

中国科学技术大学 曾凡平

billzeng@ustc.edu.cn

2023秋季,网络安全,课程编号:COMP6216P

New: Windows Server 2012及后续版本对VPN的支持

• Windows Server 2003的后续版本对VPN提供了支持, 配置方式是 相似的。

VPN配置实例

Windows Server 2012的VPN

Windows Server 2012的PPTP VPN





VPN技术











VPN技术

远程访问"角色和功能"安装成功之后的配置



	Internet 协议版本 4 (TCP/IPv4) 属性 🛛 🗙	
	常规 如果网络支持此功能,则可以获取自动指派的 IP 设置。否则,你需要从网 络系统管理员处获得适当的 IP 设置。	
	 自动获得 IP 地址(Q) ● 使用下面的 IP 地址(S): IP 地址(I): 子网掩码(U): 工55,255,0,0 取认网关(D): 166,66,66,233 	
	 ○ 自动获得 DNS 服务器地址(B) ● 使用下面的 DNS 服务器地址(E): 首选 DNS 服务器(P): 	
正确设置IP地址和默认网关的IP地址。	备用 DNS 服务器(A): Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ	
	确定 取消	



路由和远程访问的配置: 同Windows 2003

	路由和远程访问服务器安装向导
	配置 你可以启用下列服务的任意组合,或者你可以自定义此服务器。
	 远程访问(拨号或 VPN)(R) 允许远程客户端通过拨号或安全的虚拟专用网络(VPN) Internet 连接来连接到此服务器。 网络地址转换(NAT)(E) 允许内部客户端使用一个公共 IP 地址连接到 Internet。 虚拟专用网络(VPN)访问和 NAT(V) 允许远程客户端通过 Internet 连接到此服务器,本地客户端使用一个单一的公共 IP 地址连 接到 Internet。 两个专用网络之间的安全连接(S)
	将此网络连接到一个远程网络,例如一个分支机构。 ○ 自定义配置(C)
在此选择"虚拟专用网	X 选择在路由和远程访问中的任何可用功能的组合。
(VPN)访问和NAT";	
其他的配置方法与 Windows2003完全一样。	ー フ マ 上一步(B) 下一步(N) > 取消

VPN用户的设置: 同Windows 2003

					vpn 属性 ? × 常规 隶属于 配置文件 环境 会话
		计管机会	·····································		远程控制 远程桌面服务配置文件 拨入
□□□ 文件(F) 操作(A) 查看(V) 帮	助(H)	PT #7/08	5/I		网络访问权限
🗢 🄿 🖄 📰 😫	?				① 允许访问(W)
፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟፟	名称	全名	描述	操作	C: 拒绝访问(D)
▲ 🕌 系统工具 ▶ 🚇 任务计划程序	Administrat		管理计算机(域)的内置帐户 供来完实词计算机或实词域的中	用户	C 通过 NPS 网络策略控制访问(P)
▶ 🛃 事件查看器	st odest Vpn	vpn	(天本共初间11 异小666001月28613133	更多操作 ▶	
▶ 100 共享文件夹 ▲ ▲ 本地用户和组				vpn ▲	
				5C371#1 F	
					C 由呼叫方设置(仅路由和远程访问服务)(S)
→ 设备管理器					
⊿ 譬 存储 ▷ 狐 Windows Server Back					
₩ 磁盘管理					□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
▶ 🌆 服务和应用程序					定义要为此拨入连接启用的 IP 地址。
	1				前态 17 乃伍(1) ***
					□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □
					为此拨入连接定义要启用的路由。 静志路由(1)
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	田白、	nn的"坩	入" 届性为'	"	() 确定 取消 应用(A) 帮助
以且	) I] ) · V		い、両上り		er 2012 R2 Standard

远程客户端的VPN拨入

		1
我的电脑	▲ C:\work>ipconfig	
	Windows IP Configuration	
Ericka Gpg4win Document 203 Kleopatra 安全配置向 Wireshark 号	Ethernet adapter 本地连接: Connection-specific DNS Suffix . : IP Address	
	C:\work>ping 10.0.0.13	
	Pinging 10.0.0.13 with 32 bytes of data:	
	Reply from 10.0.0.13: bytes=32 time=3ms TTL=127 Reply from 10.0.0.13: bytes=32 time=2ms TTL=127 Reply from 10.0.0.13: bytes=32 time=1ms TTL=127 Reply from 10.0.0.13: bytes=32 time=1ms TTL=127	
	<pre>Ping statistics for 10.0.0.13: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 3ms, Average = 1ms</pre>	1
🦺 开始 🧑 🚱 🕿 🚄 🏹 🙃 🦿 🧰 🔤 CMD		alian 😵 😨 💀 🖗 16:36

