# iStorage Server: IP SEC under Windows Server 2008 R2

Monday, July 4, 2011



KernSafe Technologies, Inc.

www.kernsafe.com

Copyright © KernSafe Technologies 2006-2011. All right reserved.

### **Table of Contents**

Configuring iStorage Server	4
Creating Target	4
Server Side Local Security Policy Setting	13
Client Side Local Security Policy Setting	39
Logging on to the target	65
Effect	73
Contact	74

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. It is shown how to do it under Windows Server 2008 R2. At the time this article also 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.

## **Configuring iStorage Server**

## **Creating Target**

Open iStorage Server Management Console.

😓 iStorage Server Management Console					
<u><u>F</u>ile <u>Server</u> <u>Storage</u> <u>Clients</u> <u>V</u>iew <u>T</u>ool</u>	s <u>H</u> elp				
Create Delete Start Stop	Refresh Add Remove	View Access Settings Print	(1) About		
KernSafe Servers KernSafe_Matt (127.0.0.1:3261) Targets Applications	iStorage Server: LocalH <sup>al</sup> Targets Applications IPFilte	ost s Users Groups Logs			
	torage General Pro	perties	Properties		
	General				
	Hostname:	LocalHost			
	Bind Address:	All Address	=		
	Port:	3260			
	Management Method:	Password			
	State:	ОК			
	Status				
	Status:	Started			
	License:	Ultimate License			
< •	Server Portal				
	100.100.10		S Connected: LocalHost (Ultimate License)		

Launch the **iStorage Server Management Consolle**, press the **Create** button on the toolbar, the **Create iSCSI Target Wizard** will appear.

Select device type.

Create iSCSI Target Wizard	×
<b>iSCSI Device Type</b> Select which device type of the iSCSI target you want to create.	
<ul> <li>Hard Disk Create iSCSI target by using physical disk, partition, standard image file or VHD.</li> <li>CD/ DVD Device Create iSCSI target by using physical optical drive or CD / DVD image file.</li> <li>Generic SCSI Create iSCSI target by using generic SCSI device, such as disk, CD-ROM, tape, printer.</li> </ul>	ancel

Chose Hard Disk.

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

Choose Image File in iSCSI Medium Type page.

Create iSCSI Target Wizard	<b>x</b>
<b>iSCSI Image Type</b> Select image type of the iSCSI disk you want to create.	<u></u>
Image File         Create iSCSI disk by using a standard disk image file.         Image File         Image File         Create iSCSI disk by using a Virtual Hard Disk image file.         Image File         Image File	Cancel

Chose Standard Image File in iSCSI Image Type.

Create iSCSI Target Wizard	×
Image Disk Configuration You can specify a image file as an iSCSI device.	1
Device Parameters	
Use existing image file Oreate a new image file	
D:\IPSEC.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	
< <u>Back</u> Next > Can	cel

Select **Create a new image file** or **Use existing image file** if you already have one. Then specify the device size.

Checking **Use sparse file on NTFS file system** will save your hard disk space by expanding image file depending on its content used.

Create iSCSI Target Wizard	x
Authorization You can select an authorization mode, Anonymous, CHAP or IP filter.	4
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 > C	Cancel

Decide which authentication mechanisms you would want to use: **Anonymous**, **CHAP**, **IP Filter** or **Mixed** authentication.

#### 1) Anonymous

All initiators will get full access permission without any authorization required.

#### 2) CHAP (Challenge-handshake authentication protocol)

All initiators need to specify a CHAP user and secret to connect to the target. iStorage Server has a built-in user called "Guest", which is used for initiators without CHAP secret specified.

#### 3) IP Filters

All initiators will be authorized by the incoming IP address defined by IP Filter roles.

#### 4) Mixed

Security policy is determined by both CHAP and IP Filters.

If you check **Inherit security roles from global settings**, all client security roles are form global settings, otherwise, each client will have its own permission.

For this purpose I will choose **Mixed** and I will uncheck **Inherit security roles from global settings** since I will set it up manually for this target.

Create iSCSI Target Wizard	×
<b>Completing the Create iSCSI Wizard</b> You can specify a target name and other options to complete iSCSI target creating.	4
Basic Target Information	
iqn.2006-03.com.kemsafe:IPSEC	
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.	
< <u>Back</u> Finish	Cancel

Enter the name for your target device.

If you check **Report as readonly device when initiator cannot get write access**, the system will give you a report when you load the target without write access.

Press the **Finish** button to continue.

Now we need to set up CHAP and IP filter.

To set up **CHAP** for this target please switch to the **Users** group in the left side panel. **Right click** on empty space and choose **New User** ....

