

How to configure Quadro IPSec with MS IPSec



Abstract: This document describes the configuration settings for Quadro while creating VPN between Quadro and MS Windows 2000.

Table of Contents:

1	Intro	oduction	3
2	How	to configure	3
	2.1	Quadro IPSec ←→ MS IPSec	. 3
	2.2	The Windows 2000 IPSec setup	.6
3	Usef	ul Links2	7

1 Introduction

This document describes the configuration settings for Quadro while creating VPN between Quadro and MS Windows 2000.

2 How to configure

2.1 Quadro IPSec ←→ MS IPSec

To configure IPSec on Quadro the follow the steps below:

- **1.** Go to **Internet Uplink**→**VPN Configuration**→**IPSec Configuration** page.
- 2. Add a new connection.
- **3.** Fill in the connection name and select **Windows 2000/XP** from the Peer type drop-down list and go to the next page of the wizard.

Main System Users	Telephony Internet Uplink LAN Services		ygi 1adro225
IPSec Conn	ection Wizard		
Connection Name: Peer type: VPN Network Topology:	Quadro_MSWin2k Windows 2000/XP 💌 Quadro<->Peer		
Previous	Next	Cancel Help	

4. The basic parameters are already set on this page. Enter the peer's IP in the **Remote Gateway** IP Address field. MS peer should use 3DES/MD5 Keying type.

Main System Users Telephony Internet Uplink LAN Services		ygi dro225
IPSec Connection Wizard		
IPSec Connection Properties - Quadro_MSWin2k		
 Dynamic IP / Roadwarrior Static IP / Remote Gateway Remote Gateway Quadro <> Remote Gateway Local Subnet <> Remote Gateway Quadro <> Remote Subnet Local Subnet <> Remote Subnet 	 ♦ Auto Keying Internet Key Exchange (IKE) Encryption Triple DES Authentication MD5 Diffie-Hellman Group 2 (1024 bit) Encapsulated Security Payload (ESP) Encryption Triple DES Authentication MD5 	
Remote Subnet IP 192 168 1 0 / 24 IP-Clipboard Local Subnet IP 172 168 2 0 / 24 IP-Clipboard	Manual Keying Encryption Single DES Authentication MD5	
Previous Next	Cancel Help	

Figure 2

 The same shared secret key must be used on both Quadro and MS peer sides. Also MS peer should have the same state of PFS (Perfect Forward Secrecy) as Quadro.

Nain System Users	Telephony Internet Uplink LAN Services	1	Cepygi TQuadro225
PSec Conr	nection Wizard		
Automatic ke	eying - Quadro_MSWin2k		
 Shared Secret 	This is my preshared ke		
O RSA	Remote RSA public key		
Local ID 172.35. Remote ID 207.151	.222.2 ard Secrecy)		
Previou	Finish	Cancel	Help

- 6. Press Finish and Start connection.
- 7. Configure **MS peer** and enjoy connection.

2.2 The Windows 2000 IPSec setup

1. Run MMC from **Start** –>**Run** window.





Console1			
	21 xi		
Action Yiew Action View Use this page to add or remove a standalone S	nap-in from the console.		
Console Root Snap-ins added to: Snap-ins added to:	Add Standalone Snap-in		? ×
	Available Standalone Snap-ins:		
	Snap-in	Vendor	-
	FrontPage Server Extensions Group Policy Indexing Service Internet Information Services FSecurity Policy Management Link to Web Address Cocal Users and Groups Performance Logs and Alerts Resource Storage Management	Microsoft Corporation Microsoft Corporation, I Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	
Description	Security Configuration and Analysis	Mignaround Systems, Inc. Microsoft Corporation	-
Add Remove About.	Description Internet Protocol Security (IPSec) Admir policies for secure communication with	nistration. Manage IPSec other computers.	