#### 在路由器上用wireshark观察到的现象

Capturing from VMInet6 [Vireshark 1.	10.6 ( <del>v</del> 1.10.6 from ma	ster-1.10)]		_ [5] ×
<u>File Edit View Go Capture Analyze Statis</u>	itics Telephon <u>y T</u> ools <u>I</u> r	nternals <u>H</u> elp		
● ● ◢ ■ ◢   ⊡ ▷ ≭ 22   9	् 🔅 🕸 🖨 🕹		⊕, ⊖, ⊕,    👪 🗵 畅 %   🕱	
Filter:		▼ Expression	Clear Apply Save	
No. Time Source	Destination	Protocol Le	ngth Info	
1 0.00000000 55.0.0.15	166.66.66.213	PPP Con	111 Compressed data	
2 0.00073900 166.66.66.213	55.0.0.15	PPP Cont	115 Compressed data	
3 0.09445300 55.0.0.15	166.66.66.213	GRE	60 Encapsulated PPP	
4 1.02095600 55.0.0.15	166.66.66.213	PPP Cont	111 Compressed data	
5 1.02141500 166.66.66.213	55.0.0.15	PPP Cont	115 Compressed data	
6 1.11539200 55.0.0.15	166.66.66.213	GRE	60 Encapsulated PPP	
/ 1.99688/00 55.0.0.15	166.66.66.213	PPP Cont	111 Compressed data	
8 1.99766900 166.66.66.213	55.0.0.15	PPP Cont	115 Compressed data	
9 2.09734200 55.0.0.15	166.66.66.213	GRE	60 Encapsulated PPP	
10 2.99886300 55.0.0.15	166.66.66.213	PPP Con	111 Compressed data	
11 2.99976900166.66.66.213	55.0.0.15	PPP Con	115 Compressed data	
12 3.09774400 55.0.0.15	100.00.00.213	GRE	60 Encapsulated PPP	
13 4.73014400 CadmusCo_SC:15:16	CadmusCo_36:72:8a	ARP	60 Who has 166.66.66.2337 Tell 166.66.66.213	
14 4.73019400 CadmusCo_36:72:8a		ARP	42 100.00.00.233 15 at U8:00:27:30:72:8a	
	55.U.U.IS	PPTP	70 Echo-Request	
16 /.//812900 55.0.0.15		PPIP	74 ECHU-REPTY 60 metrix 1020 [Actv] com 17 Act 21 win 62664 Lon 0	
17 7.83926000166.66.66.213	55.U.U.IS	TCP	60 pptp > 1030 [ACK] Sed=17 ACK=21 WIN=63664 Len=0	
4				
The second secon	·+-> 111 but a com		hita) an intanfasa A	
Ethonpot II Spc: CodmusCo 26:72:	95 (08.00.37.26.73.9	ureu (888 20) - Detti	pris) on interface o admusca 56:15:16 (08:00:27:56:15:16)	
Toternet Protocol Version 4 Src:		5a), DSL. ( 15) Det. (	66 66 66 712 (166 66 66 712)	
E Generic Pouting Encansulation (PP)	)).0.0.1) ()).0.0.1	LJ), DSL	00.00.00.215 (100.00.00.215)	
Repaint to Point Protocol	e)			
PBD Compressed Datagram				
PPP Compressed Datagram				
0000 08 00 27 5c 15 1b 08 00 27 30	6 72 8a 08 00 45 00		'6rE.	
0010 00 61 00 d9 00 00 7f 2f 1a 6f	F 37 00 00 0f a6 42	.a,	.07B	
0020 42 d5 30 01 88 0b 00 41 aa 4a	a 00 00 00 35 fd 90	в.0)		
10030 24 c2 39 5c 10 c2 45 3a 62 a2	2 bc 08 96 70 db 11	\$.9\E	bp.	
10040 up 86 69 CT 46 C8 11 42 02 8. 10050 pp 25 05 d6 pd bc f2 d1 0p 01	L 104 93 UC IC 88 74 1 77 17 17 76 ds 55	N	ω θ. Π	▼
🔘 💅 VMnet6: <live capture="" in="" progress=""> File: C</live>	Packets: 17 · Displayed: 1	7 (100.0%)		Profile: Default

