Firewall configuration guideline for PcVue

Last update :	April 30, 2021
Revision :	1.0/15.1
Content :	This document describes the firewall rules commonly required in the context of PcVue projects.

The last revision of the technical content accommodates changes in PcVue 15.1. Unless otherwise stated, this document is valid for releases made publicly available since.

PcVue® Solutions

Content

Introduction

1. Purpose

The aim of this document is to provide the commonly used TCP and UDP ports and is designed as a guideline for firewall configuration.

It can be used by PcVue application designers and system administrators to configure the local firewall of computers running PcVue as well as firewalls used to control network perimeters and interconnections.
Depending on the context, in particular the regulations in force and practices in place, it is up to the system administrator to determine the relevant network control measures, including the applicable firewall rules.
In all cases, ARC Informatique recommends users to take defensive measures to minimize the network exposure of the system.

2. How to use this document

This guideline provides tables describing typical firewall rules for the most commonly used interfaces based on TCP and UDP in PcVue.
These rules are organized according to the involved PcVue roles and interfaces. When configuring the local firewall of a PcVue station, several rules from a variety of subsets may be applicable depending on the project design and network architecture. For example rules from the Networking and Data Acquisition Server subsets.

Each table includes the necessary parameters to configure individual firewall rules:

Parameter name	Description
Interface name	The name of the interface or component involved in PcVue
Installed	Indicates how the component managing the interface is installed: - Always: The component is always installed, - Option: The component can be installed optionally, Add-on: The component is part of an external Add-on with a dedicated installation procedure.
Activated	If installed, indicates: - Always: The interface is always active, Config: The interface is activated/deactivated depending on the project configuration.
Rule type	Indicates if it is a rule for the inbound or outbound traffic
Process	The process involved – Useful for rules defined for the host firewall.
Protocol	Transport layer (TCP or UDP), and the Application layer protocol if it is well-known by most firewalls on the market
Local port	The local port involved
Remote port	The remote port involved

In practice, it is recommended to set 2 additional parameters whenever possible:

- Local address: In case of multiple attachments to the network, only the address used by the PcVue process for the corresponding interface should be configured for a particular network flow,
- Remote address: Only the list of identified and authorized remote hosts (application or device) for a particular network flow should be configured.

Local and Remote address parameters are always specific to the target system and therefore not documented here. You will find indications about the host where a rule shall be set and what are the typical legitimate remote hosts.

For some interfaces, the value -*local*- is indicated as Rule type. These rules correspond to IP-based local inter-process exchanges on the host and need a dedicated port. Non-local traffic on this port can be blocked.

Default ports are indicated in the tables and whether they can be modified by configuration or not. Configurable ports are marked with a '*' all along this document.

3. Default rules

This document assumes that all inbound and outbound traffic is disabled by default.

The base configuration of firewalls varies, industrial firewalls may already have rules for industrial protocols, Microsoft Windows firewall already have rules for RDP… In all cases, the information in this document shall be adapted to the specific target system and used responsibly by the administrator.

In particular, on the first launch of the PcVue application, Microsoft Windows® may have automatically added rules allowing all inbound/outbound traffic to/from the sv32.exe process. If you are using the Microsoft Windows firewall, you can refer to this article for more information: https://docs.microsoft.com/windows/security/threat-protection/windows-firewall/best-practices-configuring

Note that Microsoft recommends having the proper firewall rules in place before a user first launches the application.

Rule subsets

4. Networking

This section details the list of applicable rules for client/server or distributed PcVue systems taking advantage of the Networking capabilities to exchange data between stations.

Interface name	Installed	Activated	Rule type	Process	Protocol	Local port	Remote port
Networking – Client node(1)	Always	Config	outbound	sv32.exe	TCP	any	1981*(3)
Networking – Server node(2)	Always	Config	inbound	sv32.exe	TCP	1981*(1)	any
Networking – RDS Client	Always	Config	*- Please refer to Microsoft® documentation -*				
Networking – RDS Server	Always	Config	*- Please refer to Microsoft® documentation -*				

(1) This rule applies to all the client stations of the project and to all server stations belonging to an association (redundancy), as a passive server requires client connections to active servers.

(2) This rule applies to all server stations of the project, whether they belong to an association or not.

