StarWind Virtual SAN®

Configuring Access Control List (ACL) Rules

2023

TECHNICAL PAPERS

Trademarks

“StarWind”, “StarWind Software” and the StarWind and the StarWind Software logos are registered trademarks of StarWind Software. “StarWind LSFS” is a trademark of StarWind Software which may be registered in some jurisdictions. All other trademarks are owned by their respective owners.

Changes

The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, StarWind Software assumes no liability resulting from errors or omissions in this document, or from the use of the information contained herein. StarWind Software reserves the right to make changes in the product design without reservation and without notification to its users.

Technical Support and Services

If you have questions about installing or using this software, check this and other documents first - you will find answers to most of your questions on the Technical Papers webpage or in StarWind Forum. If you need further assistance, please contact us .

About StarWind

StarWind is a pioneer in virtualization and a company that participated in the development of this technology from its earliest days. Now the company is among the leading vendors of software and hardware hyper-converged solutions. The company’s core product is the years-proven StarWind Virtual SAN, which allows SMB and ROBO to benefit from cost-efficient hyperconverged IT infrastructure. Having earned a reputation of reliability, StarWind created a hardware product line and is actively tapping into hyperconverged and storage appliances market. In 2016, Gartner named StarWind “Cool Vendor for Compute Platforms” following the success and popularity of StarWind HyperConverged Appliance. StarWind partners with world-known companies: Microsoft, VMware, Veeam, Intel, Dell, Mellanox, Citrix, Western Digital, etc.

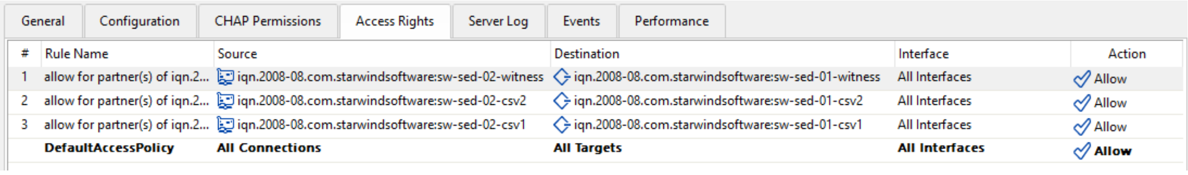
Copyright ©2009-2018 StarWind Software Inc.

Configuring the ACL rules for the StarWind Virtual SAN provisioned iSCSI target allows complying with security requirements or keeping targets separated in case multiple environments are served with the same storage based on the StarWind Virtual SAN server.

Configuring Global Access Rights Rules

By default, if no HA devices are configured on the server, a StarWind VSAN server has only one access rule added: DefaultAccessPolicy. This rule allows for all connections from all servers to all targets via all network interfaces and does not restrict access to any target or interface in any way. The Access Rights view for a standalone StarWind device is demonstrated in the screenshot below.

When HA devices are created on the StarWind VSAN node, the ACL rules for partner connections are added automatically as shown below.