🍓 iStorage Server Management Console		_ <b>_</b> ×
<u>File Server</u> Storage Clients View	<u>I</u> ools <u>H</u> elp	
Create Delete Start Stop	O     Image: Constraint of the second s	
KernSafe Servers KernSafe_Matt (127.0.0.1:3261) Targets FSEC Applications Users Scoups Logs	iStorage Server: LocalHost General Targets Applications IPFilters Users Groups Logs User Name Guest Create/Edit User User Name: CHAP Password: Confrim password: User name and password are case sensitive. OK Cancel	
· · · · ·		
Ready	Connected: LocalHost (Ultim	ate License)

Type desired **User Name** and **Password** but keep in mind that perfect password should be from 12 to 16 characters long and it is case sensitive.

Click **OK** to continue.

After finishing, please click on name of your target in left side panel and switch to **CHAP** tab. **Right click** on empty space and choose **Add Item...** 

Cł	noose User o	or Group				×	
	Special — Guest User — CHAP						
	Access:	Full Access		ĸ	Ca	•ncel	]

Choose your chap user and specify access rights. Click **OK** button to continue.

Now please switch to **IPFilters** tab.

Right Click on empty space and choose Add Item..., the Add clients to IP filter dialog is shown.

Add clients to IP filter				×	
Add Type					
O Any O IP	Address	© IP	Range		
- IP or IP Range					
Begin IP:	192 . 168	. 0	. 188		
End IP:	192 . 168	. 0	. 188		
Access Mode					
Full Access					
OK Cancel					

Set up your IP filter.

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.

Here, for example, I chose IP Adress.

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

🌜 iStorage Server Management Console							
<u>File Server Storage Clients Vie</u>	w <u>T</u> ools <u>H</u> elp						
Create Delete Start St	Image: Second system         Image: Se	- Construction - Cons	ut				
E-IIII KernSafe Servers KernSafe_Matt (127.0.0.1:3261) Targets Local Local	Target IQN: iqn.2006-03.com.ker	nsafe:IPSEC					
Applications	IP Address	Computer Name	Access Control Status				
IPFilters	192.168.0.188	KernSafe_Matt	Full Access Static				
Groups	<b>192.168.0.199</b>	KernSafe_Matt	Readonly Static				
Logs							
<							
Ready S Connected: LocalHost (Ultimate License)							

Here you can modify IP filter item's access right - Read Only, Refuse, Virtual Write and Full Access.

Now we successfully finished configuration of our iSCSI Target in iStorage Server.

## Server Side Local Security Policy Setting

To access **Local Security Policy** under Windows Server 2008 R2, you can either type **Local Security Policy** in **Start search box** or you can navigate there by going:

```
Start --> Control Panel --> Administrative Tools --> Local Security Policy
```



Select IP Security Policies on Local Computer in the left side panel, then select Create IP Security Policy... from the content menu, the IP Security Policy Wizard is shown.



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

#### Type KernSafe IP Security Policy.

Press **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 requests for secure communication.	
The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.	
Note: The default response rule is supported only on computers that are running Windows 2003 and Windows XP.	
Activate the default response rule (earlier versions of Windows only).	
< <u>B</u> ack <u>N</u> ext > Cancel	

Do not select Activate the default response rule.



Select the Edit properties.

Press the Finish to continue.

Then the KernSafe IP Security Policy Properties dialog is shown.

KernSafe IP Security I	Policy Properties	? ×
Rules General		
Security ru	les for communicating with o	ther computers
IP Security rules:		
IP Filter List	Filter Action	Authentication Tu
Oynamic>	Default response (ea	Kerberos <n< td=""></n<>
		F
		1
<u>Add</u>	<u>Edit</u> <u>H</u> emove	Use Add <u>W</u> izard
		OK Cancel

Do not select Use Add Wizard.

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

New Rule Properties	×
Authentication Methods Tur IP Filter List	nnel Setting Connection Type
The selected IP filter list	t specifies which network traffic will be
IP Filter <u>Li</u> sts:	
Name	Description
Add Edit	<u>R</u> emove
0	K Cancel <u>A</u> pply

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

Input IP Filter name.

🔝 IP Filte	r List			×
	An IP filter list is comp addresses and protoc	osed of multiple filters. In ols can be combined into	this way, multiple su one IP filter.	bnets, IP
<u>N</u> ame:				
KemSaf	e			
<u>D</u> escripti	on:			<u>A</u> dd
			<u></u>	<u>E</u> dit
			7	<u>R</u> emove
IP Filters	:			Use Add <u>W</u> izard
Mirrore	d Description	Source DNS Name	Source Address	[
•				▶
			ОК	Cancel

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

Press the **Add** button to continue.



