ASA/PIX: ءالمعل ماسقنا يقفنب حامسلا VPN نيوكت لاثم ىلع VPN

المحتويات

المقدمة المتطلبات الأساسية المتطلبات المكونات المستخدمة ال<u>رسم التخطيطي للشبكة</u> المنتجات ذات الصلة <u>الاصطلا</u>حات معلومات أساسية <u>تكوين الاتصال النفقي المنقسم على ASA</u> تكوين ASA 7.x باستخدام Adaptive Security Device Manager (ASDM) 5.x باستخدام Adaptive Security Device Manager تكوين ASA 8.x مع ASA 8.x مع ASA 8.x مع ASA 8.x مع تكوين ASA 7.x والإصدارات الأحدث عبر CLI تكوين PIX 6.x من خلال CLI (واجهة سطر الأوامر) التحقق من الصحة الاتصال بعميل شبكة VPN عرض سجل عميل شبكة VPN إختبار الوصول إلى شبكة LAN المحلية باستخدام إختبار الاتصال استكشاف الأخطاء وإصلاحها تحديد باستخدام عدد الإدخالات في قائمة التحكم في الوصول (ACL) إلى النفق المقسم معلومات ذات صلة

<u>المقدمة</u>

يقدم هذا المستند إرشادات خطوة بخطوة حول كيفية السماح لعملاء شبكات VPN بالوصول إلى الإنترنت أثناء إنشاء قنوات لهم في جهاز أمان Cisco Adaptive Security Appliance (ASA) 5500 Series. يتيح هذا التكوين لعملاء الشبكات الخاصة الظاهرية (VPN) إمكانية الوصول الآمن إلى موارد الشركة عبر IPsec أثناء منح وصول غير آمن إلى الإنترنت.

ملاحظة: يعتبر إنشاء قنوات الاتصال النفقي الكامل التكوين الأكثر أمانا لأنه لا يتيح الوصول المتزامن للجهاز إلى كل من الإنترنت وشبكة LAN الخاصة بالشركات. يسمح حل توفيقي بين الاتصال النفقي الكامل والنفقي المنقسم لعملاء VPN الوصول إلى شبكة LAN المحلية فقط. راجع PIX/ASA 7.x: السماح بالوصول إلى شبكة LAN المحلية لمثال <u>تكوين عملاء VPN</u> للحصول على مزيد من المعلومات.

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

يفترض هذا المستند أن تكوين VPN للوصول عن بعد عاملا موجود بالفعل على ASA. ارجع إلى <u>PIX/ASA 7.x</u> <u>كخادم VPN بعيد باستخدام مثال تكوين ASDM</u> إذا لم يتم تكوين واحد بالفعل.

المكونات المستخدمة

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

- برنامج جهاز الأمان Cisco ASA 5500 Series Security Appliance Software، الإصدار x.7 والإصدارات الأحدث
 - Cisco Systems VPN Client، الإصدار 4.0.5

ملاحظة: يحتوي هذا المستند أيضا على تكوين PIX 6.x CLI المتوافق مع عميل Cisco VPN 3.x.

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

<u>الرسم التخطيطي للشبكة</u>

يتواجد عميل شبكة VPN على شبكة SOHO نموذجية ويتصل عبر الإنترنت بالمكتب الرئيسي.



<u>المنتجات ذات الصلة</u>

كما يمكن إستخدام هذا التكوين مع برنامج جهاز الأمان Cisco PIX 500 Series Security Appliance Software، الإصدار x.7.

<u>الاصطلاحات</u>

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

<u>معلومات أساسية</u>

في سيناريو أساسي VPN Client إلى ASA، يتم تشفير جميع حركات مرور البيانات من عميل شبكة VPN وإرسالها إلى ASA بغض النظر عن الوجهة الخاصة بها. استنادا إلى التكوين الخاص بك وعدد المستخدمين المدعومين، يمكن أن تصبح عملية الإعداد هذه ذات نطاق ترددي كبير. يمكن أن يعمل تقسيم الاتصال النفقي على تخفيف هذه المشكلة لأنه يسمح للمستخدمين بإرسال حركة المرور الموجهة إلى شبكة الشركة عبر النفق فقط. يتم إرسال جميع حركات المرور الأخرى مثل المراسلة الفورية أو البريد الإلكتروني أو الاستعراض العرضي إلى الإنترنت عبر الشبكة المحلية (LAN) لعميل الشبكة الخاصة الظاهرية (VPN).