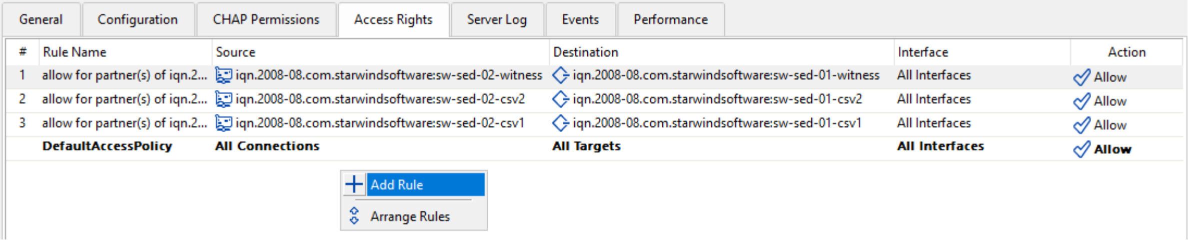


#	Rule Name	Source	Destination	Interface	Action
1	allow for partner(s) of iqn.2...	iqn.2008-08.com.starwindsoftware:sw-sed-02-witness	iqn.2008-08.com.starwindsoftware:sw-sed-01-witness	All Interfaces	✓ Allow
2	allow for partner(s) of iqn.2...	iqn.2008-08.com.starwindsoftware:sw-sed-02-csv2	iqn.2008-08.com.starwindsoftware:sw-sed-01-csv2	All Interfaces	✓ Allow
3	allow for partner(s) of iqn.2...	iqn.2008-08.com.starwindsoftware:sw-sed-02-csv1	iqn.2008-08.com.starwindsoftware:sw-sed-01-csv1	All Interfaces	✓ Allow
	DefaultAccessPolicy	**All Connections**	**All Targets**	**All Interfaces**	✓ **Allow**

Configuring Individual Access Rights Rules

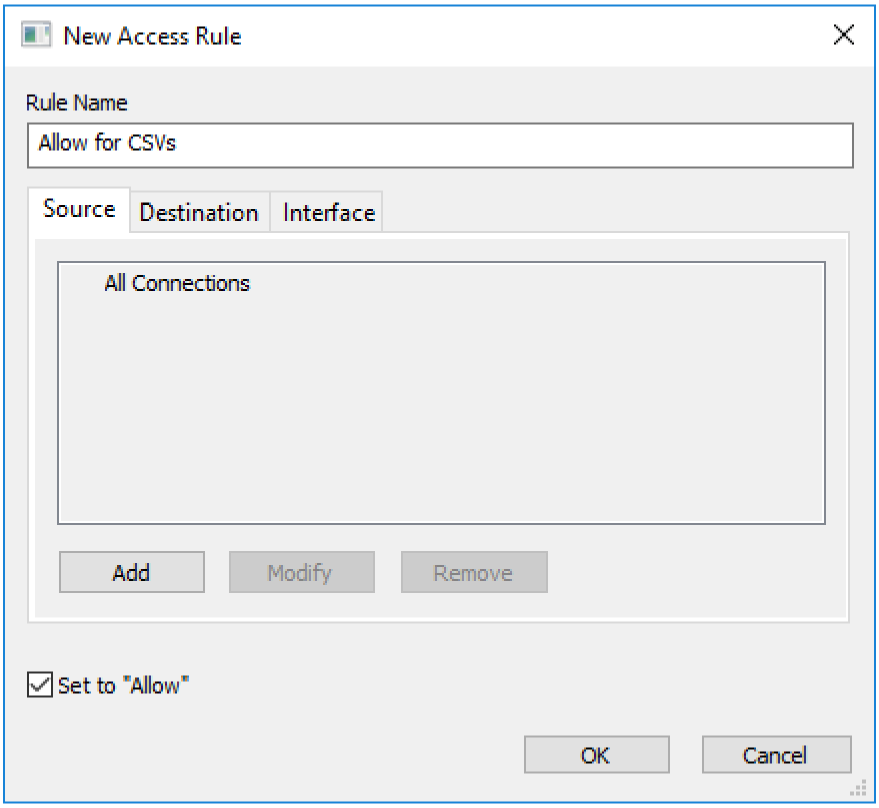
If a target should be accessed from certain hosts and through certain network interfaces only, a separate rule can be created.

1. Right-click on the Access Rights pane and select Add Rule.



#	Rule Name	Source	Destination	Interface	Action
1	allow for partner(s) of iqn.2...	iqn.2008-08.com.starwindsoftware:sw-sed-02-witness	iqn.2008-08.com.starwindsoftware:sw-sed-01-witness	All Interfaces	✓ Allow
2	allow for partner(s) of iqn.2...	iqn.2008-08.com.starwindsoftware:sw-sed-02-csv2	iqn.2008-08.com.starwindsoftware:sw-sed-01-csv2	All Interfaces	✓ Allow
3	allow for partner(s) of iqn.2...	iqn.2008-08.com.starwindsoftware:sw-sed-02-csv1	iqn.2008-08.com.starwindsoftware:sw-sed-01-csv1	All Interfaces	✓ Allow
	DefaultAccessPolicy	**All Connections**	**All Targets**	**All Interfaces**	✓ **Allow**