Select Any IP Address in the Source address.

Select My IP Address in the Destination address.

Then change to the **Protocol** tab.

IP Filter Properties	×
Addresses Protocol Description	
Select a protocol type: TCP	
Set the IP protocol port:	
<u>F</u> rom any port	
C From this port:	
C To any port	
To this port:	
3260	
OK Cancel	

Select **TCP** in Select a protocol type field.

Type **3260** in the **To this port**.

n: <u>A</u> dd.	
· · · · · · · · · · · · · · · · · · ·	
Edit.	
- <u>B</u> emo	ve
Use Add W	liza
Description Source DNS Name Source Address	
<any address="" ip=""> <any address="" ip=""></any></any>	
Description         Source DNS Name         Source Address <any address="" ip=""> <any address="" ip=""> <any address="" ip=""></any></any></any>	

New Rule Properties	<u>×</u>
Authentication Methods Tur IP Filter List	nnel Setting Connection Type
The selected IP filter list affected by this rule.	specifies which network traffic will be
IP Filter <u>Li</u> sts:	
Name	Description
	<b>n</b>
	Kemove
Clos	se Cancel <u>Apply</u>

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

New Rule Properties			×
Authentication Methods IP Filter List	Tunnel Sett	ting Connec Filter Action	ction Type
The selected filt for secure netwo	er action specifi ork traffic, and h	ies whether this rule now it will secure the	e negotiates e traffic.
<u>F</u> ilter Actions:			
Name	Descri	ption	
A <u>d</u> d <u>E</u> dit	<u>R</u> emo	ve 🔽 Use A	dd <u>W</u> izard
[	Close	Cancel	Apply

Leave Use Add Wizard checked and click on Add... button.

Filter Action Wizard is shown.



Press Next to continue.

Filter Action Wizard	×
Filter Action Name Name this filter action and provide a brief description.	
Na <u>m</u> e:	
Request Authentication	
Description:	
< <u>B</u> ack <u>N</u> ext > Cance	!

In Name field type Request Authentication.

Press **Next** button to continue.

Filter Action Wizard			×
Filter Action General Options Set the filter action behavior.			
<ul> <li>Permit</li> <li>Block</li> <li>Negotiate security</li> </ul>			
	< <u>B</u> ack	Next >	Cancel

On the Filter Action General Options page, click Negotiate security, and then click Next.

Filter Action Wizard	×
Communicating with computers that do not support IPsec Communicating with computers that do not support IPsec may expose your network to security risks.	
Do you want to allow communication with computers that do not support IPsec?	
Do not allow unsecured communication.	
Allow unsecured communication if a secure connection cannot be established.	
Use this option if there are computers on your network that do not support IPsec or have an incompatible IPsec configuration. Allowing unsecured communication may expose your network to security risks.	
On a computer with Windows Vista or a later version of Windows, this option allows unsecured communication to be sent anytime a secure connection cannot be established.	
On a Windows 2000, Windows XP, or Windows 2003 computer, this option allows unsecured communications to be sent only when the remote computer does not support IPsec.	
< <u>B</u> ack <u>N</u> ext > Cancel	

On the **Communicating with computers that do not support IPsec page**, click **Allow unsecured communication if a secure connection cannot be established**.

Press **Next** to continue.

Filter Action Wizard	×
IP Traffic Security Specify a security method for IP traffic. To add multiple security methods, edit the filter action after completing the wizard.	
This filter action requires at least one security method for IP traffic.	
<ul> <li>Integrity and encryption Data will be encrypted, authenticated, and unmodified.</li> <li>Integrity only Data will be authenticated and unmodified, but will not be encrypted.</li> <li>Custom</li> <li>Settings</li> </ul>	
< <u>B</u> ack <u>N</u> ext > Cancel	

On the **IP Traffic Security** page, click **Integrity only**, and then click **Next**.



On the last page, select **Edit properties**, and then click **Finish**.

The **Properties** page for the filter action appears.

Request Authentication Properties	×
Security Methods General	
<ul> <li>Permit</li> <li>Block</li> <li>Negotiate security:</li> <li>Security method preference order:</li> </ul>	
Type AH Integrity ESP Confidential ES	Add
Integrity <none></none>	<u>E</u> dit
	Move up
<ul> <li>Accept unsecured communication, but always respond to Allow fallback to unsecured communication if a secure of can not be established</li> <li>Use session key perfect forward secrecy (PFS)</li> </ul>	using IPsec connection
OK Cancel	Apply

Select **Accept unsecured communication, but always respond using IPsec** to enable inbound fallback-to-clear behavior.

