iStorage Server and IP SEC

Friday, May 28, 2010

KernSafe Technologies, Inc.

www.kernsafe.com

Copyright © KernSafe Technologies 2006-2009. All right reserved.

Table of Contents

1. iSCSI	Target Setting	3
A)	Create Target	3
B)	iSCSI Target Setting	7
2. Serve	er Side Local Security Policy Setting	13
3. Client	t Side Local Security Policy Setting	30
4. Loggi	ing on to the target	47
5. Effect	t	52

KernSafe iStorage Server is an advanced and powerful, full-featured software-only iSCSI Target that fully conforms to the latest iSCSI Standard 1.0 (former Draft 20). It is an IP SAN solution allowing you to quickly export existing storages such as disk images, VHD files, physical disks, partitions, CD/DVD-ROMs, tapes or any other type of SCSI based devices and even a variety of popular CD/DVD images to the client machines. The software thus delivers immediate benefits, as it allows storage to be consolidated, virtualized and centrally managed. iStorage Server also provides RAID-1 (mirror) feature enabling you to create two iSCSI devices for mirror backup. Furthermore, iStorage Server also supports a lot of features such as: VHD (Virtual Hard Disk) target, snapshots, STPI, RAID-1 and failover, these features are very important and poplar in storage industry world and make iStorage Server is suitable for any size of business.

After iStorage Server 2.0, it supports server side mirroring, synchronous replication and failover which allows user to create a high-availability iSCSI SAN.

Internet Protocol Security (IPSec) is an architecture defined by the Internet Engineering Task Force (IETF) RFC 2401. This architecture involves several protocols that perform various functions in the architecture.

A network is not secure until servers can identify the computers communicating with them. IPSec enables secure, trusted communications between IP addresses. The system behind the IP address has an identity that is verified by using an authentication process. The only computers that must be aware of IPSec are the sending and receiving computers. Each computer handles security at its respective end, and assumes that the medium over which the communication takes place is not secure. Any computers that route data between the source and destination computer are not required supporting IPSec.

This article demonstrates how to make a Security iSCSI Target under the Windows IP Security Policies (IP Sec) environment by using KernSafe iStorage Server. Take Windows Server 2003 as an example, It is also similar to Windows 2000, Windows XP, Windows Vista and Windows Server 2008. At the same time, this article demonstrates how to use the two method of security policy in the iStorage Server, CHAP and IP Address authentication mechanism and how to configurate Local Security Policy in the both client and server side.

1. iSCSI Target Setting

- A) Create Target
- Launch KernSafe iStorage Server Management Console, Select Storage -> Create Target menu item, the Create Target wizard is shown.



Choose Hard Disk.

Press the **Next** button to continue.

Create iSCSI Target Wizard	×
iSCSI Medium Type Select medium of the iSCSI disk you want to create.	
 Image File Create iSCSI disk by using standard image file or Virtual Hard Disk (.VHD). RAM Space Create iSCSI disk by using memory space. 	
 Security Images Create iSCSI disk images for each initiators, any image is individual for each initiator. Disk Partition Create iSCSI target by using a disk partition 	
Physical Disk Create iSCSI target by using physical disk.	
< Back Next > Car	ncel

Choose Image File in iSCSI Medium Type window.

Then press **Next** button to continue.



We choose Standard Image File and then press Next button.

Set image disk parameters

Create iSCSI Target Wizard	x
Image Disk Configuration You can specify a image file as an iSCSI device.	
Device Parameters	
 Use existing image file Oreate a new image file 	
E:\newimage.img Browse	
Device Size in MBs: 1024	
Options	
Use sparse file on NTFS file system	
Note: Using sparse file can save your harddisk space, the size of disk image file only depend on its content used. But we recommentd that using this feature when image file size is less than 1T bytes	
< Back Next >	Cancel

Select Create a new image file or Use existing image file if you already have a one.

Specify the device size.

Press the **Next** button to continue.

Set Authorization Mode.

Create iSCSI Target Wizard	×
Authorization You can select an authorization mode, Anonymouns, CHAP or IP filter.	<u> </u>
 Anonymous Select this option to disable any authorization. CHAP Select this option to use CHAP authorization. 	
 IP Filter Select this option to use IP address authorization. Mixed Select this option to use both CHAP and IP address authorization. Inherit security roles from global settings. 	
< Back Next > Car	ncel

Choose authorization mode as you required.

Press the **Next** button to continue.

Finish iSCSI Target Creating.