2. In the popup window, type in the rule name and select the Set to “Allow” checkbox.



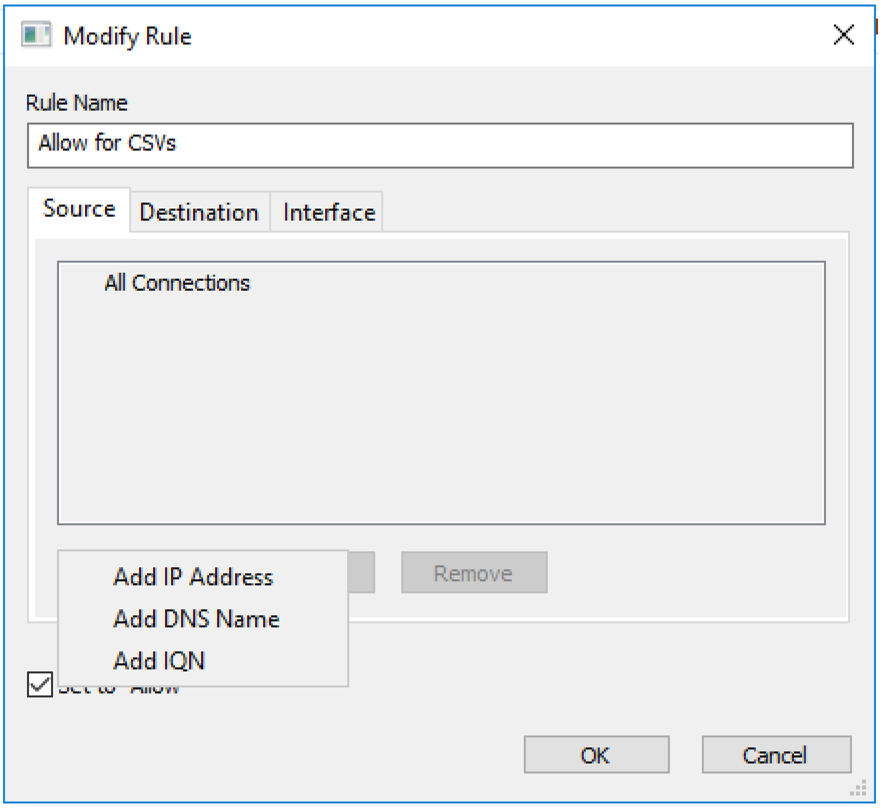
New Access Rule

Rule Name: Allow for CSVs

Source tab: All Connections

☑ Set to "Allow"

3. In the Source tab, where the source is a server that connects to a StarWind target, click Add and choose the required option.