# Windows Server 2012的"网关一网关" VPN

#### 配置方法与Windows 2003的相似

在VPN网关上安装"远程访问"角色和功能

#### 配置方法同Windows 2012的 远程访问VPN (PPTP VPN)



### 通过"服务管理器"-"工具"选择"本地安全策略"



### VPN网关上的"IP安全策略"的配置





IP 安全策略向导 X			
	欢迎使用 IP 安全策略向导		
	此向导帮助你创建 IP 安全策略。你将指定对于特定的 IP 通信类 型,以及与特定计算机或计算机组(子网)通信时使用的安全级 别。		
	单击"下一步"继续。		
	< 上一步(B) 下一步(N) > 取消		

IP 安全策略向导	IP 安全策略向导 X
IP 安全策略名称 命名这个 IP 安全策略并且给出一个简短的描述	<b>安全通讯请求</b> 指定这个策略如何对安全通讯的请求作出响应。
名称( <u>M</u> ): VPN(网关A和网关B的IPSec)	默认响应规则在没有其他规则适用时,对请求安全的远程计算机作出响应。为了安全地通讯,计算机必须对安全通讯请求做出响应。
描述(D):	注意: 仅在运行 Windows 2003 和 Windows XP 的计算机上支持默认响应规则。
	□ 激活默认响应规则(仅限于 Windows 的早期版本)(R)。
< 上一步(B) 下一步(N) > 取消	< 上一步( <u>B</u> ) 下一步( <u>N</u> ) > 取消

VPN(网关A和网关B的IPSec) 属性 ? ×	
	安全规则向导
	欢迎使用创建 IP 安全规则向导
 IP 安全规则([]:	安全规则根据条件,如 IP 筛选器列表中的源、目标、IP 流量类型来决定启动安全的方式和时间。
IP 筛选器列表     筛选器操作     身份验证方法     隧道终结点       □ <动态>     默认响应(仅限于     Kerberos     <无>	安全规则包含安全操作的集合,当通讯与 IP 筛选器列表中的条件匹配时,会激活这些操作。
	安全操作: - IP 隧道操作属性 - 身份验证方法
	单击"下一步"继续。
< Ⅲ > 添加(D) 编辑(E) 删除(R) ☑ 使用"添加向导"(W)	
 确定 取消	<ul> <li>&lt; 上一步(B) 下一步(N) &gt; 取消</li> </ul>

安全规则向导	安全规则向导	×
<b>隧道终结点</b> 隧道终结点是最接近 IP 流量目标的隧道操作计算机,正如安全规则的 IP 筛选器列表所指 定的。	<b>网络类型</b> 安全规则必须应用到一种网络类型。	
IPsec 隧道允许数据包在两台计算机间以直接的专用连接的安全级别通过公用或专用网络。	选择网络类型:	
指定 IP 安全规则的隧道终结点: ○ 此规则不指定隧道① ④ 隧道终结点由下列 IP 地址指定①: IPv4 隧道终结点: 166.66.66.213 IPv6 隧道终结点:	<ul> <li>所有网络连接(C)</li> <li>局域网(LAN)(L)</li> <li>远程访问(<u>R</u>)</li> </ul>	
< 上一步(B) 下一步(N) > 取消	< 上一步(B) 下一步(N) >	取消

安全规则向导	IP 筛选器列表 X
IP 筛选器列表 请为采用这个安全规则的 IP 流量类型选择 IP 筛选器列表。	■ IP 筛选器列表由多个筛选器组成。这样,多个子网、IP 地址和协议可被整合到一个 IP ■ 筛选器中。
如果下面的列表没有符合你需要的 IP 筛选器,请单击"添加"来创建新的。	名称(N): A to B 添加(A)
名称 描述 添加(A) 编辑(E) 删除(R)	Imple(D):
	镜像     描述     源 DNS 名称     源地址     目标 DNS 名称            >
< 上一步( <u>B</u> ) 下一步( <u>N</u> ) > 取消	确定取消