<u>تكوين الاتصال النفقي المنقسم على ASA</u>

<u> Adaptive Security Device Manager (ASDM) 5.x يتكوين ASA 7.x باستخدام ASA 7.x المعا</u>

أتمت هذا steps in order to شكلت ك نفق مجموعة أن يسمح انقسام tunneling للمستخدمين في المجموعة.

1. أخترت **تشكيل>VPN>عام>مجموعة سياسة** وحدد المجموعة سياسة أن أنت تريد أن يمكن محلي منفذ في. ثم انقر فوق

File Options Too	is VVizordis	Help							Search:	تحرير. • Find
Home C	onfiguration	Monitoring	C Back	Forward	C Packet Tracer	Refr	esh Save	? Help		CISCO SYSTEMS
Interfaces Security Policy NAT	Configuratio	n > VPN > Gen Wizard ral VPN System Optio Clent Update Curnel Group Group Policy Jeers Default Turnel Ga Zone Labs Integrif	eral > G FG ms tev y ≦	roup Policy roup Policy Manage VPN may be storer referenced by Nam	group policies. A 5 Internally on the 7 VPN tunnel gro	. VPN gro a device o ups and u Type	up policy is a colle x externally on a f iser accounts. Turneling F	etion of user RADIUS serve Protocol	oriented atbibuteAvalue ; er. The group policy infor AAA Server Group	pairs that mation is Add _▼
VPN IPS CSD Manager	B-Sei B-Sei B-Sei P As B-Sei P As NAC B-Sei B-S	s Idress Manageme VPN Il Proxy	rt	altveteyopa DritiGrpPolicy (Sy	stem Defa	internal	PBos L2TP4PSec PSec		N/A, N/A,	Delete
Routing Routing Global Objects Properties							Apply	Rese	1	
Continuention of our	I					ainea				0 0 0 7 20 20 PM UT

2. انتقل إلى علامة التبويب تكوين العميل.

General IPSec Client Configuration Client Firewall	Hardware Client	NAC WebVPN
Banner:	Inherit	Edit Banner
Default Domain:	🔽 Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Split Tunnel Policy:	🔽 Inherit	
Split Tunnel Network List:	🔽 Inherit	Manage
Address pools		
Available Pools	Add>> < <remove< th=""><th>Assigned Pools (up to 6 entries)</th></remove<>	Assigned Pools (up to 6 entries)

3. قم بإلغاء تحديد مربع **Inherit** لنهج النفق المقسم واختر **قائمة شبكة النفق** أدناه.

Name:	hilvalleyvpn		
General IP	Sec Client Configuration Client Firewall	Hardware Client	NAC WebVPN
Check an	Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.
General	Client Parameters Cisco Client Parameters	s Microsoft Client	Parameters
Banne	r:	🔽 Inherit	Edit Banner
Defau	it Domain:	🔽 Inherit	
Solit T	unnel DNS Names (snace delimited);	V Inberit	
Opir 1	uniter pres realities (apace delinited).	iv milen	1
Split T	unnel Policy:	🗌 Inherit	Tunnel All Networks
C-8 T	un al Makazarda Lista		Tunnel All Networks Tunnel Network List Below
Spirit	unner Network List.	I ™ Innent	Exclude Network List Below
Addre	ess pools		
⊡ Ir	herit Avaietie Porte		Assigned Pagle (up to 6 entries)
			Assignment of the (up to the interes)
		Add>>	
		< <remove< td=""><td>]</td></remove<>]

4. قم بإلغاء تحديد مربع **Inherit** لقائمة شبكات النفق المقسم ثم انقر فوق **إدارة** لتشغيل إدارة قائمة التحكم في الوصول (ACL).

lit Internal Group Policy: hillvalleyvpn		
Name: hillvalleyvpn		
General IPSec Client Configuration Client Firewal	Hardware Client	NAC WebVPN
Check an Inherit checkbox to let the corresponding	setting take its valu	ue from the default group policy.
General Client Parameters Cisco Client Parameter	s Microsoft Client	Parameters
Banner:	🗹 Inherit	Edit Banner
Default Domain:	🔽 inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Split Tunnel Policy:	☐ Inherit	Tunnel Network List Below
Split Tunnel Network List:	inherit	None Manage
Address pools		
Aveilable Pools		Assigned Pools (up to 6 entries)
	Add>>	
	< <remove< td=""><td>]</td></remove<>]
	Cancal	Help
	COLICOT	

5. ضمن إدارة قائمة التحكم في الوصول (ACL)، أختر **إضافة > قائمة التحكم في الوصول (ACL)**.. لإنشاء قائمة وصول جديدة.