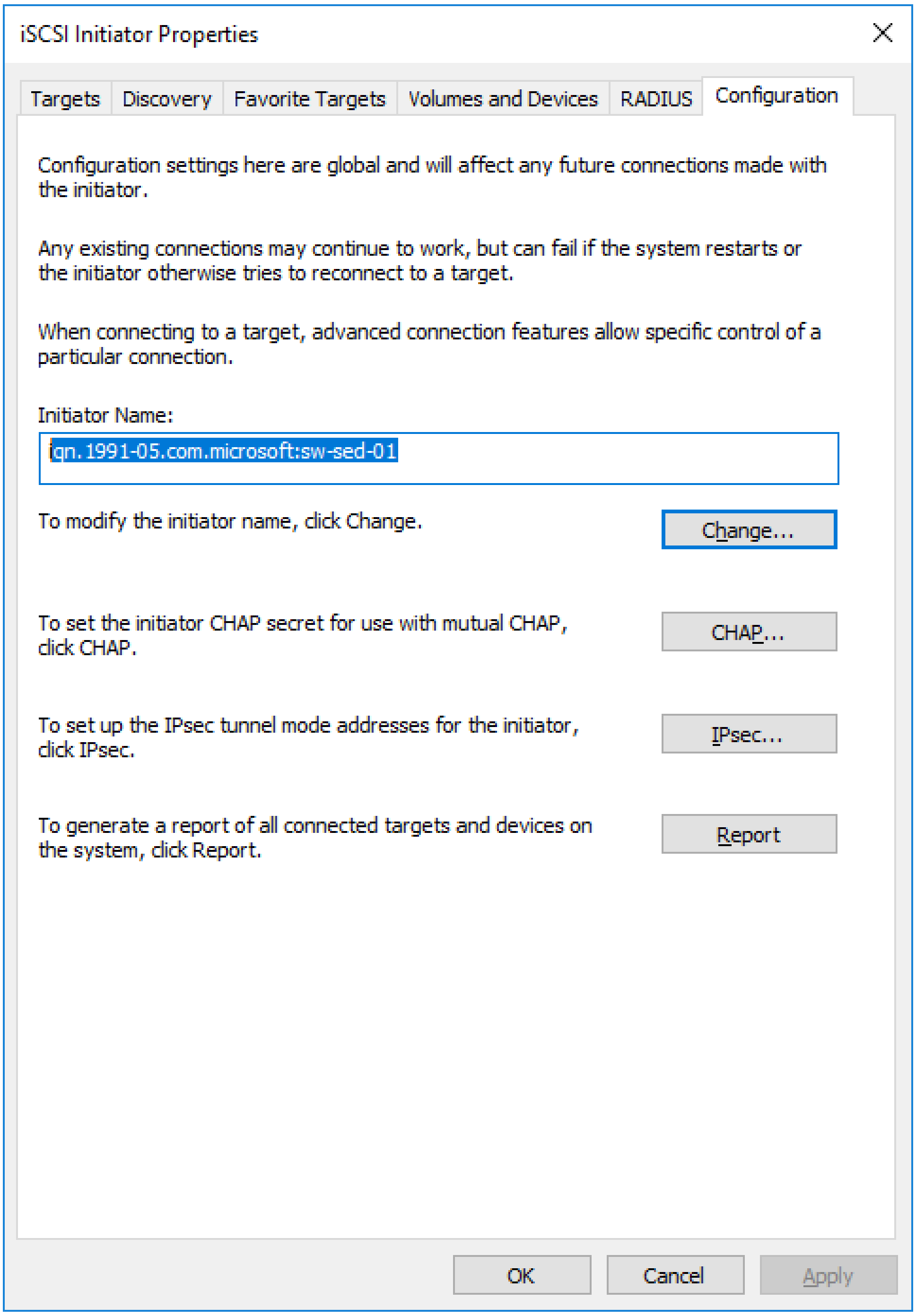
Modify Rule

Rule Name: Allow for CSVs

Source tab: All Connections

☑ Set to "Allow"

NOTE: Here, server IQNs will be used for configuring the connection source. To obtain the server IQN, open Microsoft iSCSI Initiator and navigate to the Configuration tab:



Configuration settings here are global and will affect any future connections made with the initiator.

Any existing connections may continue to work, but can fail if the system restarts or the initiator otherwise tries to reconnect to a target.

When connecting to a target, advanced connection features allow specific control of a particular connection.

Initiator Name:

iqn.1991-05.com.microsoft:sw-sed-01

To modify the initiator name, click Change.

To set the initiator CHAP secret for use with mutual CHAP, click CHAP.

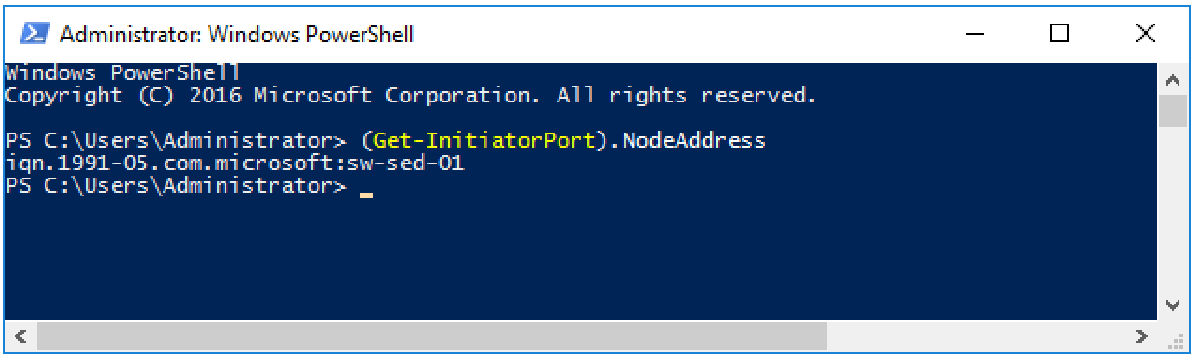
To set up the IPsec tunnel mode addresses for the initiator, click IPsec.

