~	Manage
IPsec Protocol:	Enabled OK	Cancel) Help]	

ملاحظة: تأكد من تطابق المفتاح المشترك مسبقا مع الطرف الآخر من شبكة VPN.

ملاحظة: في حقل "الاسم"، يجب إدخال عنوان IP فقط للنظير البعيد عندما يكون وضع المصادقة مفاتيح مشتركة مسبقا. يمكن إستخدام أي اسم فقط عندما تكون طريقة المصادقة من خلال الشهادات. يظهر هذا خطأ عندما تتم إضافة اسم في حقل الاسم ويتم مشاركة طريقة المصادقة مسبقا:

Warr	ning
^	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
WARNI iddress nethod xonfigur OK] tun OK] tun OK] isa	ING] tunnel-group New-525-VPN type ipsec-I2I L2L tunnel-groups that have names which are not an IP may only be used if the tunnel authentication is Digital Certificates and/or The peer is red to use Aggressive Mode nnel-group New-525-VPN ipsec-attributes hel-group New-525-VPN ipsec-attributes e-shared-key *********** kmp keepalive threshold 10 retry 2
	Close

<u>تحرير خريطة التشفير الموجودة</u>

يمكن تحرير خريطة التشفير الموجودة لإقران معلومات النظير الجديدة.

أكمل الخطوات التالية:

1. انتقل إلى *التكوين > VPN من موقع إلى موقع > متقدم > خرائط التشفير*، ثم حدد خريطة التشفير المطلوبة وانقر فوق

Configurati	on >	Site-to-Site VPN > Advanced	> Crypto Maps							ىخرىر.
🗣 Add 🔹	C'	idt 🔹 👔 Delete 🗇 🌾 👗	🖻 🛍 - 🛛 Q, Fir	nd 🖭 Diagr	am					
Traching	đ	Edt				Transform Eat	Date:	DEC	MAT. T. Fashlad	Denverse Dente Fashlad
туресятог	Ø	Edit Crypto Map	Destination	Service	Action	Trensrumn Sec	Peer	PES	WAT-1 Chapted	Reverse Kouce chapled
🕞 interfac	đ	Edit Traffic Selection	Mark The second		1.00				423	
stable: 1	1	I ge inside-netwo	192.168.25	💌 (p	Protect	ESP-AES-128-SHA	200.200.200		Sec.	

تظهر نافذة *تحرير قاعدة IPSec*.

2. تحت علامة التبويب سياسة النفق (أساسي)، في منطقة إعدادات النظير، حدد النظير الجديد في حقل عنوان IP الخاص بالنظير المراد إضافته. بعد ذلك، انقر فوق إضافة.

🖆 Edit IPsec Rule		
Tunnel Policy (Crypto Map) - Basic	Tunnel Policy (Crypto Map) - Advanced Traffic S	Selection
Interface: outside	Policy Type: static	Priority: 1
Transform Set to Be Added:	Add >>	Move Up
	Remove	Move Down
Peer Settings - Optional for The Connection Type is appli for LAN-to-LAN redundancy.	Dynamic Crypto Map Entries cable to static tunnel policies only. Uni-directional o Tunnel policies of the 'Originate Only' connection t	connection type policies are used ype may specify up to 10
Connection Type: bi	directional	
IP Address of Peer to Be Add	ded: 200.200.200.200	Move Up
209.165.201.2	Remove	Move Down
Enable Perfect Forwarding	Secrecy	
	OK Cancel Help	