AEL Manager				2
Standard ACL Extended ACL				
🛧 Add 🔹 🗃 Edit. 🏦 Delete 🔶	4 % mm -			
Add ACL dress	Action	Description		
🔹 Add ACE 🤸				
🚖 Inseri				
🔹 Insert Atter				
				I
-Rule Flow Diagram				×
	3- 	inside out	side 🔤	
		A deput		
		V deny		
	ОК	Cancel	Help	

6. قم بتوفير اسم لقائمة التحكم بالوصول (ACL) وانقر فوق موافق

				اقق.
CL Manager		Ĩ.		
tandard ACL Extended ACL				
Add - State Calendar Acc	V Do. etc.			
	6 18 16 T			
No Address	Action Descr	iption		
	2		and and	
	S Add ACL		×	
	ACL Name: Splt_Tunnel_List			
		1	1	
	ок се	ncel	Help	
	n			
Rule Flow Diagram				×
	B- inside	outside	-3	
	.04			
	v 0	any		
		ncel	Help	
			тер	

7. بمجرد إنشاء قائمة التحكم في الوصول، أختر **إضافة > إضافة ACE..** لإضافة إدخال التحكم في الوصول

				.(ACE)
ACL Manager	— 1 1 , 0.,			×
Standard ACL Extended ACL				
🗣 Add 🕞 📝 Edit 📋 Delete	+ + X == @	+		
🗣 Add ACL dress	Action	Description		
Add ACE				
Rule Flow Diagram		iosida outoida		×
	3	→ v deny		
	0	K Cancel	Help	

8. عينت ال ACE أن يماثل ال LAN خلف ال ASA. في هذه الحالة، الشبكة هي 24/10.0.1.0.أختر **سماح**.أختر عنوان IP **من 10.0.1.**أختر قناع شبكة 255.255.0(*إختياري)* قم بتوفير وصف.وانقر فوق OK.

🕵 ACL Manager	×
Stenderd ACL Extended ACL	
💠 Add 🝷 📝 Edic 🗻 Delete 🎓 🎸 👗 ங 🏨 🗧	
No Address Action Description	
Spit_Tunnel_List	
🕵 Add ACE	
Action	
Action 🖌 Permit 💌	
HostAletwork	
IP Address: 10.0.1.0	
Netmosk: 255.255.255.0	
The compare network behind the ASA	
OK Cancel Haip	
	,
Rule Flow Diagram	×
deny	
OK Cancel Help	

9. انقر فوق **موافق** للخروج من إدارة قائمة التحكم في الوصول (ACL).

P AGO	· mor moste 7			
No	Address	Action	Description	
-Splt_1	unnel_List			
àule Flov	v Diagram	54	inside outside	

10. تأكد من تحديد قائمة التحكم في الوصول (ACL) التي قمت بإنشائها للتو لقائمة شبكات النفق

Name: hillvalleyvpn			
General PSec Client Configuration Client Firewall	Hardware Client	NAC WebVPN	
Check an Inherit checkbox to let the corresponding	setting take its valu	ue from the default group policy.	
	1		
General Client Parameters Cisco Client Parameters	s Microsoft Client	Parameters	1
Banner:	🔽 Inherit	Edit Banner	
	_		
Default Domain:	M Inherit		
Split Tunnel DNS Names (space delimited):	🔽 Inherit		
Soft Turned Delet	- Interest	Tunnel Metwork List Palaus	
Split Tunner Policy.) innent		
Split Tunnel Network List:	🗖 Inherit	Splt_Tunnel_L Manage	
- Address node		None Solt Turnel List N	
Imperit		outside_cryptomap	
Available Pools		Assigned Pools (up to 6 entries)	
	Add>≻	1	
	< <remove< td=""><td>1</td><td></td></remove<>	1	
		1	
	1	1	_

11. انقر فوق **موافق** للعودة إلى تكوين "نهج المجموعة".