Create iSCSI Target Wizard	×
Completing the Create iSCSI Wizard You can specify a target name and other options to complete iSCSI target creating.	
Basic Target Information	
Enter Target Name: iqn.2006-03.com.kemsafe.kemsafe.test.lmageDisk0	
 Report as readonly device when initiator can not get write access Enable multiple initiators with full access connected (sharing and clustering) 	
Note	
By default, only one client has full access right, when the second initiaor log on with full access, it will fail. But this option is usfull for clustering, disk sharing and NAS.	
< Back Finish C	ancel

Type the target name or use the default name.

Press the **Finish** button to continue.

B) iSCSI Target Setting

This chapter is not necessary for every users of iStorage Server.

Back to iStorage Server Management Console.

iStorage Server Management Consol	e					x
<u>S</u> torage <u>C</u> lients <u>V</u> iew <u>T</u> ools <u>I</u>	<u>H</u> elp					
Create Delete Start	Stop Refresh Add	Remove View	Access	کې Settings	Print	1 About
	iStorage Server: kerns	afe-PC				
Ign. 2006-03. com. kernsate. k	General Targets Applications IP Fil	ters Users Groups Logs				
IPFilters	Target Name	Devic Source	Capa	Authentic	Status	
	👒 iqn.2006-03.com.kernsafe.kern	Disk E:\newimage.img	1.00G	Anonymo	Ena	
Logs						
۰ III • •						
Done	- p	8	Connected:	kernsafe-PC (U	Iltimate Lio	ense)

B1. Modify iSCSI Target authorization method. User may modify iSCSI Target settings by through this method. Right click on the Target node, and then select the **Properties** menu item, the **Target Settings** dialog is shown.

Target Settings	
General Device Settings Security Portal Ca	ache Virtual Write
Target Name: ign.2006-03.com.kemsafe.ken Capacity: 1.00G	nsafe-test.lmageDisk0
Device Interface: DiskDrive	
Media Type: Standard Disk Image	
To rename the target name: click Change.	Change
To expand the capacity of this target: click Expan	nd. Expand
To commit changes of this target: click Commit.	Commit
	OK Cancel Apply

In **General** page, you can change the target name and expand the capacity of the target when it is a standard image file. The **commit** button is only available for RAM target.



In the **Device Settings** Page, if you check **"Report as readonly device when initiator can not get write access"**, the system will give you a report when you load the target without write access.

When your storage server is running in the environment of cluster, the function of concurrent writing of multi-users is needed and the writing synchronization control is realized by cluster software. Thus, you need to check **"Enable multiple initiators with full access connected"**



In the **Security** page, you can change the target's authorization mechanism.

arget Settings					×
General Devic	e Settings Se	curity Portal	Cache Virtual	Write	
🔽 Inherit from	global settings				
Target portal	address list				
Portal:	0.	0.0	. 0	Add	Delete
IP Address			Туре		Up
62 192.168	8.0.195		Built In		Тор
192.168	3.254.1 3.142.1		Built In Built In		Down
					Down
					Bottom
Note, if need router IP add	to make iStora ress to the list.	ge Server work	ing behind the fire	wall, pleas	e add the
				C	
			OK	Cancel	Apply

In the Portal page, when you check **"Inherit from global settings"** the settings will follow the **"Settings"** in tool bar, otherwise, you can have your own portal address for this target.

Target Settings		x					
General Device Settings Se	curity Portal Cache Virtual Write						
Enable cache on this target							
Cache Parameters							
Cache size in MBs:	64						
Cache refresh interval ms:	3000						
Cache Granularity:	4K •						
	OK Cancel App	ily					

If you want to speed up the read and wire rate, check **Enable cache on this target** in the **Cache** page.

Target Settings
General Device Settings Security Portal Cache Virtual Write
Enable Virtual Write
Work folder for clients write data:
Browse
Data Quota for Virtual Write in MBytes (zero indicate no limitation):
Mode
Ø Volatile
Target will reset all changes after initiators log out.
Persistent
Target will preserve all changes for each initiators with Virtual Write access mode.
OK Cancel Apply

If you want your target has the COW protection, check the **"Enable Virtual Write"** in the **Virtual Write** page.

Once user selected IP filter authorization, he can manage this target's access right by IP filter. Click the View->IP Filters on the toolbar or click IP Filters on the left tree of the main interface.

3 iStorage Server Management Co	nsole			- • ×
<u>Storage</u> <u>Clients</u> <u>View</u> <u>T</u> ool	<u>H</u> elp			
Create Delete Sta	t Stop Refresh Add	Remove View A	ccess Settings	Print About
E@ kernsafe-PC È@ Targets	iStorage Server: kerns	afe-PC		
iqn.2006-03.com.kerns	^{afe.k} General Targets Applications IP F	ilters Users Groups Logs		
	Target Name	Devic Source	Capa Authentic	Status
Users	iqn.2006-03.com.kernsafe.kern	Disk E:\newimage.img	1.00G Anonymo	Ena
< III	•			
Done		🔇 C	onnected: kernsafe-PC (U	Iltimate License)

Click the Add button on the Toolbar, the Add clients to IP filter dialog is shown.