IP 筛选器 属性 X
地址 协议 描述
源地址(S):
一个特定的 IP 地址或子网 v
IP 地址或子网([): 192.168.86.0/24
目标地址(D):
一个特定的 IP 地址或子网 🛛 🗸
IP 地址或子网(R): 10.0.0.0/8
_ 現像(0)。与源地址和日标地址上好相反的数据包相匹配。
确定取消

	安全规则向导	X
<b>IP 筛选器列表</b> 请为采用这个安全规则的	IP 流量类型选择 IP 筛选器列表。	
如果下面的列表没有符合	你需要的 IP 筛选器,请单击"添加"来创建新的。	
IP 筛选器列表(]):		
名称	描述	添加( <u>A</u> )
	网络A到网络B	
		编辑(E)
		删除(R)
	< 上一步(B) 下一步(N) >	取消

安全规则向导	×
常选器操作,请单击"添加"创建一个	新的。选择"使用
🗌 使用"添加向导	<b>寻</b> "( <u>₩</u> )
描述	添加( <u>A</u> )
	编辑( <u>E</u> )
	删除(R)
< 上一步(B) 下一步(	<u>N)</u> > 取消
	<mark>安全规则向导</mark>

		AB 属性		x	
安全方法	常规				
<ul> <li>许可(M</li> <li>阻止(L)</li> <li>動商安</li> <li>安全方法律</li> </ul>	)) 全(N): 育选顺序( <u>S</u> ):				
类型	AH 完整性	ESP 机密性	ESP 完整性	添加( <u>D</u> )	
加密并…	<无>	3DES	SHA1	编辑(E)	
				10/24 (D)	
				<u> </u>	
				上移(U)	
<	Ш		>	下移( <u>O</u> )	
□ 接受不安全的通讯,但始终用 IPsec 响应(C) □ 如果无法建立安全连接,则允许回退到不安全的通信(W) □ 使用会话密钥完全向前保密(PFS)(K)					
		确定	取消	应用(A)	



# B to A方向的安全规则

	VPN(网关A和网关E	B的IPSec) 属性	? X
规则 常规			
	的计算机通讯的安全规则		
IP 安全规则(]):			
IP 筛选器列表	筛选器操作	身份验证方法	隧道终结点
A to B	AB	预共享密钥	166.66.66.2
□ <动态>	默认响应(仅限于.	Kerberos	<无>
< 添加( <u>D</u> )	III 编辑(E)	削除( <u>R)</u> ▼使用	> *添加向导"( <u>W</u> )
		确定	取消

安全规则向导	x
<b>隧道终结点</b> 隧道终结点是最接近 IP 流量目标的隧道操作计算机,正如安全规则的 IP 筛选器列表所指 定的。	
IPsec 隧道允许数据包在两台计算机间以直接的专用连接的安全级别通过公用或专用网络。	
指定 IP 安全规则的隧道终结点:	
<ul> <li>● 隧道终结点由下列 IP 地址指定①:</li> <li>IPv4 隧道终结点:</li> </ul>	
55.55.503	
IPvo 隧道终结点:	
< 上一步(B) 下一步(N) > 取消	

安全规则向导	IP 筛选器列表
<b>网络类型</b> 安全规则必须应用到一种网络类型。	□ IP 筛选器列表由多个筛选器组成。这样 , 多个子网、IP 地址和协议可被整合到一个 IP □ 筛选器中。
选择网络类型: <ul> <li>所有网络连接(C)</li> <li>局域网(LAN)(L)</li> <li>远程访问(<u>R</u>)</li> </ul>	名称(N): B to A 描述(D): 「「」」」 「編損(E)… 」 一 一 一 一 一 一 一 一 一 一 一 一 一
< 上一步(B) 下一步(N) > 取消	镜像 描述     源 DNS 名称     源地址     目标 DNS 名称       <     Ⅲ     >       确定     取消

IP 筛选器 属性 ×
地址 协议 描述
·源地址( <u>S</u> ):
一个特定的 IP 地址或子网 V
IP 地址或子网([): 10.0.0/8
目标地址(D):
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □
IP 地址或子网(R): 192.168.86.0/24
□镜像(0)。与源地址和目标地址正好相反的数据包相匹配。
确定 取消