To generate a report of all connected targets and devices on the system, click Report.

Alternatively, run the following PowerShell command:

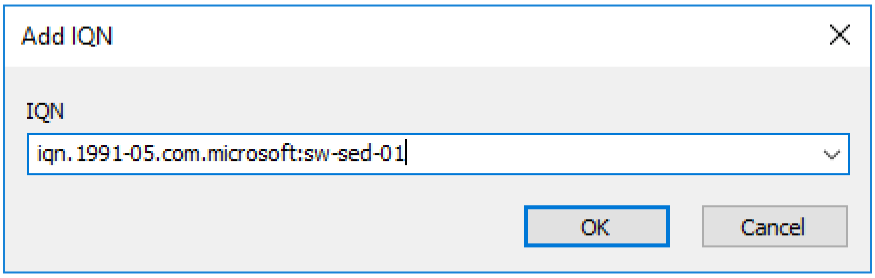
```
(Get-InitiatorPort).NodeAddress
```

```
(Get-InitiatorPort).NodeAddress
```



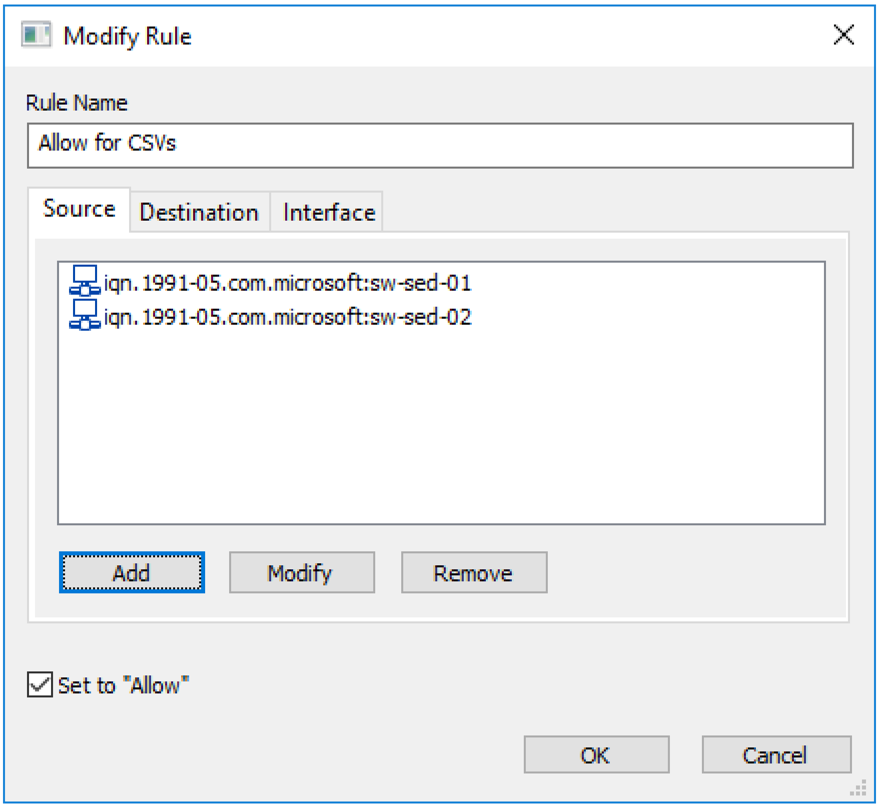
```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> (Get-InitiatorPort).NodeAddress
iqn.1991-05.com.microsoft:sw-sed-01
PS C:\Users\Administrator> _
```