Add clients to IP fil	ter					×
Add Type						
 Any 	🔘 IP Addr	ess	0	IP Ra	inge	
- IP or IP Range -						
Begin IP:	0	. 0		Ο.	0	
End IP:	0	. 0		0.	0	
-Access Mode -						
	Full	Acces	S		•	
		(O	K	Ca	ancel

Any: Indicate all of the clients connected to the target have the same access right. IP Address: Indicate the IP address has the given access right.

IP Range: Indicate the clients specified by the range has the given access right.

Press the **OK** button to add an IP filter item.

iStorage Server Management Consol			- • ×
<u>S</u> torage <u>C</u> lients <u>V</u> iew <u>T</u> ools <u>F</u>	lelp		
Create Delete Start	Stop Refresh Add Remove	View Access Settings	Print About
E@ kernsafe-PC E@ Targets	iStorage Server: kernsafe-PC		
Applications	General Targets Applications IP Filters Users	Groups Logs	
	IP Address	Computer Name	Access Control
Users	60 0.0.0.0	Any Address	Full Access
	192.168.0.111	kernsafe-PC	Virtual Write
	192.168.0.102	kernsafe-PC	ReadOnly
	192.168.0.101	kernsafe-PC	Refuse
		11	
Ready S Connected: kernsafe-PC (Ultimate License)			

User can modify IP filter item's access right, Read Only, Refuse, Virtual Write and Full Access, or remove some IP filter items if they are not needed.

2. Server Side Local Security Policy Setting

Click "Start -> Control Panel -> Administrative Tools -> Local Security Policy" open the "Local Security Settings Management Console.



Select the **IP Security Policies** on Local Computer, right click on the blank of right panel, then select the **Create IP Security Policy** menu item, the **IP Security Policy Wizard** is shown.



Press the **Next** button to continue.

Type IP Security Policy Name

IP Security Policy Wizard	? ×
IP Security Policy Name Name this IP Security policy and provide a brief description	Ē
Na <u>m</u> e: <mark>KernSafe IP Security Policy</mark>	
Description:	
	T
< <u>B</u> ack <u>N</u> ext >	Cancel

Type "KernSafe IP Security Policy".

Press the **Next** button to continue.

Specify how this policy responds to requests for secure communication.

IP Security Policy Wizard		? ×
Requests for Secure Communication Specify how this policy responds to request	s for secure communicatio	n.
The default response rule responds to remo other rule applies. To communicate securely secure communication.	te computers that request y, the computer must respo	security, when no and to requests for
Activate the default <u>r</u> esponse rule.		
	< <u>B</u> ack <u>N</u> ext	:> Cancel

Do not select Activate the default response rule.

Press the Next button to continue.

Completing the IP Security Policy Wizard



Select the Edit properties by default.

Press the **Finish** to continue.

Then the KernSafe IP Security Policy Properties dialog is shown.

KernSafe IP Security Poli	cy Properties		? ×		
Rules General					
Security rules for communicating with other computers					
IP Security rules:					
IP Filter List	Filter Action	Authentication	Tu		
Comparise	Default Response	Kerberos	<n td="" <=""></n>		
			<u> </u>		
A <u>d</u> d <u>E</u> d	it <u>R</u> emove	Use Add <u>W</u> i	zard		
		OK Car	ncel		

Do not select Use Add Wizard.

Press the Add button, the New Role Properties dialog is shown.

New Rule Properties	<u>? ×</u>
Authentication Methods Tur IP Filter List	nnel Setting Connection Type Filter Action
The selected IP filter list	t specifies which network traffic will be
IP Filter <u>L</u> ists:	
Name	Description
O All ICMP Traffic	Matches all ICMP packets betw
<u>Add</u> <u>E</u> dit	<u>H</u> emove
01	Cancel Apply

Press the Add button, the IP Filter List dialog is shown.

Input IP Filter name.

IP Filter List			? ×
An IP filter list is compo	nets, IP		
Name:			
KernSafe			
Description:			<u>A</u> dd
			<u>E</u> dit
		V	<u>R</u> emove
IP Filter <u>s</u> :		🗖 L	Ise Add <u>W</u> izard
Mirrored Description	Protocol	Source Port	Destination
•			Þ
		ОК	Cancel

Type KernSafe in the Name and do not select Use Add Wizard.

Press the **Add** button to continue.