(3) The port number can be modified on a per node basis in the PcVue configuration. Further details are provided in the following sections of the online help:

- The Application Explorer > Communication > Networked Application
- Deployment > Deploying desktop application

5. Data Acquisition Server

This section details the list of applicable rules for interfaces used for data acquisition. Only the most common drivers are listed here.
These rules are given for a single remote host (PLC, controller, data source host…). Some interfaces may be used with several hosts, rules will have to be adjusted according to the system configuration (remote address, identical or different remote port…).

Interface name	Installed	Activated	Rule type	Process	Protocol	Local port	Remote port
BACnet/IP Client	Always	Config	outbound	sv32.exe	UDP	any	47808*
			inbound	sv32.exe	UDP	47808*	any
DDE Client	Always	Config	*-local-*	*-NA-*	*-COM-*	*-NA-*	*-NA-*
DNP3 Client	Always	Config	outbound	sv32.exe	TCP	any	20000*
	Always	Config	inbound	sv32.exe	TCP	20000*	any
Ethernet/IP	Add-on	Config	outbound	sv32.exe	TCP	any	44818
			outbound	sv32.exe	UDP	any	2222
			inbound	sv32.exe	UDP	2222	any
Hilscher-NL	Always	Config	outbound	sv32.exe	TCP	any	1099
IEC 60870-5-101 Master TCP profile	Always	Config	outbound	sv32.exe	TCP	any	2404*
IEC 60870-5-101 Master UDP profile	Always	Config	outbound	sv32.exe	UDP	any	2404*
	Always	Config	inbound	sv32.exe	UDP	2405*(1)	any
IEC 60870-5-104 Client	Always	Config	outbound	sv32.exe	TCP	any	2404*
IEC 61850 Client	Always	Config	outbound	sv32.exe	TCP	any	102*
IP-CITILOG	Always	Config	outbound	sv32.exe	TCP	any	33000*
IP-ISO-S7	Always	Config	outbound	sv32.exe	TCP	any	102
IP-ME100	Always	Config	outbound	sv32.exe	TCP	any	47001
IP-MEWTOCOL7	Always	Config	outbound	sv32.exe	TCP	any	5800*
IP-MOXA	Always	Config	outbound	sv32.exe	TCP	any	502*
IP-OPENWEBNET	Always	Config	outbound	sv32.exe	TCP	any	20000
IP-POSM	Always	Config	outbound	sv32.exe	TCP	any	50000*
IP-SAIA	Always	Config	outbound	sv32.exe	TCP	any	5050*
IP-SRTP	Always	Config	outbound	sv32.exe	TCP	any	18245
IP-XGT	Always	Config	outbound	sv32.exe	TCP	any	1099*

Interface name	Installed	Activated	Rule type	Process	Protocol	Local port	Remote port
KNX	Add-on	Config	outbound	falcon.exe	UDP	any	3671*
			inbound	falcon.exe	UDP	3671*	any
LNS	Always	Config	inbound	sv32.exe	UDP	1629	1628
			-local-	sv32.exe	TCP	6001, 6002	any
LoRa Gateway	Add-on	Config	outbound	sv32.exe	TCP	any	1978*
			inbound	sv32.exe	TCP	1978*	any
MEWTOCOLCOM-IP	Always	Config	outbound	sv32.exe	UDP	any	5800*
MITSU TCP/IP	Always	Config	outbound	sv32.exe	TCP	any	3000*
MOXA-IOLOGIK	Always	Config	outbound	sv32.exe	TCP	any	9500
			inbound	sv32.exe	TCP	9900*	any
MQTT	Add-on	Config	outbound	sv32.exe	TCP	any	1883*
			inbound	sv32.exe	TCP	1883*	any
OPC DA[2]	Always	Config	*-local-*	*-NA-*	*-COM-*	*-NA-*	*-NA-*
OPC UA Gateway Client	Add-on	Config	outbound	uagateway.exe	TCP	any	48050*
OPC XML-DA	Always	Config	outbound	sv32.exe	TCP (HTTP/SOAP)	any	80/443*
S7-IP-MASTER	Always	Config	outbound	sv32.exe	TCP	any	2000*, 2001*
SAIA Ether S-Bus	Always	Config	outbound	sv32.exe	TCP	any	5050*
SNMP Manager	Always	Config	outbound	sv32.exe	UDP	any	161*
			inbound	sv32.exe	UDP	162*	any
TWINCAT	Always	Config	outbound	sv32.exe	TCP	any	801
XBUS-IP-MASTER	Always	Config	outbound	sv32.exe	TCP	any	502*
YOKOGAWA TCP/IP	Always	Config	outbound	sv32.exe	TCP	any	12289

[1] When using the UDP profile, distinct listening ports have to be configured for each IEC 60870-5-101 device.