2. Go to Console -> Add/Remove Snap-in. Add IP Security Policy Management.

Figure 5

3. Choose Local Computer and press Finish.

ect Computer		3
Select which computer this Sna When this console is saved the lo	p-in will manage cation will also be saved	
C Local computer		
The computer this console is runnin	g on	
Manage domain policy for this com	puter's domain	
C Manage domain policy for another	domain:	
C Another computer:		
	Browse	
	< Back Finish	Cancel

Action View Eavorites 📙 🖨 🔿 🖡	i 🖬 🚯 😫 🞽 🗄	2	
Create IP Security Policy Manage IP filter lists and filter actions All Tasks New Window from Here New Taskpad View Refresh Export List Help	ame ∇ Server (Request Security) Secure Server (Require Security) Client (Respond Only)	Description For all IP traffic, always request For all IP traffic, always require s Communicate normally (unsecure	Policy Assigne No No
uste an IR Security Policy	1	J	ľ

4. Create a new IPSec Security Policy.

Figure 7

5. Press Next.



6. Enter a name for the new policy.

IP Security Policy Wizard	? ×
IP Security Policy Name Name this security policy and optionally give it a brief description	
Name:	
Site1-to-site2	
Description:	
IPsec tunnel from site1 to site2	*
	*
< Back Next >	Cancel

F	ia	ur	е	9
	чy	u	c	

7. Deactivate the default response rule and press **Next**.

ecurity Policy Wizard	
Requests for Secure Communica Specify how this policy responds t	ation to requests for secure communication.
The default response rule respond other rule applies. To communicate secure communication.	is to remote computers that request security, when no e securely, the computer must respond to requests for
Activate the default response i	rule.

8. Click Finish.



Figure 11

9. Create the first IP filter for the traffic from the left subnet to the right subnet. Uncheck **Use Add Wizard** checkbox.

ules General			
Security Bules:	ules for communicating with	other computers	
IP Filter List	Filter Action	Authentication	. Tı
🗌 <dynamic></dynamic>	Default Response	Kerberos	No
۹			<u>)</u>
	Edit Remove	Use Add \	Vizaro

Figure 12

10. Press Add.

Rule Properties	?
Authentication Methods IP Filter List	Tunnel Setting Connection Type Filter Action Iter list specifies which network traffic will be rule.
P Filter Lists:	Description
O All ICMP Traffic O All IP Traffic	Matches all ICMP packets betw Matches all IP packets from this
Add Edit	Remove
	Close Cancel Apply

Figure 13

11. Enter a name, description and add the filter.

Name: left-to-righ	ŧ			
Description	n:			Add
Traffic goi	ing from the leftsub	net to the rightsubnet	<u> </u>	Edit
			-	Remove
Filters:				Use Add Wizard
Mirrored	Description	Protocol	Source Port	Destination



12. Enter the left subnet as the source address and the right subnet as the destination address.

IP Address:	192	04	168		1	-	0
Subnet mask:	255		255	ile:	255	25	0
A specific IP Subnet		_		_	2	-	
	109		100	_	-	<u></u>	0
Subnet mask:	255	31 32	255		255	•8	0
Mirrored. Also match pack destination addresses.	cets with I	the	exact o	pp	osite sc	ource	e and

Figure 15

13. Close that filter's properties box.

left-to-right			_
) Description:			Add
Traffic going from the	e leftsubnet to the right:	subnet	Edit
			Remove
Filters:			Use Add Wizar
Source Address	Source Mask	Destination Address	Destination Mask
192.168.1.0	255.255.255.0	192.168.2.0	255.255.255.0



14. Assign the newly created filter to the current rule.

Rule Properties	?		
Authentication Methods	Tunnel Setting Connection Type Filter Action		
The selected IP filter secured with this rule	list specifies which network traffic will be a.		
P Filter Lists:	Description		
All ICMP Traffic	Matches all ICMP packets betw		
O Airle Hanic O left-to-right ↓	Traffic going from the leftsubnet		
Add Edit	Remove		