IP Filter Properties
Addresses Protocol Description
Source address:
Any IP Address
Destination address:
My IP Address
Mirrored. Match packets with the exact opposite source and destination addresses.
OK Cancel

Select **Any IP Address** in the Source address.

Select My IP Address in the Destination address.

Then change to the **Protocol** page.

IP Filter Properties	? ×
Addresses Protocol Description	
Select a protocol type: TCP	
Set the IP protocol port:	
• Erom any port	
C From this port:	
◯ <u>I</u> o any port	
 To this port: 	
3260	
OK Ca	ancel

Select TCP in Select a protocol type field.

Type 3260 in the To this port.

Press the **OK** button to continue.

IP Filter List				? ×
An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.				
<u>N</u> ame:				
KernSafe				
				<u>A</u> dd
			<u> </u>	<u>E</u> dit
			_	<u>R</u> emove
IP Filter <u>s</u> :			🗖 Us	e Add <u>W</u> izard
Mirrored De	scription	Protocol	Source Port	Destination
Yes		TCP	ANY	
•				Þ
			ОК	Cancel

Press the **OK** button to continue.

N	ew Rule Properties	<u>? ×</u>			
	Authentication Methods Tur IP Filter List	nnel Setting Connection Type			
	The selected IP filter list specifies which network traffic will be affected by this rule.				
	IP Filter <u>L</u> ists:				
	Name	Description			
	O All ICMP Traffic	Matches all ICMP packets betw			
	O All IP Traffic Matches all IP packets from this				
	<u> </u>				
	A <u>d</u> d <u>E</u> dit	Remove			
	Clo	se Cancel <u>A</u> pply			

Select the KernSafe IP Filter item which we just created and change to Filter Action page.

New Rule Properties	<u>? ×</u>
Authentication Methods Tur IP Filter List	nnel Setting Connection Type Filter Action
The selected filter actio for secure network traff	n specifies whether this rule negotiates ic, and how it will secure the traffic.
Eilter Actions:	
Name	Description
O Permit	Permit unsecured IP packets to
O Request Security (Optional)	Accepts unsecured communicat
	Accepts unsecured communicat
A <u>d</u> d <u>E</u> dit	<u>R</u> emove
Clo	se Cancel <u>A</u> pply

Select Require Security and then change to Connection Type page.

New Rule Properties			? ×
IP Filter List	Turnel Celli	Filter Acti	on
Authentication Methods This rule only a E the selected typ	pplies to network	traffic over con	nections of
• All network connections			
C Local area network (LAN)		
C <u>R</u> emote access			
[Close	Cancel	Apply

Select the All network connections, and then change to Tunnel Setting page.

New Rule Properties			? ×
IP Filter List Authentication Methods	s Tunnel Set	Filter Acti ting Conr	on hection Type
The tunnel IP traffic de list. It takes	endpoint is the tunn estination, as specifie two rules to describ	eling computer c d by the associa e an IPSec tunni	losest to the ted IP filter el.
 This rule does not sp The tunnel endpoint 0 . 0 . 0 	ecify an IPSec tunne is specified by this [F) . 0	al) address:	
,			
	Close	Cancel	Apply

Select **This rule does not specify an IPSec tunnel**, and then change to **Authentication Methods** page.

New Rule Properties		<u>? </u> ×
IP Filter List Authentication Methods	F Tunnel Setting	ilter Action
Authentication between comp offered and ac computer.	methods specify how tru outers. These authenticat cepted when negotiating	st is established on methods are security with another
Authentication <u>m</u> ethod prefe	rence order:	
Method Kerberos	Details	<u>Add</u>
		<u>E</u> dit
		<u>R</u> emove
		Move <u>up</u>
		Move d <u>o</u> wn
	Close Ca	ncel <u>Apply</u>

Select Kerberos, press the Edit button, the Edit Authentication Method Properties dialog is shown.

Edit Authentication Method Properties	<u>?</u> ×
Authentication Method	
The authentication method specifies how trust is establishe	:d
Active Directory <u>default</u> (Kerberos V5 protocol)	
O Use a certificate from this certification authority (CA):	
Browse	
Exclude the CA name from the certificate request	
Enable certificate to account mapping	
 Use this string (preshared key): 	_
123	1
OK Cano	;el

Select Use this string (preshared key), type the preshared key, we take "123" as an example.

New Rule Properties		<u>? ×</u>
IP Filter List Authentication Methods Authentication between com offered and ac	Tunnel Setting Tunnel Setting methods specify how tru: puters. These authenticati ccepted when negotiating	ilter Action Connection Type st is established ion methods are security with another
Authentication <u>m</u> ethod prefit	erence order: Details 123	A <u>d</u> d <u>E</u> dit <u>R</u> emove Move <u>up</u> Move d <u>o</u> wn
	Close Ca	ncel <u>Apply</u>

Press the **Apply** button to save settings and press the **Close** button to close this dialog.