		IP 筛选器	翻表		х
	IP 筛选器列表由多 筛选器中。	3个筛选器组成。这样	, 多个子网、IP 地址	和协议可被整合到一个!	ĮΡ
名称( <u>N</u> ):					
B to A					
描述( <u>D</u> ):				添加( <u>A</u> )	
网络B到	网络A			^ 编辑(E)	
				→ 删除(R)	
IP 筛选器	≩( <u>S</u> ):			使用"添加向导"(W)	
镜像	描述	源 DNS 名称	源地址	目标 DNS 斜	名利
否	B to A	<一个特定的 IP	172.16.0.0/20	<一个特定的	\$ I
<	III				>
			确	定 取消	



	安全规则向导			X
<b>筛选器操作</b> 请为这个安全规则选择筛选器操作。				
如果下面的列表中没有符合你需要的 添加向导"来创建新筛选器操作。	筛选器操作,请单	击"添加"创建一个新	的。选择"使用	
筛选器操作(C):		🗌 使用"添加向导"	″( <u>W</u> )	
名称	描述		添加( <u>A</u> )	
O AB				
⊙ BA			编辑(E)	
			MIRA (D)	
			<u> </u>	
	< 上一	步(B) 下一步(N	)> 取消	



VPN(网关A和网关B的IPSec) 属性 ? ×					
规则常规					
	轨通讯的安全规则				
IP 安全规则(I):					
IP 筛选器列表	筛选器操作	身份验证方法	隧道终结点		
B to A	BA	预共享密钥	55.55.55.203		
A to B	AB	预共享密钥	166.66.66.2		
□ <动态>	默认响应(仅限于	Kerberos	<无>		
< 添加(D)	III 扁辑(E) 删除	±(R) ↓ 使用	> *·添加向导"(W)		
		确定	取消		



### 右击策略"VPN(网关A和网关B的IPSec)"并"分配"

4	2	本地安全策略			_ <b>D</b> X	
文件(F) 操作(A) 查看(V) 帮助(H)						
🗢 🄿 📶 🖬 🖬 👔	 					
🔒 安全设置	名称	描述		策略已指派	上次	大更
▷ 🔂 帐户策略	🛃 VPN(网关A和网关B的IPSec)	网关A(55.55.55.203)—	—网关B(166.66.66.213)VPN	是	202	21/
▷ 📴 本地策略						
▷ 🧰 高级安全 Windows 防火墙						
🧰 网络列表管理器策略						
▷ 🧰 公钥策略						
▷ 🧰 软件限制策略						
▷ 🧰 应用程序控制策略						
🜏 IP 安全策略 , 在 本地计算机						
▷ 🧰 高级审核策略配置						
	<	Ш				>
	-					

# 在"路由和远程访问"中配置VPN服务器网关

<b>b</b>		朋友	务器管理器		
<ul> <li>▶ 服务器管</li> <li>● ● ■ 服务器</li> <li>● 本地服务器</li> <li>● 所有服务器</li> <li>● IIS</li> <li>● IIS</li> <li>● 过程访问</li> </ul>	服务器管理器 器管理器 ・ 仪表板 交迎使用服务器管理器 ・ 使速启动(2) 2 添加角色和功能 3 添加要管理的其他服务器 新購助能(W) 4 创建服务器组			- 3	<ul> <li>□ ×</li> <li>管理(M) 工具(T) 视图(V) 帮助(H)</li> <li>Embedded Lockdown Manager</li> <li>Internet Information Services (IIS)管理器</li> <li>iSCSI 发起程序</li> <li>Microsoft Azure 服务</li> <li>ODBC 数据源(32 位)</li> <li>ODBC 数据源(64 位)</li> <li>Windows PowerShell</li> <li>Windows PowerShell ISE</li> <li>Windows PowerShell ISE (x86)</li> </ul>
	5 将此 了解详细信息(L) 角色和服务器组:1   服务器总数:1 で IIS 1 で 可管理性 事件 服务 性能 BPA 结果	<ul> <li>         ・</li></ul>	<ul> <li>☑ 远程访问 1</li> <li>① 可管理性 事件 服务 性能 BPA 结果</li> </ul>	<ul> <li>本地服务器</li> <li>① 可管理性 事件 服务 性能 BPA 结果</li> </ul>	安全配置向导 本地安全策略 服务 高级安全 Windows 防火墙 计算机管理 连接管理器管理工具包 路由和远程访问 任务计划程序 事件查看器 碎片整理和优化驱动器 网络策略服务器 系统配置 系统信息 性能监视器 远程访问管理
	C*Y				▲ 11 🕼 🖫 🗟 英 9:59 2021/10/14