Figure 17

15. Set the filter action to the **Require Security** action.

Authentication Methods Tunnel Setting Connection Type IP Filter List Filter Action IP Filter List Filter Action Image: The selected filter action specifies whether this rule negotia for secure network traffic, and how it will secure the traffic. Iter Actions: Name Description Image: Permit Security (Optional) Request Security Image: Provide Security				
IP Filter List Filter Action The selected filter action specifies whether this rule negotia for secure network traffic, and how it will secure the traffic. Iter Actions: Name Description Permit Permit Unsecured IP packets to Request Security (Optional) Accepts unsecured communicat Require Security Accepts unsecured communicat	Authentication Methods T	unnel Setting Connection Typ		
The selected filter action specifies whether this rule negotia for secure network traffic, and how it will secure the traffic. Iter Actions: Name Description Permit Permit Unsecured IP packets to Request Security (Optional) Accepts unsecured communicat Require Security Accepts unsecured communicat	IP Filter List	Filler Action		
Iter Actions: Name Description O Permit Permit unsecured IP packets to O Request Security (Optional) Accepts unsecured communicat O Require Security Accepts unsecured communicat	The selected filter act	ion specifies whether this rule negotia (fic. and how it will secure the traffic.		
Iter Actions: Name Description Permit Permit unsecured IP packets to Request Security (Optional) Accepts unsecured communicat Require Security Accepts unsecured communicat				
Name Description O Permit Permit unsecured IP packets to O Request Security (Optional) Accepts unsecured communicat O Require Security Accepts unsecured communicat	ilter Actions:			
Permit Permit unsecured IP packets to Request Security (Optional) Accepts unsecured communicat Require Security Accepts unsecured communicat	Name	Description		
Request Security (Optional) Accepts unsecured communicat Require Security Accepts unsecured communicat	O Permit	Permit unsecured IP packets to Accepts unsecured communicat		
Require Security Accepts unsecured communicat	O Request Security (Optional)			
	Require Security	 Accepts unsecured communicat 		
Add Edit Remove 🔽 Use Add Wiza	Add	Remove Use Add Wiza		



 Set these action properties and move the proposal 3DES-MD5 to the top of the list. Select Session Key Perfect Forward Secrecy checkbox.

Perm Block Nego	it < bliate security:			
Type	Method prefer AH Integrity	rence order: ESP Confidenti	ESP Integri	Add
Custom Custom	<none> <none></none></none>	3DES 3DES	MD5 SHA1	Edit
Custom Custom	<none> <none></none></none>	DES SHA1 DES MD5	SHA1 MD5	Remove
				Move up
•			Þ	Move down
Z Acce ⊂ Allow Z Sess	pt unsecured unsecured c ion key Perfec	communication, bu ommunication with st Forward Secrecy	it always respond non IPSec-aware	l using IPSec e computer

Figure 19

17. Set the connection type for LAN.

w Rule Properties		?
IP Filter List	1	Filter Action
Authentication Methods	Tunnel Setting	Connection Type
This rule only app the selected type	olies to network traff	ic over connections of
C All network connections		
Cocal area network (LAN)		
	Close	Cancel Apply



18. Specify the right gateway IP address.



Figure 21

19. Modify the authentication method.

11.11.115	er List		-ilter Action
Authentication M	1ethods Tunn	el Setting	Connection Type
The bety auti ano	authentication metho veen the computers. C ientication methods w ther computer.	d specifies ho)ffer and accr hen negotiatir	w trust is established ept these ng security with
uthentication M	ethod preference orde	r:	
Method	Details		Add
Kerberos			Edit
			Remove
			Move up
			Move down



20. Set it to pre-shared key and enter it there.

lit Authent	ication Method Properties	?
Authenticati	ion Method	
	The authentication method specifies how trust is establi between the computers.	shed
C Windo	ws 2000 default (Kerberos V5 protocol)	
C Use a	certificate from this certificate authority (CA):	
	Brows	se
G Lloo Ho	is string to protect the barrough upon (proclement barr).	
se Ose u	is saing to protect the key exchange (preshared key).	
This	is my preshared key !!!	<u>_</u>
		-
		10000
	OK Cancel A	Apply

Figure 23

21. Close the first rule's properties box.

Authenticat					T INCOLO	Cuon.
	ion Methods	1	Tunnel S	etting] Co	nnection Type
aa	The authentic between the c authentication another compl	ation ompu meth uter.	method sp iters. Offer iods when	ecifies h and aco negotia	now trus cept the ting sec	t is established se urity with
uthenticatio	n Method prefe	erence	e order:			
Method	Deta	is			_	Add
Freshared N	ley This	s my	presnareo	K		E dit
						Remove
						Move up
						Move dowr



22. Create a second rule for the traffic from the right subnet to the left subnet.

les General	rity rules for commun	icating with other c	omputers
Security Rule:	5.		
IP Filter List	Filter Action	Authentication	Tunnel Setting
✓ Tett-to-right	Require Security Default Respon	Préshared Key Kerberos	172.35.55.8 None
1		- T	<u>)</u>
Add	Edit	Remove	Use Add Wiza