[2] In case of remote OPC server, a suitable DCOM configuration is required. Only the rule between PcVue and the OPC server are described here, additional rules may be necessary between the OPC server and the data source (e.g.: device).

6. Data Server

This section details the list of applicable rules for interfaces used to expose data to third-party applications.

Interface name	Installed	Activated	Rule type	Process	Protocol	Local port	Remote port
BACnet/IP Server	Add-on	Config	Inbound	sv32.exe	UDP	47808*	any
			outbound	sv32.exe	UDP	any	47808*
DDE Server	Always	Always	*-local-*	*-NA-*	*-COM-*	*-NA-*	*-NA-*
IEC 60870-5-104 Outstation	Always	Config	inbound	sv32.exe	TCP	2404*	any
ICCP/TASE.2	Add-on	Config	inbound	sv32.exe	TCP	102*	any
	Add-on	Config	outbound	sv32.exe	TCP	any	102*
OPC DA Classic[1]	Always	Config	*-local-*	*-NA-*	*-COM-*	*-NA-*	*-NA-*
OPC UA Gateway Server	Add-on	Config	inbound	uagateway.exe	TCP	48050*	any
SNMP Agent[2]	Add-on	Config	inbound	snmp.exe	UDP	161	any
			outbound	snmp.exe	UDP	any	162
XBUS-IP-SLAVE	Always	Config	inbound	sv32.exe	TCP	502*	any

[1] In case of a remote OPC client, a suitable DCOM configuration is required.

[2] Based on the Microsoft Windows SNMP Agent service. Please refer to the Microsoft Windows documentation.

7. Web and Mobile Server

This section details the list of applicable rules for interfaces used as part of the Web & Mobile extensions. These interfaces are required to deploy any of the following Web & Mobile client:

- Web Service Toolkit
- WebVue
- Web Scheduler
- Instant Messaging
- TouchVue & SnapVue mobile apps

These clients require the deployment of a Core back end and may need the Instant Messaging and Geolocation back ends.

Depending on the architecture, some rules may be unnecessary, as the traffic will remain local. This is the case when the Web Server and the Back ends are deployed on the same host computer.

Further details related to recommended architecture and network segmentation are provided in the following sections of the online help:

- Deployment > Architecture examples > Web based architectures
- Deployment > Deploying server applications > Deploying the Web Server and the Web & Mobile back end

Interface name	Installed	Activated	Rule type	Process	Protocol	Local port	Remote port
Web Server Web interface[1]	Option	Always	inbound	IIS	TCP (HTTPS)	443	any
Web Server Back ends interface[2]	Option[3]	Config	inbound	IIS	TCP	8091*	any
	Option[3]	Config	outbound	IIS	TCP	any	8090*
	Option[4]	Config	outbound	IIS	TCP	any	8811*
	Option[5]	Config	outbound	IIS	TCP	any	8810*
Core back end[6]	Option	Config	inbound	sv32.exe	TCP	8090*	any
	Option	Config	outbound	sv32.exe	TCP	any	8091*
Instant Messaging back end[6]	Option	Config	inbound	sv32.exe	TCP	8810*	any
Geolocation back end[6]	Option	Config	Inbound	sv32.exe	TCP	8811*	any

[1] The port number can be configured with Web Deployment Console that is used to configure IIS bindings. Further details are provided in the following section of the online help: Deployment > Deploying server applications > Deploying the Web Server and the Web & Mobile back end > Using the Web Deployment Console. These rules usually already exists in the firewall configuration and just need to be activated.

[2] Only required on the computer hosting the IIS Web Server.

[3] Required for communication with the computer hosting the Core back end.

[4] Required for communication with the computer hosting the Geolocation back end.

[5] Required for communication with the computer hosting the Instant Messaging back end.

[6] Only required on the computer hosting the corresponding Back end, for communication with the IIS Web Server.

8. Other PcVue features

This section describes additional features that may be used in a PcVue system.