KernSafe IP Security Poli	cy Properties		<u>?</u> ×	
Rules General				
Security rules for communicating with other computers				
IP Security rules:				
IP Filter List	Filter Action	Authentication	Tu	
✓ KernSafe	Require Security	Preshared Key	Nc	
▲ 	it	Use Add <u>W</u> iz	▶ zard	
		OK Car	ncel	

Check KernSafe in the IP Filter List and then press the \mathbf{OK} button to continue.

Back to Local Security Settings main interface.



Right click on the **KernSafe IP Security Policy** item and then select Assign to make this item enabled.

3. Client Side Local Security Policy Setting

Open Start -> Control Panel -> Administrative Tools -> Local Security Policy, The Local Security Settings Console is shown.

Cocal Security Settings				_ 🗆 🗵
<u>File Action View H</u> elp				
Security Settings Account Policies Dublic Key Policies Software Restriction Policies Decurity Policies on Local Computer	a. Name ▲ Server (Request Sec Client (Respond Only) Secure Server (Requi Greate Manac All Tas Refres Export View Arrang Ling uy Help	Description For all IP traffic, always req Communicate normally (uns For all IP traffic, always req Por all IP traffic, always req P Security Policy IP Security Policy	Policy A No No No	Last Modified Time 2009-7-9 14:52:23 2009-7-9 14:52:23 2009-7-9 14:52:23
Creates an IP Security policy.	,			

IP Security Policies on Local Computer and right click on the blank of the right panel. Then select **Create IP Security Policy**. The **IP Security Policy Wizard** is shown.

IP Security Policy Wizard		? ×
	Welcome to the IP Security Policy Wizard	
	This wizard helps you create an IP Security policy. You will specify the level of security to use when communicating with specific computers or groups of computers (subnets), and for particular IP traffic types.	
	To continue, click Next.	
	< Back Next> Canc	el

Press the **Next** button to continue.

Enter IP Security Policy Name

IP Security Policy Wizard	? ×
IP Security Policy Name Name this IP Security policy and provide a brief description	Ē
Na <u>m</u> e: KernSafe IP Security Policy	
Description:	
	×
< <u>B</u> ack <u>N</u> ext >	Cancel

Type "KernSafe IP Security Policy".

Press the Next button to continue.

Specify how this policy responds to requests for secure communication.



Don't select the "Activate the default response rule".

Press the **Next** button to continue.

Completing the IP Security Policy Wizard.

IP Security Policy Wizard	? ×
	Completing the IP Security Policy Wizard
	You have successfully completed specifying the properties for your new IP Security policy.
	To edit your IP Security policy now, select the Edit properties check box, and then click Finish.
	Edit properties
	To close this wizard, click Finish,
	< <u>B</u> ack Finish Cancel

Select the Edit properties.

Press the **Finish** button to continue.

The KernSafe IP Security Policy Properties Dialog will be shown.

KernSafe IP Security Poli	cy Properties		? ×
Rules General			
Security rules	for communicating with ot	her computers	
IP Security rules:			_
IP Filter List	Filter Action	Authentication	Tu
Comparise	Default Response	Kerberos	<n td="" <=""></n>
•			
A <u>d</u> d <u>E</u> c	it <u>H</u> emove	📕 🗖 Use Add <u>W</u> i	zard
		OK Car	ncel

Don't select the Use Add Wizard option.

Press the Add button, the New Rule Properties dialog is shown.

New Rule Properties	<u>? ×</u>
Authentication Methods Tur IP Filter List	nnel Setting Connection Type Filter Action
The selected IP filter list affected by this rule.	t specifies which network traffic will be
IP Filter <u>L</u> ists:	
Name	Description
	Matches all ICMP packets betw
	Matches all repackets nom this
Add <u>E</u> dit	<u>B</u> emove
10	Cancel Apply

Press the **Add** button to continue.

Setting IP Filter List.

IP Filter List			? ×
An IP filter list is co	omposed of multiple filters stocols can be combined	s. In this way, multiple su I into one IP filter.	bnets, IP
<u>N</u> ame:			
KernSafe			
Description:			<u>A</u> dd
		<u>^</u>	<u>E</u> dit
		V	<u>R</u> emove
IP Filter <u>s</u> :			Use Add <u>W</u> izard
Mirrored Description	Protocol	Source Port	Destination
<u></u>		OK	Cancel

Type the name of IP filter.

Don't select the Use Add Wizard option.