dit Internal Group Policy: hillvalleyvpn		
Nama		
realite. print and y that		
General IPSec Client Configuration Client Firewall	Hardware Client	NAC WebVPN
Check an Inherit checkbox to let the corresponding	setting take its val	ue from the default group policy.
General Client Parameters Cieno Client Parameters	Microsoft Cleri	Deremetere
	T Microsoft Cierr	
Banner:	🔽 Inherit	Edit Berner
Defeid Dowein:	kiberit	
Derdal Deman.	I* WHICH	
Split Tunnel DNS Names (space delimited):	🗹 Inherit	
Split Tunnel Policy:	Inherit	Tunnel Network List Below
, , , , , , , , , , , , , , , , , , , ,		
Split Tunnel Network List:	🗌 Inherit	Splt_Tunnel_L Manage
Address pools		
⊡ Inherit		
Available Pools		Assigned Pools (up to 6 entries)
	Add⊳⊳	1 1
	< <remove< td=""><td>i </td></remove<>	i
		·
OK LZ	Cancel	Heip

12. طقطقة **يطبق** وبعد ذلك **يرسل** (إن يتطلب) in order to أرسلت الأمر إلى ال ASA.

File Options To	ols VVizards	Help				Search	:	Find +
Iome	og Configuration	Monitoring Bac	k Forward Pa	cket Tracer 🛛 Ref	liresh Save	? Help		CISCO SYSTEMS
Interfaces	Configuration	on > VPN > General > I'Mizard eral VPN System Options Client Update Turnel Group Group Policy Users Default Turnel Gatev	Broup Policy Group Policy Manage VPN grou may be stored inte referenced by VPI Name	p policies. A VPN gr amaly on the device N tunnel groups and Type	oup policy is a collect or externally on a R luser accounts.	ction of user-oriente (ADIUS server. The g retocol (AAA	d attribute/value pai group policy informs 1. Server Group [rsthat tion is Add ▼
NAT	E-S KE	Zone Labs Integrity 5	hilvaleyypn	Internal	PSec	N(A		
	E-B PSe E-B PAC	c ddress Management	DthGrpPolicy (System	n Defa Internal	L2TP-IPSec JPSec	N/A		Edit
IPS CSD Manager	↓ ──讀 MAC 中國 Web 日 省 E-me) JVPN ali Praxy						Delete
Global Objects					Apply	Reset	[
	<u> </u>				N.	1 100		
				cisco	2	<u>i</u>	🔂 Z.	26/06 1:33:20 PM UTC

<u>Adaptive Security Device Manager (ASDM) 6.x مع ASA 8.x تكوين</u>

أتمت هذا steps in order to شكلت ك نفق مجموعة أن يسمح انقسام tunneling للمستخدمين في المجموعة.

Access VPN (**تكوين) > Configuration (وصول عن بعد) > Network (عميل) Access (عميل) > Network (عميل) (وصول الشبكة)** (وصول الشبكة) > Group Policy (نهج المجموعة)، واختر Group Policy (نهج المجموعة) الذي تريد تمكين الوصول إلى LAN المحلي فيه. ثم انقر فوق

			بحرير.
onfiguration > Remote Access VPN > N	letwork (Client) Acce	ss > Group Policies	
Manage VPN group policies. A VPN group p externally on a RADIUS/LDAP server. The Add - CE Edit Delete	oolicy is a collection of us group policy information	er-oriented attribute/value pairs that may n is referenced by VPN tunnel groups and u	be stored internal ser accounts.
Name	Туре	Tunneling Protocol	T
			A
DfltGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webvpn	N/A
DfltGrpPolicy (System Default) Defaultgroup	Internal Internal	L2TP-IPSec, IPSec, webvpn Inherited	N/A N/A

2. انقر فوق **تقسيم الاتصال** النفقي.

General Servers Advanced	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and th require tunneling. The security appliance makes split tunneling decisions on the basis of a network list ACL that consists of list of addresses on the private network.	ose that do n st, which is ar
	DNS Names: Inherit Policy: Inherit Network List: Inherit	Manage
-Hardware Client	Intercent DHCP Configuration Message from Micosoft Clients	
	Intercept: 🔽 Inherit C Yes C No	

3. قم بإلغاء تحديد مربع **Inherit** لنهج النفق المقسم، واختر **قائمة شبكة النفق أدناه**.