4. Type in the IQN name of the server to be allowed to connect to the StarWind VSAN targets.



IQN: iqn.1991-05.com.microsoft:sw-sed-01

5. Perform the same action for each of the servers that are expected to connect to the StarWind target. The Source tab will look similar to the screenshot below:

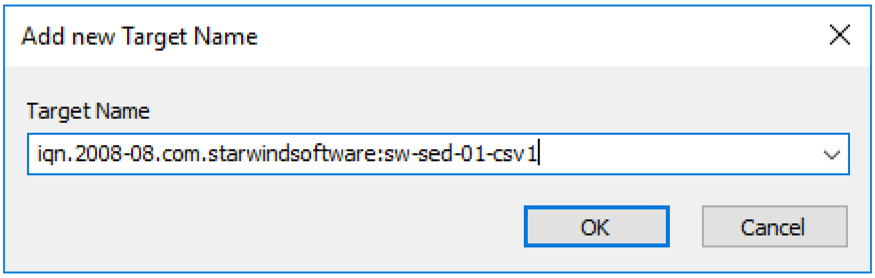


Rule Name: Allow for CSVs

iqn.1991-05.com.microsoft:sw-sed-01
iqn.1991-05.com.microsoft:sw-sed-02

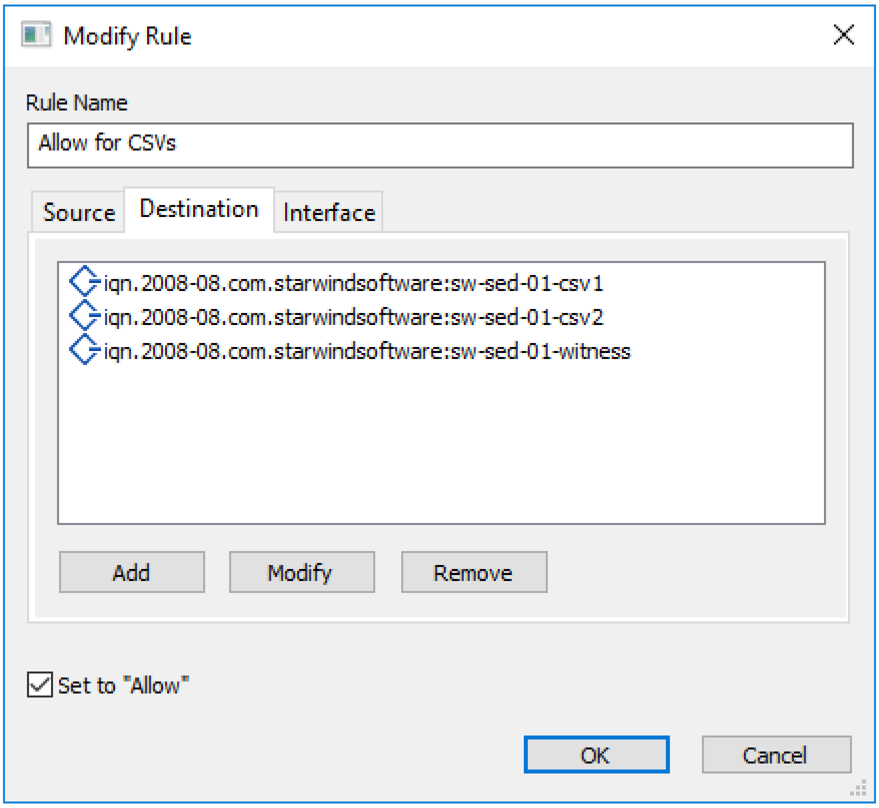
☑ Set to "Allow"

6. Open the Destination tab, press Add to select the target on the StarWind VSAN server allowed to be connected to, and press OK.


Add new Target Name

Target Name: iqn.2008-08.com.starwindsoftware:sw-sed-01-csv1

Note: Multiple targets can be configured within the same ACL rule. Also, all targets are allowed to be connected to if no target is set explicitly.