Request Authentication Properties	×
Security Methods General	
<ul> <li>Permit</li> <li>Block</li> <li>Negotiate security:</li> <li>Security method preference order:</li> </ul>	
Type AH Integrity ESP Confidential ES	A <u>d</u> d
Integrity <none> <none> SH</none></none>	<u>E</u> dit
	<u>R</u> emove
	Move <u>up</u>
	Move d <u>o</u> wn
Accept unsecured communication, but always respond	using IPsec
Allow fallback to unsecured communication if a secure of can not be established Use session key perfect forward secrecy (PES)	connection
1 Use session Key perfect forward secrecy (FFS)	
OK Cancel	Apply

Press Apply button and then hit OK.

New Rule Properties	X
Authentication Methods Tu	nnel Setting Connection Type   Filter Action
The selected filter action for secure network traff	n specifies whether this rule negotiates ic, and how it will secure the traffic.
Name	Description
Add	<u>R</u> emove
Clo	se Cancel <u>A</u> pply

Switch to **Connection Type** tab.

New Rule Properties				×
IP Filter List	. 1		Filter Action	
Authentication Methods	Tunnel	Setting	Connect	ion Type
This rule only ap	oplies to net e.	work traffic	over connect	tions of
All network connections				
C Local area network (LAN)	)			
C <u>R</u> emote access				
	Close	C	ancel	<u>A</u> pply

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

New Rule Properties			×		
IP Filter List Authentication Methods	Tunnel Settin	Filter Actio	on   lection Type		
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPsec tunnel.					
This rule does not specif     Tunnel endpoints are sp     IPv4 tunnel endpoint:	y an IPsec tunnel ecified by these <u>I</u> P	addresses:			
IPv6 tunnel endpoint:			]		
	Close	Cancel	Apply		

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

New Rule Properties				
IP Filter List Authentication Methods	Tur	nnel Setting	Filter Ac	tion nnection Type
Authentication between corr offered and a computer.	on methods nputers. Th accepted w	specify how t ese authentic /hen negotiatii	rust is est ation met ng securit	ablished hods are y with another
Authentication method pre	ference or	ler:		
Method	Details			A <u>d</u> d
Kerberos				<u>E</u> dit
				Bemove
				Tomore
				Move <u>up</u>
				Move d <u>o</u> wn
	Clos	se (	Cancel	Apply

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 established between the computers.	
C Active Directory default (Kerberos V5 protocol)	
C Use a certificate from this certification authority (CA):	
Browse	
<ul> <li>Exclude the CA name from the certificate request</li> <li>Enable certificate to account mapping</li> </ul>	
Use this string (preshared key):	
123	
UN Cancer	

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

Click **OK** button to continue.
New Rule Properties					X
IP Filter List Authentication Methods Authentication between comp offered and ac computer	Filter Action Tunnel Setting Connection Type methods specify how trust is established puters. These authentication methods are ccepted when negotiating security with another				
Authentication <u>m</u> ethod prefe	erence orde Details	er:		Add	-
Preshared Key	123			Edit <u>R</u> emove Move <u>up</u> Move d <u>o</u> wn	
	Close		Cancel	Apply	

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

KernSafe IP Security Po	licy Properties		? ×
Rules General			
Security rule:	s for communicating with ot	her computers	
IP Security rules:			
IP Filter List	Filter Action	Authentication	Tu
KemSafe	Request Authenticati	Preshared Key	No
Oynamic>	Default response (ea	Kerberos	<n< th=""></n<>
	dit	Use Add <u>W</u> izi	►
		OK Can	cel

Check KernSafe in the IP Filter List and then press the 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.

## **Client Side Local Security Policy Setting**

To access **Local Security Policy** under Windows Server 2008 R2, you can either type **Local Security Policy** in **Start search box** or you can navigate there by going:

Start --> Control Panel --> Administrative Tools --> Local Security Policy



Select IP Security Policies on Local Computer in the left side panel, then select Create IP Security Policy... from the content menu, the IP Security Policy Wizard is shown.



Press Next button to continue.

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

## Type KernSafe IP Security Policy.

Press **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 requests for secure communication.				
The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.				
Note: The default response rule is supported only on computers that are running Windows 2003 and Windows XP.				
Activate the default response rule (earlier versions of Windows only).				
< <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 P	olicy Properties		? ×
Rules General			
Security rule	es for communicating with of	her computers	
IP Security rules:			
IP Filter List	Filter Action	Authentication	Tu
Oynamic>	Default response (ea	Kerberos	<n< td=""></n<>
•			
A <u>d</u> d	Edit <u>R</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	×
Authentication Methods Tu IP Filter List	nnel Setting Connection Type
The selected IP filter lis	t specifies which network traffic will be
IP Filter <u>Li</u> sts:	
Name	Description
Add Edit	Remove
0	K Cancel Apply

Press the **Add** button to continue.