Figure 25

23. Create a new filter for that rule.





24. Enter a name, description and add the filter.

An add Name: right-to-left	IP filter list is cor dresses and prot	mposed of multiple filter ocols can be combiner	rs. In this way multiple sub d into one IP filter.	inets, IP
Name: right-to-left				
right-to-left				
1				
Description:				Add
Traffic from t	he rightsubnet to	o the leftsubnet	*	Edit
			*	Remove
Filters:				Use Add Wizard
Mirrored D	escription)	Protocol	Source Port	Destination
•				Fancel

Figure 27

25. Enter the right subnet as the source address and the left subnet as the destination address.

A specific IP Subnet	ě.				1		
IP Address:	192		168	Mili	2	35	0
Subnet mask:	255	33	255	93-33	255	23	0
estination address:							
A specific IP Subnet					-	-	
IP Address:	192	-	168		1	15	0
Subnet mask:	255	3.	255	0.0	255	-8	0
Mirrored. Also match pack destination addresses.	kets with	the	exact (qq	osite sc	ource	e and



26. Close the IP filter's properties box.

composed of multi protocols can be c	iple filters. In this way multi ombined into one IP filter.	iple subnets, IP
		Add
et to the leftsubnet		Edit
		Remove
		🔲 Use Add Wizard
ource Mask	Destination Address	Destination Mask
55.255.255.0	192.168.1.0	255.255.255.0
	et to the leftsubnet ource Mask 55.255.255.0	ource Mask Destination Address 55.255.255.0 192.168.1.0

Figure 29

27. Assign the newly created filter to that rule.

Rule Properties	1	
Authentication Methods	Tunnel Setting Connection Type	
The selected IP fil secured with this r	ter list specifies which network traffic will be ule.	
P Filter Lists:	Description	
O All ICMP Traffic	Matches all ICMP packets betw	
O All IP Traffic	Matches all IP packets from this	
O left-to-right	Traffic going from the leftsubnet	
La Ingilia Collection	Traine nom the lightsubnet to th	
Add Edit	Remove	
	Close Cancel Apply	

- **New Rule Properties** ? × Connection Type Authentication Methods Tunnel Setting Filter Action **IP Filter List** $\boldsymbol{\times}$ The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic. Filter Actions: Name Description O Permit Permit unsecured IP packets to ... O Request Security (Optional) Accepts unsecured communicat... O Require Security ■ Accepts unsecured communicat... 2 Add. Edit... Remove ☑ Use Add Wizard Close Cancel Apply
- 28. Select the Require Security radio button (no need to edit it again).

Figure 31

29. Set the connection's type to LAN.

	1	
IP Filter List		Filter Action
Authentication Methods	Tunnel Setting	Connection Type
This rule only app the selected type	ilies to network traffi	c over connections of
C All network connections		
• Local area network (LAN)		
C Remote access	\mathbf{k}	

Figure 32

30. Enter the left gateway (your side) as the tunnel endpoint.



Figure 33

31. Modify the authentication method.

IP Filter List	Filte	er Action
Authentication Methods	Tunnel Setting	Connection Type
The authenti between the authenticatic another com	cation method specifies how computers. Offer and accept in methods when negotiating puter.	trust is established these security with
Authentication Method pre	ference order:	
Method	Details	Add
Kerberos		Edit
		Remove
		Move up
		Move down



32. Enter your pre-shared key again.

lit Authentication Method Properties	?
Authentication Method	
The authentication method specifies how trust is established between the computers.	ablished
C Windows 2000 default (Kerberos V5 protocol)	
${\ensuremath{\mathbb C}}$ Use a certificate from this certificate authority (CA):	
Bro	wse
Itse this string to protect the key exchange (preshared key)	
This is real product the Key exchange (presided Key).	
I his is hig preshared key m	
	~
	Applu
	Abbia

Figure 35

33. Close that rule's properties box.

	ilter List		Filter A	liction
Authentication	n Methods	Tunnel Setting) C	onnection Type
Ti be au ar	he authentication stween the comp uthentication me hother computer.	n method specifies outers: Offer and a hods when negot	how trus ccept the iating sec	st is established ese curity with
uthentication I	Method preferen	ce order:		
Method	Details			Add
riesnaleurkey	r nis is niy	oreshared key in		E dit
				Remove
				Move up
				Move down

34. Select the 2 rules to apply on that policy.

P Security Hules	: Filter Action	Authentication	Tunnel Setting
✓ right-to-left ✓ left-to-right ✓ </td <td>Require Security Require Security Default Respon</td> <td>Preshared Key Preshared Key Kerberos</td> <td>207.151.222.2 172.35.55.8 None</td>	Require Security Require Security Default Respon	Preshared Key Preshared Key Kerberos	207.151.222.2 172.35.55.8 None
		R	
•			