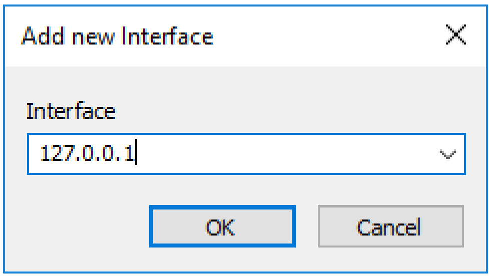

Modify Rule

Rule Name: Allow for CSVs

iqn.2008-08.com.starwindsoftware:sw-sed-01-csv1
iqn.2008-08.com.starwindsoftware:sw-sed-01-csv2
iqn.2008-08.com.starwindsoftware:sw-sed-01-witness

☑ Set to "Allow"

7. In the Interface tab, specify the IP address(es) allowed to accept connections to the StarWind VSAN target. By default, all interfaces are allowed to be used in the newly created rule. If only dedicated interfaces are intended to be used for connecting to the targets, select the required interfaces from the dropdown list in the popup window:

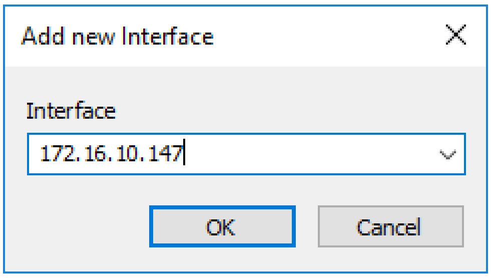


Add new Interface

Interface: 127.0.0.1

NOTE: The loopback address 127.0.0.1 should be added for the Hyper-V hyperconverged scenario. For any other configuration scenario, this IP address is not required.

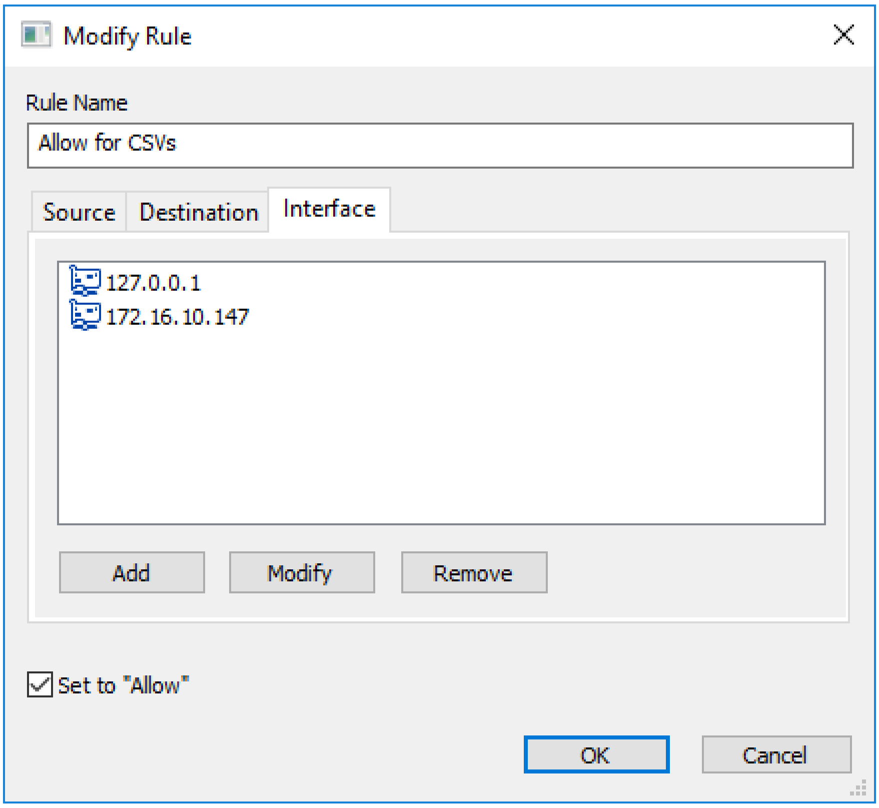
8. Add the IP address of the StarWind VSAN server interface intended for data exchange:



Add new Interface

Interface: 172.16.10.147

9. When all required IP addresses are added to the rule, press OK to confirm the rule creation.



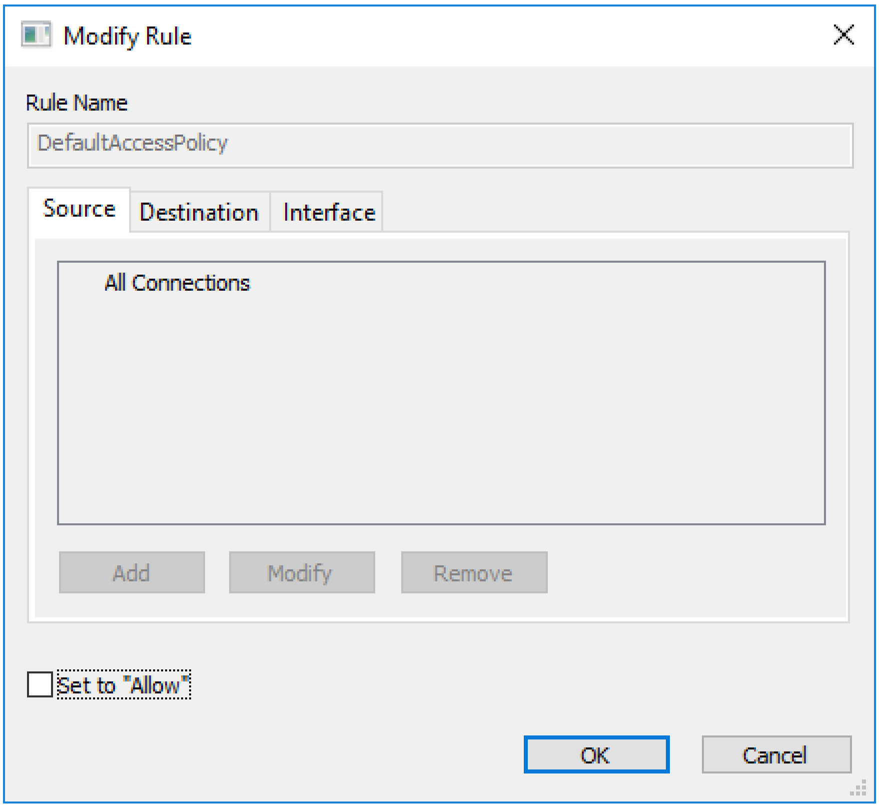
Modify Rule

Rule Name: Allow for CSVs

Interface:
127.0.0.1
172.16.10.147

☑ Set to "Allow"

10. Once all required rules are configured with the Allow checkbox selected, all other connections can be restricted. To perform this, double-click the DefaultAccessPolicy rule and uncheck the Set to “Allow” checkbox. This will block all connections that are not explicitly configured in the rules preceding DefaultAccessPolicy. Press OK to confirm.


Modify Rule

Rule Name: DefaultAccessPolicy

All Connections

□ Set to "Allow"

11. To apply the newly configured rules to all iSCSI sessions and make sure that only necessary sessions are connected, restart the StarWind VSAN service on the node where changes have been introduced. If an HA setup is used, make sure that similar rules are configured on the partner server(s).

Contacts

US Headquarters	EMEA and APAC
☎ +1 617 829 44 95	☎ +44 2037 691 857 (United Kingdom)
+1 617 507 58 45	☎ +49 800 100 68 26 (Germany)
+1 866 790 26 46	☎ +34 629 03 07 17 (Spain and Portugal)
	☎ +33 788 60 30 06 (France)

Customer Support Portal:	https://www.starwind.com/support
Support Forum:	https://www.starwind.com/forums
Sales:	sales@starwind.com
General Information:	info@starwind.com

StarWind

StarWind Software, Inc. 100 Cummings Center Suite 224-C Beverly MA 01915, USA
www.starwind.com