Setting IP Filter List.

🔜 IP Filt	er List			×
	An IP filter list is comp addresses and protoc	osed of multiple filters. In ols can be combined into	this way, multiple sub one IP filter.	onets, IP
<u>N</u> ame:				
KemSa	ife			
Descrip	tion:			<u>A</u> dd
			<u>^</u>	<u>E</u> dit
			-	<u>R</u> emove
IP Filter	<u>s</u> :			Use Add <u>W</u> izard
Mirrore	ed Description	Source DNS Name	Source Address	]
•				▶
			ОК	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 Description
Source address:
Any IP Address
Destination address:
A specific IP Address or Subnet
IP Address or Subnet: 192.168.0.188
Mirrored. Match packets with the exact opposite source and destination addresses.
OK Cancel

## Select My IP Address in Source address category.

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

Switch to the **Protocol** tab to continue.

Set protocol properties.

IP Filter Properties	×
Addresses Protocol Description	
Select a protocol type: TCP	
Set the IP protocol port:	
Erom any port	
C From this port:	
○ <u>T</u> o any port	
• To this port:	
3260	
OK Cancel	

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			×
	An IP filter list is compos addresses and protocols	ed of multiple filters. In t s can be combined into	his way, multiple sub one IP filter.	mets, IP
<u>N</u> ame:				
KemSafe				
Description	1:			<u>A</u> dd
			<u>^</u>	<u>E</u> dit
			-	<u>R</u> emove
IP Filter <u>s</u> :				Jse Add <u>W</u> izard
Mirrored	Description	Source DNS Name	Source Address	[
Yes		<any address="" ip=""></any>	<any address="" ip=""></any>	<
•				Þ
			ОК	Cancel

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

New Rule Properties	x
Authentication Methods Tu IP Filter List	nnel Setting Connection Type
The selected IP filter lis affected by this rule.	t specifies which network traffic will be
IP Filter <u>Li</u> sts:	
Name	Description
© KemSafe	
A <u>d</u> d <u>E</u> dit	<u>R</u> emove
Clo	se Cancel <u>Apply</u>

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

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

New Rule Properties			×
Authentication Methods IP Filter List	Tunnel Sett	ting Connec Filter Action	ction Type
The selected filt for secure netwo	er action specifi ork traffic, and h	ies whether this rule now it will secure the	e negotiates e traffic.
<u>F</u> ilter Actions:			
Name	Descri	ption	
A <u>d</u> d <u>E</u> dit	<u>R</u> emo	ve 🔽 Use A	dd <u>W</u> izard
[	Close	Cancel	Apply

Leave Use Add Wizard checked and click on Add... button.

Filter Action Wizard is shown.



Press Next to continue.

Filter Action Wizard	×
Filter Action Name Name this filter action and provide a brief description.	
Na <u>m</u> e:	
Request Authentication	
Description:	
< <u>B</u> ack <u>N</u> ext > Cance	!

In Name field type Request Authentication.

Press **Next** button to continue.

Filter Action Wizard			×
Filter Action General Options Set the filter action behavior.			
<ul> <li>Permit</li> <li>Block</li> <li>Negotiate security</li> </ul>			
	< <u>B</u> ack	Next >	Cancel

On the Filter Action General Options page, click Negotiate security, and then click Next.

Filter Action Wizard	×
Communicating with computers that do not support IPsec Communicating with computers that do not support IPsec may expose your network to security risks.	
Do you want to allow communication with computers that do not support IPsec?	
Do not allow unsecured communication.	
Allow unsecured communication if a secure connection cannot be established.	
Use this option if there are computers on your network that do not support IPsec or have an incompatible IPsec configuration. Allowing unsecured communication may expose your network to security risks.	
On a computer with Windows Vista or a later version of Windows, this option allows unsecured communication to be sent anytime a secure connection cannot be established.	
On a Windows 2000, Windows XP, or Windows 2003 computer, this option allows unsecured communications to be sent only when the remote computer does not support IPsec.	
< <u>B</u> ack <u>N</u> ext > Cancel	

On the **Communicating with computers that do not support IPsec page**, click **Allow unsecured communication if a secure connection cannot be established**.

Press **Next** to continue.