🖆 Edit Internal Group Policy:	hivalleyvpn
General Servers Advanced IE Browser Proxy SSL VPN Client	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do no require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network. DNS Names: Inherit Policy: Inherit Tunnel Network List Below Inherit
Client Access Rule	Network List: Inherit Tunnel All Networks Tunnel Network List Below Exclude Network List Below
	Intercept DHCP Configuration Message from Micosoft Clients
	prior to XP, DHCP Intercept provides the domain name and subnet mask. Intercept: Inherit C Yes C No
	Subnet Mask (Optional): 0.0.0.0
<u>↓</u>	
	OK Cancel Help

4. قم بإلغاء تحديد مربع Inherit لقائمة شبكات النفق المقسم، ثم انقر فوق Manage لتشغيل إدارة قائمة التحكم في الوصول (ACL).

- General - Servers - Advanced	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and require tunneling. The security appliance makes split tunneling decisions on the basis of a network ACL that consists of list of addresses on the private network.	those that do no k list, which is an
IE Browser Proxy	DNS Names: 🔽 Inherit	Ĩ
SSL VPN Client IPsec Client	Policy: Tunnel Network List Below]
Client Access Rule Client Firewall, Hardware Cleat	Network List: Tinherit None	Manage)
Hardware Cleric	Intercept DHCP Configuration Message from Micosoft Clients	*
	Subnet Mask (Optional): 0.0.0.0	×
	Subnet Mask (Optional): 0.0.0.0	¥
	Subnet Mask (Optional): 0.0.0.0	<u><u></u></u>
	Subnet Mask (Optional): 0.0.0.0	Y

5. ضمن إدارة قائمة التحكم في الوصول (ACL)، أختر **إضافة > قائمة التحكم في الوصول (ACL)**.. لإنشاء قائمة وصول

Manager		and the second se		جدیدہ.	
dard ACL Extended Ac	1)				
Add 🔻 💕 Edit 🏢	Delete 🛉 🛧 🖌	* * •	1. +		
Add ACL	53	Action	Description		
Add ACE		10			
Insert	-				
Insert After					
	Manager dard ACL Extended AC dd CL Add ACL Add ACE Insert Insert After	Manager dard ACL Extended ACL add CL Add ACL Add ACE Insert Insert After	Manager dard ACL add → Edit Delete ★ Add ACL Add ACE Insert Insert After	Manager dard ACL Add ACL Add ACL Add ACE Insert Insert After	

6. قم بتوفير اسم لقائمة التحكم بالوصول (ACL)، وانقر فوق **موافق**.

	Address	Action	Description	
	A EL	dd ACL . Name: Split_Tunnel_Li OK Car	ist ncel Help	<
في الوصول	لإضافة إدخال التحكم	ضافة > إضافة ACE	التحكم في الوصول، أختر إ	 رد إنشاء قائمة
في الوصول L Manage	لإضافة إدخال التحكم ^ا ۲	ضافة > إضافة ACE	الحجيم التحكم في الوصول، أختر إ	ـــــــــــــــــــــــــــــــــــــ
في الوصول L Manage	لإضافة إدخال التحكم er Extended ACL	ضافة > إضافة ACE	الحجيم التحكم في الوصول، أختر إ	ارد إنشاء قائمة (A
في الوصول CL Manage andard ACL Add ح	لإضافة إدخال التحكم er Extended ACL أ Edit أ Delete	ضافة > إضافة ACE	التحكم في الوصول، أختر إ	ارد إنشاء قائمة (Ai

8. عينت ال ACE أن يماثل ال LAN خلف ال ASA. في هذه الحالة، الشبكة هي 24/10.0.1.0. طقطقت **ال يسمح** لاسلكي زر.أختر عنوان الشبكة باستخدام القناع **24/10.0.1.0** .(إختياري) قم بتوفير وصف.وانقر فوق

dd 🔻 📗	and Arial a	× 1 × ~ ~		
	Edit 🔟 Delete	4 2 回國	T .	
lo	Address	Action	Description	
lit_Tunne	l_List			
	dd ACE			
	Action: 0	Permit C Deny		
	Address: 1	10.0.1.0/24		
	Description.			
	Description:	is at a set work had the	464	
	The Corpor	ate network bening the	ADA	
		ОК	Cancel	Help

9. انقر فوق **موافق** للخروج من إدارة قائمة التحكم في الوصول .(ACL)