Press the Add button, the IP Filter Properties dialog is shown.

IP Filter Properties					? ×
Addresses Protocol Descrip	otion				
<u>Source address:</u>					
My IP Address			·	•	
Destination address:				_	
A specific IP Address				-	
IP add <u>r</u> ess:	192	. 168	. 0	. 8	
Subnet mas <u>k</u> :	255	. 255	. 255	. 255	
 Mirrored. Match packets addresses. 	with the e	xact oppos	site source	e and destir	nation
			OK	Ca	ancel

Select My IP Address in Source address Categories.

Select **A specific IP Address** in **Destination address** categories, and then type the IP address of your server machine.

Select the **Protocol** page to continue.

Set protocol properties.

IP Filter Properties	<u>?</u> ×
Addresses Protocol Description	
Select a protocol type: TCP	
Set the IP protocol port:	_
Erom any port	
F <u>r</u> om this port:	
○ <u>I</u> o any port	
To this port: 3260	
OK Can	cel

Select **TCP** in the **Select a protocol type** categories, and then type **3260** in the **To this port**. Press the **OK** button to continue.

Now we come back to the **IP Filter List** interface.

IP Filter	List			<u>? ×</u>
	An IP filter list is compo addresses and protocol	sed of multiple filters. In s can be combined into	this way, multiple subr one IP filter.	iets, IP
<u>N</u> ame:				
KernSafe				
Description	n:			<u>A</u> dd
			<u> </u>	<u>E</u> dit
				<u>R</u> emove
IP Filter <u>s</u> :				se Add <u>W</u> izard
Mirrored	Description	Protocol	Source Port	Destination
Yes		TCP	ANY	3260
•				•
			ОК	Cancel

Press the **OK** button to complete the IP Filter Item creation.

New Rule Properties	<u>? ×</u>
Authentication Methods Tu IP Filter List	Innel Setting Connection Type Filter Action
The selected IP filter lis affected by this rule.	st specifies which network traffic will be
IP Filter <u>L</u> ists:	
Name	Description
O All ICMP Traffic	Matches all ICMP packets betw
O All IP Traffic	Matches all IP packets from this
A <u>d</u> d <u>E</u> dit	<u>R</u> emove
	ose Cancel Apply

Select the KernSafe IP Filter item we just create. Change to **Filter Action** page.

New Rule Properties	<u>? ×</u>
Authentication Methods Tu IP Filter List	innel Setting Connection Type Filter Action
The selected filter action for secure network traft	on specifies whether this rule negotiates fic, and how it will secure the traffic.
<u>F</u> ilter Actions:	
Name	Description
O Permit	Permit unsecured IP packets to
O Request Security (Optional)	Accepts unsecured communicat
	Accepts unsecured communicat
A <u>d</u> d <u>E</u> dit	<u>R</u> emove
Clo	ose Cancel Apply

Select Require Security.

Change to **Connection Type** page.

New Rule Properties			? ×
IP Filter List Authentication Methods	Tunnel Setti	Filter Actio	on ection Type
This rule only a This selected typ	pplies to network	traffic over con	nections of
• All network connections			
C Local area network (LAN)		
O <u>R</u> emote access			
[Close	Cancel	Apply

Select All network connections.

Change to **Tunnel Setting** page.

New R	ule Prop	perties				? ×		
A	uthentica	IP Filter List ation Methods	 Tunnel Sett	Filt	er Actio Conn	n ection Type		
		The tunnel endp IP traffic destina list. It takes two	coint is the tunn ation, as specifie rules to describ	eling comp d by the a e an IPSe	outer clo ssociati c tunne	osest to the ed IP filter I.		
•	This rule does not specify an IPSec tunnel. The tunnel endpoint is specified by this <u>I</u> P address:							
			0					
		[Close	Cano	el	Apply		

Select This rule does not specify an IPSec tunnel. Change to Authentication Methods page.

New Rule Pro	perties			<u>?</u> ×
Authentica	IP Filter List Authentication Methods		Filter Ad g Co	nnection Type
	between comp offered and ac computer.	outers. These authe cepted when nego	intication me tiating securi	thods are ty with another
Authenticati	ion <u>m</u> ethod prefe	erence order:		
Kerberos				<u>E</u> dit <u>R</u> emove
				Move d <u>o</u> wn
		Close	Cancel	<u>A</u> pply

Select Kerberos.

Press the Edit button, the Edit Authentication Method Properties dialog is shown.