Filter Action Wizard	×
IP Traffic Security Specify a security method for IP traffic. To add multiple security methods, edit the filter action after completing the wizard.	
This filter action requires at least one security method for IP traffic.	
<ul> <li>Integrity and encryption Data will be encrypted, authenticated, and unmodified.</li> <li>Integrity only Data will be authenticated and unmodified, but will not be encrypted.</li> <li>Custom</li> <li>Settings</li> </ul>	
< <u>B</u> ack <u>N</u> ext > Cancel	

On the **IP Traffic Security** page, click **Integrity only**, and then click **Next**.



On the last page, select **Edit properties**, and then click **Finish**.

The **Properties** page for the filter action appears.

Request Authentication Properties	×
Security Methods General	
<ul> <li>Permit</li> <li>Block</li> <li>Negotiate security:</li> <li>Security method preference order:</li> </ul>	
Type AH Integrity ESP Confidential ES	A <u>d</u> d
Integrity <none> SH</none>	Edit
	Move <u>up</u>
	Move down
<ul> <li>Accept unsecured communication, but always respond to Allow fallback to unsecured communication if a secure of can not be established</li> <li>Use session key perfect forward secrecy (PFS)</li> </ul>	using IPsec connection
OK Cancel	Apply

Select **Accept unsecured communication, but always respond using IPsec** to enable inbound fallback-to-clear behavior.

Request Authentication Properties	×
Security Methods General	
<ul> <li>Permit</li> <li>Block</li> <li>Negotiate security:</li> <li>Security method preference order:</li> </ul>	
Type AH Integrity ESP Confidential ES	A <u>d</u> d
Integrity <none></none>	<u>E</u> dit
	<u>R</u> emove
	Move <u>up</u>
	Move d <u>o</u> wn
Accept unsecured communication, but always respond	using IPsec
Allow fallback to unsecured communication if a secure of can not be established Use session key perfect forward secrecy (PES)	connection
Use session Key perfect forward secrecy (FFS)	
OK Cancel	Apply

Press Apply button and then hit OK.

New Rule Properties	X
Authentication Methods Tur	nnel Setting Connection Type   Filter Action
The selected filter action for secure network traff	n specifies whether this rule negotiates ic, and how it will secure the traffic.
Filter Actions: Name Request Authentication	Description
Add <u>E</u> dit	<u>R</u> emove Use Add <u>W</u> izard
Clo	se Cancel <u>A</u> pply

Switch to **Connection Type** tab.

New Rule Properties				2
IP Filter List	. 1		Filter Action	
Authentication Methods	Tunne	el Setting	Connec	tion Type
This rule only a the selected typ	pplies to ne be.	twork traffic	over connec	ctions of
• All network connections				
C Local area network (LAN	)			
C <u>R</u> emote access				
	Close	C	ancel	<u>A</u> pply

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

New Rule Properties			×
IP Filter List Authentication Methods	Tunnel Settin	Filter Actio	on   lection Type
The tunnel end IP traffic destin list. It takes two	lpoint is the tunnelin ation, as specified l o rules to describe a	ng computer cl by the associat an IPsec tunne	osest to the ed IP filter I.
<ul> <li>This rule does not specif</li> <li>Tunnel endpoints are specified</li> <li>IPv4 tunnel endpoint:</li> </ul>	y an IPsec tunnel ecified by these <u>I</u> P	addresses:	
IPv6 tunnel endpoint:			]
	Close	Cancel	Apply

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

New Rule Properties				2
IP Filter List Authentication Methods	3 Tur	nnel Setting	Filter Act	ion nection Type
Authenticat between co offered and computer.	ion methods omputers. Th l accepted w	specify how t ese authentic /hen negotiatir	rust is esta ation meth ng security	ablished ods are with another
Authentication method pr	reference or	ler:		
Method	Details			A <u>d</u> d
Kerberos				Edit
				Bemove
				Towns to
				Move <u>u</u> p
				Move d <u>o</u> wn
	Clos	se (	Cancel	Apply

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 established between the computers.	
C Active Directory default (Kerberos V5 protocol)	
C Use a certificate from this certification authority (CA):	
Browse	
<ul> <li>Exclude the CA name from the certificate request</li> <li>Enable certificate to account mapping</li> </ul>	
Use this string (preshared key):	
123	
UN Cancer	

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

Click **OK** button to continue.