Standard ACL Extended ACL Add C Extended ACL Address Action Description Split_Tunnel_List I Extended ACL Address Action Description Desc	Standard ACL Exten	ded ACL]			
Add C C Edit Delete C Action Description Split_Tunnel_List 1 C 10.0.1.0/24 Permit The Corporate network behind the ASA	Excon	dog Her I			
No Address Split_Tunnel_List 1 r 10.0.1.0/24 Permit The Corporate network behind the ASA	🖨 Add 👻 🗖 Edit	🛱 Delete 🛛 🔺	x x	s m +	
No Address Action Description □ Split_Tunnel_List					
Spit_Tunne_List The Corporate network behind the ASA	No	Address	Action	Descript	on
		1.0/24	A Dormit	The Corporate petwork	behind the ASA
	1 <u>E</u> e 10.0.	1.0/24	Perilic	The Corporate network	
			7		1
OK Z Cancel Help			ال ال	OK Cano	el Heln

10. تأكد من تحديد قائمة التحكم في الوصول (ACL) التي قمت بإنشائها للتو لقائمة شبكات ا المقسم.

General Servers Advanced Split Tunneling	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and the require tunneling. The security appliance makes split tunneling decisions on the basis of a network list ACL that consists of list of addresses on the private network.	se that do n , which is an
E Browser Proxy SSL VPN Client	DN5 Names: ✓ Inherit Policy: □ Inherit Tunnel Network List Below	
Client Access Rule Client Firewall Hardware Client	Network List: Inherit Split_Tunnel_List	Manage
	Intercept DHCP Config Split_Tunnel_List	*
	DHCP Intercept lets Microsoft XP clients use split tunneling with the security appliance. For Windows prior to XP, DHCP Intercept provides the domain name and subnet mask. Intercept: Inherit C Yes C No Subnet Mask (Optional): 0.0.00	; clients

11. انقر فوق **موافق** للعودة إلى تكوين "نهج المجموعة".

音 Edit Internal Group Policy: hivalleyvpn

General Servers ⊡-Advanced Split Tunneling	Split tunneling network list require tunneling. The set ACL that consists of list of	ts distinguish networks that require traffic to go through the tunnel and curity appliance makes split tunneling decisions on the basis of a networ f addresses on the private network.	d those that do not rk list, which is an
IE Browser Proxy	DNS Names: 🔽 Inherit	1	
SSL VPN Client IPsec Client	Policy: 🗖 Inherit	Tunnel Network List Below]
	Network List: 🔲 Inherit	Split_Tunnel_List	Manage
	Intercept DHCP Conf	iguration Message from Micosoft Clients	*
	DHCP Intercept lets Mic prior to XP, DHCP Inter	rosoft XP clients use split tunneling with the security appliance. For Wir cept provides the domain name and subnet mask.	idows clients
	Intercept: 🔽 Inherit	C Ves. C No	
		Subnet Mask (Optional): 0.0.0	Ŧ

12. طقطقة **يطبق** وبعد ذلك **يرسل** (إن يتطلب) in order to أرسلت الأمر إلى ال ASA.

Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored internexternally on a RADIUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.

Name	Туре	Tunneling Protocol	
tGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webvpn	N/A
faultgroup	Internal	Inherited	N/A
alleyvpn	Internal	svc,IPSec	N/A

<u>تكوين ASA 7.x والإصدارات الأحدث عبر CLI</u>

بدلا من إستخدام ASDM، أنت يستطيع أتمت هذا steps في ال ASA CLI in order to سمحت انقسام tunneling على ال ASA:

ملاحظة: تكوين اتصال CLI النفقي المنقسم هو نفسه لكل من ASA 7.x و x.8.

```
    1. ادخل إلى وضع التكوين.
    1. ادخل إلى وضع التكوين.
    2. ciscoasa
    2. ASA دiscoasa(config)#access-list Split_Tunnel_List remark The corporate network behind the ASA ciscoasa(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0
```

- 3. أدخل وضع تكوين "نهج المجموعة" للنهج الذي ترغب في تعديله. ciscoasa(config)#**group-policy hillvalleyvpn attributes** (ciscoasa(config-group-policy#
- .4. حدد نهج نفق التقسيم. في هذه الحالة، يتم **تحديد** النهج **tunnelspecified**. ciscoasa(config-group-policy)#split-tunnel-policy tunnelspecified