Interface name	Installed	Activated	Rule type	Process	Protocol	Local port	Remote port
Actions - Emails[1]	Always	Config	outbound	sv32.exe	TCP (SMTP)	any	587*
SCADA Basic - FTP	Always	Config	outbound	sv32.exe	TCP (FTP)	any	21*
Map Servers	Always	Config	*- Please refer to the Map Provider documentation -*				
Configuration tools	Always	Always	*-local-*	*-NA-*	*-COM-*	*-NA-*	*-NA-*

[1] The rule configuration depends on the email server requirements as reflected in the PcVue project configuration. Further details are provided in the following section of the online help: The Application Explorer > Actions > Message profiles and templates > Configuring an e-mail profile.

9. Other system level dependencies

These functions may be used par PcVue depending on the system architecture and project configuration details. They use built-in features of the operating system.

Interface name	Installed	Activated	Rule type	Process	Protocol	Local port	Remote port
Active Directory	Always	Config	*- Please refer to Microsoft® documentation*[1] -				
Printers	Always	Config	*- Please refer to Microsoft® documentation*[2] -				
Version's Management	Always	Config	*- Please refer to Microsoft® documentation*[3] -				
HDS[4]	Always	Config	*-local-*	*-NA-*	*-COM-*	*-NA-*	*-NA-*
Sv DbConnect[4][5] Sql connections	Always	Config	*- Please refer to the RDBMS® and ADO.Net providers documentation -*				

[1] Please refer to https://docs.microsoft.com/troubleshoot/windows-server/identity/config-firewall-for-ad-domains-and-trusts.
[2] Please refer to https://docs.microsoft.com/windows-hardware/drivers/print/installing-tcp-ip-printers.
[3] Based on SMB, please refer to https://docs.microsoft.com/troubleshoot/windows-server/networking/direct-hosting-of-smb-over-tcpip.
[4] SQL Server documentation: https://docs.microsoft.com/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access
[5] Oracle documentation: https://docs.oracle.com/en/database/oracle/oracle-database/20/dbseg/keeping-your-oracle-database-secure.html

Appendix-A: OPC and firewalls

It is quite common to have both the OPC server and the OPC client on the same computer. In such a configuration, the traffic between the server and the clients remains local to the host.

With certain network architectures, it could be necessary to have the OPC server and OPC clients on different hosts, which require configuring Distributed Component Object Model (DCOM). This technology uses Remote Procedure Call (RPC) dynamic port allocation.
If you are using PcVue as a remote OPC server, you must change its permissions as you would with any other OPC server (Component Services\Computers\My Computer\DCOM Config). PcVue appears in the DCOM configuration as *SV Application*.

The following documentation and articles indicates how to enable and configure DCOM communication:

- https://technet.microsoft.com/library/cc771387(v=ws.11).aspx
- https://docs.microsoft.com/troubleshoot/windows-server/networking/configure-rpc-dynamic-port-allocation-with-firewalls

Accordingly, the default inbound ports used are:

- TCP 135, for the RPC Endpoint Mapper
- random port number between TCP 49152 and 65535

These ports are used by all the applications needing DCOM configuration and RPC calls, enabling or disabling them will also have an impact on all these applications.
As an alternative, OPC Tunneller products exist on the market to avoid the need for DCOM configuration.

Appendix-B: Useful links

Service overview and network port requirements for Windows:
https://docs.microsoft.com/troubleshoot/windows-server/networking/service-overview-and-network-port-requirements

Best practices for configuring Windows Defender Firewall
https://docs.microsoft.com/windows/security/threat-protection/windows-firewall/best-practices-configuring

CISA - Recommended practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies
https://us-cert.cisa.gov/ics/Abstract-Defense-Depth-RP

ANSSI - Recommendations for the definition of a firewall configuration policy (in French):
https://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-definition-dune-politique-de-filtrage-reseau-dun-pare-feu/
https://www.ssi.gouv.fr/entreprise/guide/recommandations-et-methodologie-pour-le-nettoyage-dune-politique-de-filtrage-reseau-dun-pare-feu/

ARC Informatique

Headquarters and Paris offices
2 avenue de la Cristallerie
92310 Sèvres - France

tel + 33 1 41 14 36 00
fax + 33 1 46 23 86 02
hotline +33 1 41 14 36 25
arcnews@arcinfo.com
www.pcvuesolutions.com

ARC Informatique
Private limited company
capitalized
at 1 250 000 €
RCS Nanterre B 320 695 356
APE 5829C
SIREN 320 695 356
VAT N°FR 19320695356

Firewall configuration guideline for PcVue

ISO 9001 and ISO 14001 certified

We would love to hear your thoughts and suggestions
so we can improve this document
Contact us at team-doc@pcvuesolutions.com