Edit Authentication Method Properties	? ×
Authentication Method	
The authentication method specifies how trust is establisher between the computers.	ed .
C Active Directory default (Kerberos V5 protocol)	
O Use a certificate from this certification authority (CA):	
Browse	
 Exclude the CA name from the certificate request Enable certificate to account mapping 	
• Use this string (preshared key):	
123	A
OK Can	cel

Select **Use this string (preshared key),** then type 123 or other text as password in the input box. Press the **OK** button to apply.

New Rule Properties		<u>?</u> ×
IP Filter List Authentication Methods	Tunnel Setting	Filter Action Connection Type
Authenticatior between com offered and ac computer.	n methods specify how tru puters. These authentical ccepted when negotiating	ist is established ion methods are g security with another
Authentication method prefe	erence order:	
Method	Details	A <u>d</u> d
Preshared Key	123	<u>E</u> dit <u>R</u> emove
		Move <u>up</u> Move d <u>o</u> wn
	Close Ca	ncel <u>Apply</u>

Press the **Apply** button and then press the **Close** button to close this dialog.

KernSafe IP Security Po	olicy Properties		? ×
Rules General			
Security rule	es for communicating with o	ther computers	
IP Security rules:			
IP Filter List	Filter Action	Authentication	Tu
✓ KernSafe	Require Security	Preshared Key	Nc
Oynamic>	Default Response	Kerberos	<n< td=""></n<>
▲ 	dit	Use Add <u>W</u>	▶ izard
		OK Ca	incel

Select KernSafe IP Filter item and then press the **OK** button.

Back to the Local Security Settings Console main interface



Select **IP Security Polices on Local Computer** and then right click on the blank of right panel. Select the **Assign** menu item in the popup menu to make this item enabled.

4. Logging on to the target

Open Microsoft Initiator

iSCSI Init	iator Prope	rties				×
General	Discovery	Targets P	ersistent Targ	jets Bound	Volumes/Devic	es
$\lceil \underline{I} $ arg	et Portals —					
Ad	dress	Port	Adapter		IP Address	
				-		
<u> </u>	Add		<u>R</u> emove	R	<u>e</u> fresh	
iSN9	Servers —					1
Na	ime					
		1		1		
	A <u>d</u> d		Remove	R	e <u>f</u> resh	
					1	
			UK	Cancel	Apply	

Select the Discovery tab page.

Press the **Add** button in the Target Portals, the **Add Target Portal dialog** is shown.

Add Target Portal		×
Type the IP address or DNS name a want to add. Click Advanced to sele session to the portal.	nd socket number of ct specific settings fi	the portal you or the discovery
IP address or DNS name:	<u>P</u> ort:	
192.168.0.8	3260	<u>A</u> dvanced
	OK	Cancel

Type the IP address and port of your server.

Press the **OK** button to continue.

iSCSI Initiator Properties					
General	Discovery	Targets	Persistent Target	s Bound Vo	lumes/Devices
<u> </u>	et Portals —				
Add		Port	Adapter		PAddress
	. 166.0.8	3260	Derault		Perault
	<u>A</u> dd		<u>R</u> emove	R <u>e</u> fr	resh
iSNS Servers					
Nar	ne				
	A <u>d</u> d		Remove	Re <u>f</u> r	resh
			ОК	Cancel	Apply

Change to Targets page.

iSCSI Initiator Properties	×		
General Discovery Targets Persistent Targets	Bound Volumes/Devices		
Select a target and click Log On to access the storage devices for that target. Click details to see information about the sessions, connections and devices for that target.			
Targets:			
Name ign 2008-03 com kernsste kernsste test image	Status		
<u>D</u> etails <u>L</u> og O	n Refresh		
ОК	Cancel Apply		

Select the target in the Targets list, and then press the Log On button.

Then the Log On to Target dialog is shown.

Log On to Target 🔀			
Target name:			
ign.2006-03.com.kernsafe.kernsafe-test.ImageDisk0			
\square Automatically restore this connection when the system boots			
Enable multi-path			
Only select this option if iSCSI multi-path software is already installed on your computer.			
Advanced OK Cancel			

If your iSCSI target using IP filter authorization, just press the **OK** button to continue.

If your iSCSI target using CHAP user authorization, press the **Advance** button, the **Advanced Settings dialog** is shown.

Advanced Settings			
General IPSec			
Connect by using			
Local <u>a</u> dapter: Default			
Source IP: Default			
Iarget Portal: Default			
CRC / Checksum			
□ Data digest □ Header digest			
- 🔽 CHAP logon information			
CHAP helps ensure data security by providing authentication between a target and an initiator trying to establish a connection. To use it specify the same target CHAP secret that was configured on the target for this initiator.			
User name: test			
Target secret:			
Perform mutual authentication			
To use mutual CHAP specify an initiator secret on the Initiator Settings page and configure that secret on the target.			
OK Cancel Apply			

Select CHAP login information and type User name and Target secret.