New Rule Properties					X
IP Filter List Authentication Methods Authentication between comp offered and ac computer	Tunn methods s outers. The ccepted wh	nel Setting specify how t se authentic sen negotiati	Filter Ac Co trust is es cation met ng securi	ction innection Type tablished thods are ty with another	
Authentication <u>m</u> ethod prefe	erence orde Details	er:		Add	-
Preshared Key	123			Edit <u>R</u> emove Move <u>up</u> Move d <u>o</u> wn	
	Close		Cancel	Apply	

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

KernSafe IP Security Po	licy Properties		? ×
Rules General			
Security rule	s for communicating with ot	her computers	
IP Security rules:			
IP Filter List	Filter Action	Authentication	Tu
KemSafe	Request Authenticati	Preshared Key	No
Oynamic>	Default response (ea	Kerberos	<n< th=""></n<>
	dit	Use Add <u>W</u> iz	► zard
		OK Car	ncel

Check KernSafe in the IP Filter List and then press the 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.

## Logging on to the target

<u>I</u> argeti		2	uick Connect
)iscovered ta	irgets		<u>R</u> efresh
Name		Status	
Fo connect u	sing advanced options, select a target	and then	Connect
To connect u click Connect To completely then click Dise	sing advanced options, select a target / disconnect a target, select the targe connect.	and then	Cognect Disconnect
To connect u click Connect Fo completely then click Disc =or target pr select the tar	sing advanced options, select a target , y disconnect a target, select the targe connect. operties, including configuration of ses get and click Properties.	and then	Connect Disconnect Properties
To connect u dick Connect To completely then click Disk For target pri select the tar For configura the target an	sing advanced options, select a target , y disconnect a target, select the targe connect. operties, including configuration of ses get and click Properties. ition of devices associated with a targe id then click Devices.	and then	Cognect Disconnect Properties Devices

Switch to the **Discovery** tab page.

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

Discover Target Portal	×
Enter the IP address or DNS name and p want to add.	ort number of the portal you
To change the default settings of the dis the Advanced button.	covery of the target portal, dick
IP address or DNS name:	Port: (Default is 3260.)
192.166.0.188	3260
<u>A</u> dvanced	<u>O</u> K <u>C</u> ancel

Type the **IP address** and **port** of your server.

Press the **OK** button to continue.

	rtals	c	<b>C H</b>			Refresh
The syste	em will lool	(for <u>T</u> argets)	on following p	ortals:		TO
Address 192.166	.0.188	3260	Adapt Defau	er It		IP address Default
To add a	target por	rtal, click Disc	over Portal.		Dis	cover <u>P</u> ortal
To remov then click	/e a target Remove.	t portal, selec	t the address	above and		<u>R</u> emove
Name				servers.		
Name						
Name To add a	n iSNS ser	ver, dick Add	Server.		A	dd Server
Name To add a To remov then dick	n iSNS serv ve an iSNS « Remove.	ver, click Add server, selec	Server. t the server a	bove and	A	dd Server Remove

Switch to Targets tab.

and name of	the target and the	n dick Quick Connect.		
<u>F</u> arget:				Quick Connect
)iscovered ta	argets			
				<u>R</u> efresh
Name			Stat	us
Fo connect u	sing advanced optic	ons, select a target and th	en	Connect
To connect u dick Connect To completel then click Dis	sing advanced optic : y disconnect a targe connect.	ons, select a target and the	en	Connect Disconnect
To connect u click Connect To completel then click Dis For target pr select the tar	ising advanced optic y disconnect a targe connect. roperties, including o rget and click Prope	ons, select a target and the et, select the target and configuration of sessions, rties.	en	Connect Disconnect Properties
To connect u click Connect To completel then click Dis For target pr select the tar for configura the target ar	ising advanced optic y disconnect a targe connect. operties, including o rget and click Prope ation of devices asse ation of devices asse	ons, select a target and the et, select the target and configuration of sessions, rties. ociated with a target, selects.	en	Connect Disconnect Properties De <u>v</u> ices

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

Then the Log On to Target dialog is shown.

Connect To Target	×
Target name:	
iqn.2006-03.com.kernsafe:IPSEC	
Add this connection to the list of Favorite Targets. This will make the system automatically attempt to resta connection every time this computer restarts.	ore the
Enable multi-path	
Advanced OK	Cancel

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

If your iSCSI target is using CHAP user authorization (and IP filter authorization), press the **Advanced** button, the **Advanced Settings** dialog is shown.

vanced Settings		? ×
General IPsec		
Connect using		_
Local adapter:	Default	
Initiator IP:	Default	
 Target portal IP:	Default	
Data digest	Header digest	
CHAP helps ensure co an initiator. To use, specify the sa initiator. The name w specified.	onnection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this vill default to the Initiator Name of the system unless another name is	
<u>N</u> ame:	CHAP	1
Target secret:	••••••	1
<u>P</u> erform mutual au To use mutual CHAP, RADIUS. <u>Use RADIUS to ge</u> Use <u>R</u> ADIUS to au	uthentication either specify an initiator secret on the Configuration page or use enerate user authentication credentials uthenticate target credentials	
	OK Cancel Ap	ply

Select EnableCHAP log on information and type Name and Target secret.