			欢迎使用路由和远程访问服务器安装向导
<u>a</u>	路由和远程访问	×	ACT OF DEFENSIVE AND ADDRESS AND ADDRESS AND ADDRESS A
文件(F) 操作(A) 查看(V) 帮助	b(H)		
(= -) 💽 🚺			此向导帮助你设置服务器,使你可以连接到其他网络并允许来
直路由和远程访问	路由和远程访问		日远程各广ज的连接。
<ul> <li>■ 服务器状态</li> <li>▶ ● SERVERB2012STD (本地)</li> </ul>	欢迎使用路由和远程访问	^	单击"下一步"继续。
	路田和远程访问提供到专用网络的安全远程访问。 使用路由和远程访问配置下列内容:		
	•两个专用网络之间的安全连接。 • 虚拟专用网络(VPN)网关。		
	• 拨号远程访问服务器。		
	・ 网络地址转换(NAT)。 ・ LAN 路由。		
	•基本防火墙。		
	若要添加路由和远程访问服务器,请在"操作"菜单上,单击"添加服务 器"。	;	
		~	
完成			
			< 上一步( <u>B</u> ) ト <b>一步(<u>N</u>) &gt; 取消</b>

路由和远程访问服务器安装向导

#### 路由和远程访问服务器安装向导

<b>配置</b> 你可以启用下列服务的任意组合,或者你可以自定义此服务器。	<b>请求拨号连接</b> 请求拨号连接允许你路由数据到远程网络。
<ul> <li>远程访问(拨号或 VPN)(R) 允许远程客户端通过拨号或安全的虚拟专用网络(VPN) Internet 连接来连接到此服务器。</li> <li>网络地址转换(NAT)(E) 允许内部客户端使用一个公共 IP 地址连接到 Internet。</li> <li>虚拟专用网络(VPN)访问和 NAT(V) 允许远程客户端通过 Internet 连接到此服务器,本地客户端使用一个单一的公共 IP 地址连接到 Internet。</li> <li>两个专用网络之间的安全连接(S) 将此网络连接到一个远程网络,例如一个分支机构。</li> <li>自定义配置(C) 选择在路由和远程访问中的任何可用功能的组合。</li> </ul>	你想使用请求拨号连接访问远程网络吗? ① 是(Y) ④ (A) 完成此向导后,你可以设置请求拨号连接。
< 上一步(B) 下一步(N) > 取消	< 上一步( <u>B</u> ) 下一步( <u>N</u> ) > 取消

路由和远程访问服务器安装向导

路由和远程访问服务器安装向导				
	正在完成路由和远程访问服务器安装向导			
	你已经成功地将此服务器设置为路由器。 摘要: 在此网络和一个专用网络之间创建安全连接。			
	若要关闭此向导,请单击"完成"。 在使用此路由器前: h 确认所有接口都有地址 h 在每一接口安装和设置路由协议			
	< 上一步(B) 完成 取消			

正在启动 远程访问管理				
	摘要: 在此网络和一个专用网络之间创建安全连接。			
	, 若要关闭此向导 , 请单击"完成"。			

<u>ē</u>	路由和远程访问	x
文件(E) 操作(A) 查看(V) 帮助(H)		
🗢 🔿 📶 🗙 🗐 🙆 🔢		
<ul> <li>● 路由和远程访问</li> <li>● 服务器状态</li> <li>▲ ● SERVERB2012STD (本地)</li> <li>● 奧 网络接口</li> <li>● 遵 端口</li> <li>● 通 正程访问日志记录和策略</li> <li>● ⑨ IPv4</li> <li>▲ ⑨ IPv6</li> <li>● ⑨ 帮规</li> <li>● 静态路由</li> </ul>	SERVERB2012STD (本地) 此服务器上配置了路由和远程访问 已经使用"路由和远程访问服务器安装向导"对此服务器进行了配置。若要对当前配置进行更改,请在控制台树中选择一个项目,然后。 "操作"菜单上的"属性"。 在此服务器上启用 DirectAccess 你当前仅使用 VPN 为客户满提供远程访问,你可以通过在此服务器上启用 DirectAccess 来使用基于 DirectAccess 的丰富远程访问 验、使用 DirectAccess,已加入域的客户满可以无缝地连接到企业网络。若要在此服务器上启用 DirectAccess,你可以通过选择在 操作窗格上的"启用 DirectAccess"选项或者右键单击左侧的计算机节点来运行"启用 DirectAccess"向导。	单击 体则的
 完成		