حدد قائمة الوص	ل النفق المقسم. في هذه الحالة، تكون القائمة SPLIT_TUNNEL_LIST. 5.
Tunne1_List_:	ciscoasa(config-group-policy)#split-tunnel-network-list value Sp
قم بإصدار هذا	مر:
1-attributes	ciscoasa(config)# tunnel-group hillvalleyvpn gen
إقران نهج المج	عة بمجموعة النفق
nillvalleyvpn	ciscoasa(config-tunnel-ipsec)# default-group-polic
8. خرجت الإثنان ت. policy)# exit (config)# exit #ciscoasa	کیل أسلوب. ciscoasa(config-grow ciscoas
9. احفظ التكوين 9	ى ذاكرة الوصول العشوائي غير المتطايرة (NVRAM) واضغط على Enter عند طلبها لتحديد
اسم الملف المد	ر.
artup-config	ciscoasa# copy running-config

?[Source filename [running-config Cryptochecksum: 93bb3217 0f60bfa4 c36bbb29 75cf714a

(bytes copied in 3.470 secs (1282 bytes/sec 3847 #ciscoasa

<u>تكوين PIX 6.x من خلال CLI (واجهة سطر الأوامر)</u>

أكمل الخطوات التالية:

قم بإنشاء قائمة الوصول التي تعرف الشبكة خلف PIX.

PIX(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0

2. قم بإنشاء مجموعة VPN *VPN3000* وحدد قائمة التحكم في الوصول للنفق المنقسم إليها كما هو موضح: PIX(config)#vpngroup vpn3000 split-tunnel Split_Tunnel_List

ملاحظة: ارجع إلى <u>Cisco Secure PIX Firewall 6.x و Cisco VPN Client 3.5 ل Windows مع مصادقة</u> <u>Microsoft Windows 2000 و IAS RADIUS 2003</u> للحصول على مزيد من المعلومات حول تكوين الوصول عن بعد VPN ل PIX 6.x.

.1

<u>التحقق من الصحة</u>

اتبع الخطوات الواردة في هذه الأقسام للتحقق من التكوين الخاص بك.

- <u>الاتصال بعميل شبكة VPN</u>
- <u>عرض سجل عميل شبكة VPN</u>
- إختبار الوصول إلى شبكة LAN المحلية باستخدام إختبار الاتصال

<u>الاتصال بعميل شبكة VPN</u>

قم بتوصيل عميل الشبكة الخاصة الظاهرية (VPN) بمركز الشبكة الخاصة الظاهرية (VPN) للتحقق من التكوين الخاص بك.

				2
ه ان ما		الذيب المالية الم		1 1
ىم ايف على	اك من القائمة	الانصال الحاص د	כע ונכוו.	I.I
0		. 0 0	<u> </u>	

-		1

VPN Client - Version 4.0.5 (Rel)		صیل. د ا ت ا ـــــــــــــــــــــــــــــــــــ
onnection Entries Status Certificates Log	Options Help	
Connect New Import	odify Delete	CISCO SYSTEMS
Connection Entries Certificates Log		1+
Connection Entry	Host	I ransport
		_

2. أدخل بيانات الاعتماد الخاصة

👌 ¥PN Client Us	er Autheni	tication f	or "hillvalley	vpn"		×
CISCO SYSTEMS	<u>U</u> sername: <u>P</u> assword:	marty				_
			OK		Cancel	

3. أختر **الحالة > الإحصائيات.**. لعرض نافذة تفاصيل النفق حيث يمكنك فحص تفاصيل النفق ورؤية تدفق حركة

Funnel Details	Route Details	Firewall	
Address Info	rmation	Connection Informa	tion
Client:	10.0.1.50	Entry:	hillvalley2
Server:	172.22.1.160	Time:	0 day(s), 00:00.25
Bytes		Crypto	
Received:	0	Encryption:	168-bit 3-DES
Sent	1494	Authentication:	HMAC-SHA1
Packets		Transport	
Encrypted:	9	Transparent Tunne	ling: Inactive
Decrypted:	0	Local LAN:	Disabled
Discarded:	0	Compression:	None
Bypassed:	159		
			Reset
			Close

4. انتقل إلى علامة التبويب تفاصيل المسار للاطلاع على الموجهات التي يقوم عميل شبكة VPN بتأمينها إلى في هذا المثال، يقوم عميل الشبكة الخاصة الظاهرية (VPN) بتأمين الوصول إلى 24/10.0.1.0 بينما لا يتم تشفير جميع حركة مرور البيانات الأخرى ولا يتم إرسالها عبر