3. حدد عنوان IP للنظير الموجود وانقر فوق *إزالة* للاحتفاظ بمعلومات النظير الجديدة فقط. وانقر فوق *.OK*

nnel Policy (Crypto Map) - Basic	Tunnel Policy (Crypto Map) - Advanced Traffic S	election
Interface: outside Transform Sets	Policy Type: static	Priority: 1
Transform Set to Be Added: ESP-AES-128-MD5	Add >>	Move Up
	Remove	Move Down
Peer Settings - Optional for E	Oynamic Crypto Map Entries	oppertion type policies are use
for LAN-to-LAN redundancy. T redundant peers.	unnel policies of the 'Originate Only' connection to	ype may specify up to 10
the start set to the		
Connection Type: bidi	rectional 🔀	
Connection Type: bidi	rectional d: Add >> Add >> Add >> Add >> 200.200.200.200 209.165.201.2	Move Up
Connection Type: bidi	rectional d: Add >> Remove Remove	Move Up
Connection Type: bidi IP Address of Peer to Be Adde	rectional d: Add >> Remove iecrecy	Move Up
Connection Type: bid IP Address of Peer to Be Adde	rectional	Move Up

ملاحظة: بعد تعديل معلومات النظير في خريطة التشفير الحالية، يتم حذف ملف تعريف الاتصال المرتبط بخريطة التشفير هذه فورا في نافذة ASDM.

4. تبقى تفاصيل الشبكات المشفرة كما هي. إذا كنت بحاجة إلى تعديل هذه العناصر، فانتقل إلى علامة التبويب *تحديد حركة مرور*

unnel Policy	(Crypto Map) - basic Tunnel Policy (Crypto Map) - Advanced Traine Selectori
ction: 💿	Protect 🔘 Do not Protect
iource:	10.10.10.0/24
estination	192.168.25.0/24
iervice:	ip 🕝

5. انتقل إلى *التكوين > VPN من موقع إلى موقع > متقدم >* جزء *خرائط التشفير* لعرض خريطة التشفير المعدلة. ومع ذلك، لا تحدث هذه التغييرات حتى تنقر فوق *تطبيق*. بعد النقر فوق *تطبيق*، انتقل إلى *التكوين > شبكة VPN من موقع إلى موقع > متقدم > مجموعات النفق* للتحقق من وجود مجموعة أنفاق مقترنة أو عدم وجودها. إذا كانت الإجابة نعم، سيتم إنشاء *ملف تعريف اتصال*

TunicDiniha	Traf	fic Selection				Triansform Cab	Dear	DEC	MAT.T Fooblad	Designer Desite
Type Prioricy	*	Source	Destination	Service	Action	transform Sec	Peer	1973	NATE Chabled	Reverse Route
interface: outside			- 61 - 1							
static: 1	1	10.10.10.0/24	192.168.25	20	Protect	ESP-AES-128-SHA	209.165.201.2		Image:	1
							Ĩ			
			- 11				,			

<u>التحقق من الصحة</u>

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم <u>أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر</u> show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر show .

• أستخدم هذا الأمر لعرض معلمات اقتران الأمان المحددة لنظير واحد:<mark>عرض نظير IPsec للتشفير <عنوان IP</mark> <u>للنظير></u>

<u>استكشاف الأخطاء وإصلاحها</u>

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

<u>تعذر على بادئ IKE العثور على النهج: :INTF test_ext، SRC: 172.16.1.103، DST 10.1.4.251</u> 10.1.4.251 يعرض هذا الخطأ في رسائل السجل عند محاولة تغيير نظير VPN من مركز VPN إلى ASA.

الحل:

قد يكون هذا نتيجة لخطوات التكوين غير الصحيحة التي تم اتباعها أثناء الترحيل. تأكد من إزالة ربط التشفير بالواجهة قبل إضافة نظير جديد. تأكدت أيضا، أن أنت استعملت العنوان من النظير في النفق-مجموعة، غير أن ليس الإسم.

<u>معلومات ذات صلة</u>

- <u>موقع إلى موقع (L2L vPN مع ASA</u>
- <u>أكثر مشاكل الشبكات الخاصة الظاهرية (VPN) شيوعا</u>
 - <u>صفحة الدعم الفني ل ASA</u>
 - الدعم التقني والمستندات Cisco Systems

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