Press the **OK** button to continue.

iSCSI Initiator Properties	×
General Discovery Targets Persistent Targets Bound Volumes/De	evices
Select a target and click Log On to access the storage devices for that target. Click details to see information about the sessions, connections a devices for that target.	and
Targets:	
Name Status	
iqn.2006-03.com.kernsafe.kernsafe-test.Image Connected	
<u>D</u> etails <u>Log On</u> R <u>e</u> fresh	
OK Cancel Ap	yly

When the connection is created, you will see the connection in the Status column. Now, you may operation the iSCSI disk just as a normal disk.

5. Effect

TCP/IP online traffic when not using IP SEC.

Filter:			▼ Expression Clea <u>r</u> Apply			
	Source	Destination	Protocol	Info		
	192.168.159.142	192.168.159.131	iscsi	SCSI: Mode Sense(6) LUN: 0x00		
	192.168.159.131	192.168.159.142	iscsı	SCSI: Data In LUN: 0x00 (Mode Se		
	192.168.159.142	192.168.159.131	iscsi	SCSI: Read Capacity(10) LUN: 0x0		
	192.168.159.131	192.168.159.142	iscsi	SCSI: Data In LUN: 0x00 (Read Ca		
	192.168.159.142	192.168.159.131	iscsi	SCSI: Read(10) LUN: 0x00 (LBA: 0		
	192.168.159.131	192.168.159.142	iscsi	SCSI: Data In LUN: 0x00 (Read(10		
	192.168.159.142	192.168.159.131	iscsı	SCSI: Read(10) LUN: 0x00 (LBA: 0		
	192.168.159.131	192.168.159.142	iscsi	SCSI: Data In LUN: 0x00 (Read(10		
	192.168.159.142	192.168.159.131	iscsı	SCSI: Read Capacity(10) LUN: 0x0		
	192.168.159.131	192.168.159.142	iscsi	SCSI: Data In LUN: 0x00 (Read Ca		
	192.168.159.142	192.168.159.131	iscsı	SCSI: Read(10) LUN: 0x00 (LBA: 0		
	192.168.159.131	192.168.159.142	iscsı	SCSI: Data In LUN: 0x00 (Read(10		
	192.168.159.142	192.168.159.131	iscsı	SCSI: Read(10) LUN: 0x00 (LBA: 0		
	192.168.159.131	192.168.159.142	iscsı	SCSI: Data IN LUN: 0x00 (Read(10		
	192.168.159.142	192.168.159.131	iscsi	SCSI: Read Capacity(10) LUN: 0x0		
	192.168.159.131	192.168.159.142	iscsı	SCSI: Data In LUN: 0x00 (Read Ca		

We will "see" all the information when initiators communication with targets.

TCP/IP online traffic when using IP SEC.

Filter:				▼ Expression Clea <u>r</u> Apply		
	Source	Destination	Protocol	Info		
	195.108.128.131	192.108.109.142	ESP	ESB (SBI=0X88113C/0)		
	192.168.159.131	192.168.159.142	ESP	ESP (SPI=0x88ff3c70)		
	192.168.159.131	192.168.159.142	ESP	ESP (SPI=0x88ff3c70)		
	192.168.159.131	192.168.159.142	ESP	ESP (SPI=0x88ff3c70)		
	192.168.159.131	192.168.159.142	ESP	ESP (SPI=0x88ff3c70)		
	192.168.159.142	192.168.159.131	ESP	ESP (SPI=0x572fd6f8)		
	192.168.159.142	192.168.159.131	ESP	ESP (SPI=0x572fd6f8)		
	192.168.159.142	192.168.159.131	ESP	ESP (SPI=0x572fd6f8)		
	192.168.159.142	192.168.159.131	ESP	ESP (SPI=0x572fd6f8)		
	192.168.159.131	192.168.159.142	ESP	ESP (SPI=0x88ff3c70)		
	192.168.159.131	192.168.159.142	ESP	ESP (SPI=0x88ff3c70)		
	192.168.159.131	192.168.159.142	ESP	ESP (SPI=0x88ff3c70)		
	192.168.159.131	192.168.159.142	ESP	ESP (SPI=0x88ff3c70)		
	192.168.159.131	192.168.159.142	ESP	ESP (SPI=0x88ff3c70)		
	192.168.159.131	192.168.159.142	ESP	ESP (SPI=0x88ff3c70)		
	192.168.159.131	192.168.159.142	ESP	ESP (SPI=0x88ff3c70)		
	192.168.159.142	192.168.159.131	ESP	ESP (SPI=0x572fd6f8)		
•						

All the information is encrypted.