VPN Client Sta	tistics			×
Tunnel Details	oute Details Firewal			
Local LAN Routes	; K	Secured Routes		
Network	Subnet Mask	Network	Subnet Mask	
		10.0.1.0	255.255.255.0	
		J		-11
			_	
			<u>C</u> lose	

عرض سجل عميل شبكة <u>VPN</u>

عندما يفحص أنت ال VPN زبون سجل، أنت يستطيع حددت ما إذا أو لا المعلمة أن يعين انقسام tunneling يكون

ثبتت. لعرض السجل، انتقل إلى علامة التبويب "السجل" في عميل شبكة VPN. ثم انقر فوق **إعدادات السجل** لضبط ما تم تسجيله. في هذا المثال، يتم تعيين IKE على **3 - مرتفع** بينما يتم تعيين كل عناصر السجل الأخرى على **1 -منخفض**.

👶 VPN Client - Version 4.0.5 (Rel)	
Connection Entries Status Certificates Log Options Help	
Disable Clear Log Settings Log Window	CISCO SYSTEMS
Connection Entries Certificates Log	
Cisco Systems VPN Client Version 4.0.5 (Ref) Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Windows, WinNT Running on: 5.1.2600 Service Pack 2	
Not connected.	

(Cisco Systems VPN Client Version 4.0.5 (Rel .Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved Client Type(s): Windows, WinNT Running on: 5.1.2600 Service Pack 2

Sev=Info/6IKE/0x6300003B 07/27/06 14:20:09.532 1 .Attempting to establish a connection with 172.22.1.160

Output is supressed 18 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005D Client sending a ---! firewall request to concentrator 19 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Systems Integrated Client, Capability= (Centralized Protection Policy). 20 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Intrusion Prevention Security Agent, Capability= (Are you There?). 21 14:20:14.208 07/27/06 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.160 22 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.22.1.160 23 14:20:14.208 07/27/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.22.1.160 24 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50 25 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0 26 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300000 MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000 27 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 28 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300000E MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems, Inc ASA5510 Version 7.2(1) built by root on Wed 31-May-06 14:45 !--- Split tunneling is permitted and the remote LAN is defined. 29 14:20:14.238 07/27/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets), value = 0x00000001 30 14:20:14.238 07/27/06 Sev=Info/5 IKE/0x6300000F SPLIT_NET #1 subnet = 10.0.1.0 mask = 255.255.255.0 protocol = 0 src .port = 0 dest port=0 !--- Output is supressed

<u>إختبار الوصول إلى شبكة LAN المحلية باستخدام إختبار الاتصال</u>

هناك طريقة إضافية لاختبار تكوين عميل شبكة VPN لنفقي منقسم أثناء إنشاء قنوات في ASA هي إستخدام الأمر ping في سطر الأوامر في Windows. ال LAN المحلي من ال VPN زبون 24/192.168.0.0 ومضيف آخر حاضر على الشبكة مع عنوان 192.168.0.3.

> C:\>ping 192.168.0.3 :Pinging 192.168.0.3 with 32 bytes of data Reply from 192.168.0.3: bytes=32 time<1ms TTL=255 :Ping statistics for 192.168.0.3 (Packets: Sent = 4, Received = 4, Lost = 0 (0% loss :Approximate round trip times in milli-seconds Minimum = 0ms, Maximum = 0ms, Average = 0ms

استكشاف الأخطاء وإصلاحها

<u>تحديد باستخدام عدد الإدخالات في قائمة التحكم في الوصول (ACL) إلى النفق المقسم</u>

هناك تقييد يحتوي على عدد الإدخالات في قائمة التحكم بالوصول (ACL) المستخدمة للنفق المقسم. يوصى بعدم إستخدام أكثر من 50 إلى 60 إدخال ACE للحصول على وظائف مرضية. يوصى بتنفيذ ميزة تقسيم الشبكة إلى شبكات فرعية لتغطية نطاق من عناوين IP.

<u>معلومات ذات صلة</u>

- <u>PIX/ASA 7.x كخادم VPN بعيد باستخدام مثال تكوين ASDM</u>
- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
 - <u>الدعم التقني والمستندات Cisco Systems</u>

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