Figure 37

35. On the general tab, press the **Advanced** button.

Site1-to-site2 Properties	? ×
Rules General	1
IP security policy general properties	
Name:	
Site1-to-site2	
Description:	
IPsec tunnel from site1 to site2	×
Check for policy changes every:	
180 minute(s)	
Key Exchange using these settings: Advanced	
Close	Cancel

Figure 38

36. Select **Master Key Perfect Forward Secrecy** checkbox and press the **Methods** button.

uthentica	te and generate a new key after every:
480	minutes
uthentica	te and generate a new key after every;
1	session(s)
Protect ide Methods	ntities with these security methods:
nternet Ke Jointly deve	y Exchange (IKE) for Windows 2000 sloped by Microsoft and Cisco Systems, Inc.

Figure 39

37. Move the proposal 3DES-MD5 to the top of the list and close that policy.

ecurity	Method prefe	rence order	r.	()
Type	Encryption	Integrity	Diffie-Hellman	Add
ike Ike Ike	3DES 3DES DES DES	SHA1 SHA1 MD5	Medium (2) Low (1) Low (1)	Edit Remove
				Move up
				Move down

🚡 IPSEC - [Console Root\IP Security P	olicies on Local Ma	ichine]		_ 🗆 🗙
Console MindowHelp			🗅 😅 🖬 [I _B×
🗍 Action View Eavorites 🗍 🖨 🔿	🗈 📧 🗙 😭	B 😫 🗎	1 📩 🗍 🖹 🧕	
Tree Favorites	Name V		Description	Policy Assigned
Console Root	Site1-to-site2 Server (Reque Secure Server Client (Respor	Assign All Tasks Delete Rename Properties Help	Psec tunnel from site1 to site2 for all IP traffic, always request for all IP traffic, always require s Communicate normally (unsecure	No No No
Assign this policy, attempt to make it active				

38. Select **Assign** for that policy to make it active.

Figure 41

39. Test it. Wait and ping it again. Then check the events log because it never works the first time.



40. You'll have to modify your policy to correct what's wrong. Restart the **Ipsec** service before testing it again.

Norvices					L. C.	- 🗆 ×
Action View	← → 🛍 💽 🚰 [🗿 🖪 😫	▶ ■			_
Tree	Name /	Description	Status	Star Pectart S	g On As	
Services (Local)	🙀 File Replication	Maintains fi		Manual	LocalSystem	
	Notexing Service			Manual	LocalSystem	
	Sinternet Connectio	Provides n		Manual	LocalSystem	
	Salar Stress Antipage 1	Allows sen		Disabled	LocalSystem	
	PSEC Policy Agent	Manages I	Started	Automatic	LocalSystem	
	Kerberos Key Distri	ey Distri Generates Disabled	LocalSystem	1		
	License Logging Ser		Started	Automatic	LocalSystem	
	🖏 Logical Disk Manager	Logical Disk	Started	Automatic	LocalSystem	
	🖓 Logical Disk Manage	age Administrat Manual Loca	LocalSystem			
	Messenger	Sends and	Started	Automatic	LocalSystem	-

Figure 43

41. When it works you can monitor the tunnel with the **ipsecmon** program.

Policy Name	Security		Filter Name	Options
{23CCFE7A-4E10-4343-879D-6026D723380	D} ESP Triple	DES HMAC MD5	No Name	<u>M</u> inimize
IPSEC Statistics Active Associations	1	ISAKMP/Oakley Statisti Oakley Main Modes	DS	<u>۲</u>
Confidential Bytes Sent	780	Oakley Quick Modes		1
Confidential Bytes Received	960	Soft Associations		0
Authenticated Bytes Sent	1,040	Authentication Failures		0
Authenticated Bytes Received Bad SPI Packets	960 0		 N	
			N	
Packets Not Decrypted	0			
Packets Not Decrypted Packets Not Authenticated	0 0			

3 Useful Links

- The Quadro home site! <u>http://www.epygi.com</u>
- The Windows 2000 IPSec setup! http://jixen.tripod.com/win2k-screen.html
- Windows 2000 PPTP-client configuration! <u>http://poptop.sourceforge.net/dox/pptp_win2k/</u>