2个局域网之间的安全通信(IPSec VPN)

🙍 Capturing from VMInet5 [Tireshark	1.10.6 (v1.10.6 from mast	ter-1.10)]		_ 8 ×
File Edit View Go Capture Analyze Sta	atistics Telephon <u>y T</u> ools <u>I</u> nt	ternals <u>H</u> elp		
● ● ◢ ■ ◢   ⊨ ≞ ≭ ≈	○、 수 ⇒  주		♀, @, ??   ₩ ⊠ 畅 ※   第	
Filter:	7	Expression Cle	Ilear Apply Save	
No. Time Source	Destination	Protocol Length Info	nfo EDF (SPI=0X0I04J904)	<u> </u>
793 852.643701 166.66.66.213	55.55.55.203	ESP 126 ESI	ESP (SPI=0xd5726b77)	
794 852.832258 55.55.55.203	166.66.66.213	ESP 110 ESI	ESP (SPI=0x61045904)	
795 853.645450166.66.66.213	55.55.55.203	ESP 126 ESI	ESP (SPI=0xd5726b77)	
796 853.834954 55.55.55.203	166.66.66.213	ESP 110 ES	ESP (SPI=0x61045904)	
797 854.646903 166.66.66.213	55.55.55.203	ESP 126 ESI	ESP (SPI=0xd5726b77)	
798 854.835049 55.55.55.203	166.66.66.213	ESP 110 ESI	ESP (SPI=0x61045904)	
799 855.659173 166.66.66.213	55.55.55.203	ESP 126 ESI	ESP (SPI=0xd5726b77)	
800 855.836680 55.55.55.203	166.66.66.213	ESP 110 ESI	ESP (SPI=0x61045904)	
801 856.659932 166.66.66.213	55.55.55.203	ESP 126 ESI	SSP (SPI=0xd3/26D/)	
802 856.838920 55.55.55.203	100.00.00.213	ESP IIUESI	SP (SPI=UX6L045904)	
803 807.002130100.00.00.213	166 66 66 717	ESP 120 ESI	->P (>F1=UXU)/20U//)	
804 8J7.839037 JJ.JJ.JJ.203	100.00.00.213		->> (>1=0xdL94)904) 	
805 858 842568 55 55 55 203	166 66 66 713		<pre>csp (sp1=0x610x500/) csp (sp1=0x610x500/)</pre>	
807 859 664561 166 66 66 713	55 55 55 203		ESP (SPT=0xd5750b7)	
808 859 843494 55 55 55 203	166-66-66-213	ESP 110 ESI		
809 860, 664872 166, 66, 66, 213	55.55.55.203	ESP 126 ESI	SPI=0xd5726b77)	
810 860.854952 55.55.55.203	166.66.66.213	ESP 110 ESI	== (SPI=0x61045904)	-
$\square$ Frame 70: 126 bits on wine (10)	9 bits) 136 but as car	sturad (1008 bits	its) on interface 0	
Ethernet II Src: CadmusCo d8:22	7·1= (08·00·27·d8·27·1=	a) Dst. CadmusCo	TC 2011 TT 27 (08:00:77:20:01:37)	
Internet Protocol Version 4. Sr	-: 55,55,55,203 (55,55,	.55.203). Dst: 10	166.66.213 (166.66.66.213)	
Encapsulating Security Payload				
E Encapsulating Secarrey rayload				
0000 08 00 27 aa c1 37 08 00 27	d8 27 1e 08 00 45 00		E.	<b>A</b>
10010 00 70 60 00 00 00 71 32 76	42 37 37 37 CD a6 42 01 2d 93 8c 87 76 p3	.pm2 vB777.	//B	
0030 39 40 fc d0 f1 bb ad 0a 87	c7 Oc 6a 9b 11 9d 5d	90i.		
0040 7b 0e d7 32 6a 05 da 18 48	7a Od c2 5e 5a 33 eb	{2j Hz^z	AZ3	-
	ND 02 66 24 90 59 45	10 (100 0%)	F Profile: Default	
<ul> <li>Filmeros, kine cabrare in progress / ne. c</li> </ul>	Helli ackers, ere pisblaken, e	10 (100.070)	Profile, Defaut	