Press the **OK** button to continue.

iscovered ta	argets		
			<u>R</u> efresh
Name		Status	
To connect u	sing advanced options, select a target and	then	Co <u>n</u> nect
To connect u lick Connect To completel hen dick Dis	ising advanced options, select a target and t. y disconnect a target, select the target an connect.	then	Co <u>n</u> nect Disconnect
Fo connect u dick Connect Fo completel then click Dis For target pr select the ta	ising advanced options, select a target and t, y disconnect a target, select the target an connect. operties, including configuration of session rget and click Properties.	then	Co <u>n</u> nect Disconnect Properties

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

Filter:	er:			▼ Expression Clea <u>r</u> Apply			
	Source	Destination	Protocol	Info			
	192.168.0.188	192.168.159.139	iscsi	SCSI: Mode Sense(6) LUN: 0x00			
	192.168.159.139	192.168.0.188	iscsi	SCSI: Data In LUN: 0x00 (Mode Sei			
	192.168.0.188	192.168.159.139	iscsi	SCSI: Read Capacity(10) LUN: 0x0			
	192.168.159.139	192.168.0.188	iscsı	SCSI: Data In LUN: 0x00 (Read Ca			
	192.168.0.188	192.168.159.139	iscsı	SCSI: Read(10) LUN: 0x00 (LBA: 0)			
	192.168.159.139	192.168.0.188	iscsi	SCSI: Data In LUN: 0x00 (Read(10)			
	192.168.0.188	192.168.159.139	iscsı	SCSI: Read(10) LUN: 0x00 (LBA: 0)			
	192.168.159.139	192.168.0.188	iscsı	SCSI: Data In LUN: 0x00 (Read(10)			
	192.168.0.188	192.168.159.139	iscsı	SCSI: Read Capacity(10) LUN: 0x0			
	192.168.159.139	192.168.0.188	iscsı	SCSI: Data In LUN: 0x00 (Read Ca			
	192.168.0.188	192.168.159.139	iscsi	SCSI: Read(10) LUN: 0x00 (LBA: 0)			
	192.168.159.139	192.168.0.188	iscsi	SCSI: Data In LUN: 0x00 (Read(10)			
	192.168.0.188	192.168.159.139	iscsi	SCSI: Read(10) LUN: 0x00 (LBA: 0)			
	192.168.159.139	192.168.0.188	iscsı	SCSI: Data In LUN: 0x00 (Read(10)			
	192.168.0.188	192.168.159.139	iscsi	SCSI: Read Capacity(10) LUN: 0x0			
	192.168.159.139	192.168.0.188	iscsı	SCSI: Data In LUN: 0x00 (Read Ca			

TCP/IP online traffic when not using IP SEC.

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

TCP/IP online traffic when using IP SEC.

Filter:		▼ Expression Clear Apply		
	Source	Destination	Protocol	Info
	192.168.159.139 192.168.159.139 192.168.159.139 192.168.159.139 192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188 192.168.159.139 192.168.159.139 192.168.159.139 192.168.159.139 192.168.159.139 192.168.159.139 192.168.159.139 192.168.159.139 192.168.159.139 192.168.159.139 192.168.159.139 192.168.159.139 192.168.159.139 192.168.159.139 192.168.159.139	192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188 192.168.159.139 192.168.159.139 192.168.159.139 192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188 192.168.0.188	ESP ESP ESP ESP ESP ESP ESP ESP ESP ESP	ESP (SPI=0x88ff3c70) ESP (SPI=0x88ff3c70) ESP (SPI=0x88ff3c70) ESP (SPI=0x88ff3c70) ESP (SPI=0x572fd6f8) ESP (SPI=0x572fd6f8) ESP (SPI=0x572fd6f8) ESP (SPI=0x88ff3c70) ESP (SPI=0x572fd6f8)
•				

All the information is encrypted.

## Contact

Support:	support@kernsafe.com
Sales:	sales@kernsafe.com
Marketing:	marketing@kernsafe.com
Home Page:	http://www.kernsafe.com
Product Page:	http://www.kernsafe.com/product/istorage-server.aspx
Licenses	http://www.kernsafe.com/product/istorage-server/license-compares.aspx
Forum:	http://www.kernsafe.com/forum



KernSafe Technologies, Inc.

www.kernsafe.com

Copyright © KernSafe Technologies 2006-2011. All right reserved.