



Firewall Requirements

Version 5.10

Manual



Document: Dokument1



Created: 2020-07-29



Last changes: 2020-07-29

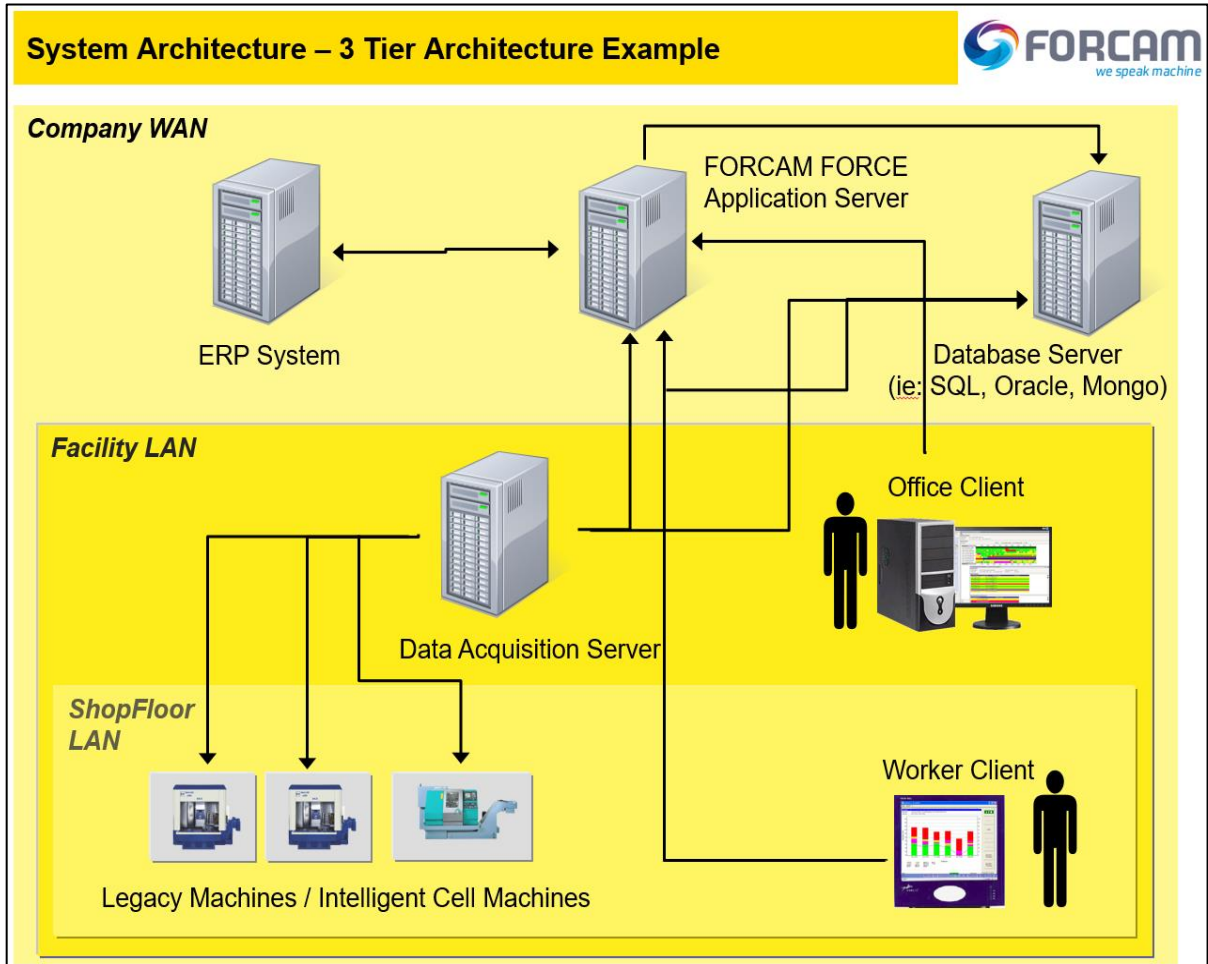



Author: AEgilmez

Content

1	System Architecture	3
2	IT Infrastructure Isolation	4
3	DNC Server Isolation (i.e.: on DCU/DACQ Server).....	6
4	Tracing Acquisition Server Isolation (i.e. on DCU/DACQ Server).....	7
5	Data Acquisition Server (DCU/DACQ) Isolation	9
6	Shop Floor Isolation	10
7	External Access	13
8	History of Changes	14

1 System Architecture



 All ports requested are to allow return traffic.

2 IT Infrastructure Isolation

Source	Description	Destination	Port	Protocol	Comment
Office PCs	Access to FORCAM FORCE™ Office Client	Forcam Application Server	19080	TCP	Configure in server.xml
	Access to FORCAM FORCE™ Workbench	Forcam Application Server	15080	TCP	Configure in server.xml
	Access to FORCAM FORCE™ MDESimulator	Forcam Application Server	16080	TCP	Configure in server.xml
	Access to FORCAM FORCE™ Shop Floor Terminal	Forcam Application Server	11080	TCP	Configure in server.xml
	Access to FORCAM FORCE™ Detailed Scheduler	Forcam Application Server	21080	TCP	Configure in server.xml
	Access to FORCAM FORCE™ webservices	Forcam Application Server	24080	TCP	Configure in server.xml
	Access to FORCAM FORCE™ Authorization	Forcam Application Server	25080	TCP	Configure in server.xml
Office PCs (secured)	Access to FORCAM FORCE™ Office Client	Forcam Application Server	19443	TCP	Configure in server.xml
	Access to FORCAM FORCE™ Workbench	Forcam Application Server	15443	TCP	Configure in server.xml
	Access to FORCAM FORCE™ MDESimulator	Forcam Application Server	16443	TCP	Configure in server.xml
	Access to FORCAM FORCE™ Shop Floor Terminal	Forcam Application Server	11443	TCP	Configure in server.xml
	Access to FORCAM FORCE™ Detailed Scheduler	Forcam Application Server	21443	TCP	Configure in server.xml
	Access to FORCAM FORCE™ webservices	Forcam Application Server	24443	TCP	Configure in server.xml
	Access to FORCAM FORCE™ Authorization (prefer)	Forcam Application Server	25443	TCP	Configure in server.xml

Source	Description	Destination	Port	Protocol	Comment
Application Server	SQL Server database connections	Forcam Database Server	1433	TCP	Database configuration
	Mongo connections	Forcam Mongo Server	27017 or 27024 or 37028	TCP	Configure on Mongo install
	Mongo Apache Drill component	Forcam Mongo Server	2181, 31010	TCP	configure in tool install
	Emailing reports and alerts (AutoReporting)	Company Mail Server	25	TCP	Configure in context.xml
	Access to ActiveMQ	Forcam Application Server	61616	TCP	If seperated, not likely
	Access to artifactory	Forcam Application Server	8081	TCP	If seperated, not likely
	Ignite	Forcam Application Runtime Ignite	48100, 48500	TCP	Configure in context.xml
	http/remote/runtime/server/port	Forcam Application Runtime	10080	TCP	Configure in context.xml
	rmi/remote/server/port	Forcam Application Runtime	1199	TCP	Configure in context.xml
	rmi/exporter/server/port	Forcam Application Runtime	1299	TCP	Configure in context.xml
	Detailed Scheduler RMI	Forcam Application Server	1998	TCP	Configure in context.xml

3 DNC Server Isolation (i.e.: on DCU/DACQ Server)

Source	Description	Destination	Port	Protocol	Comment
DNC Server	SQL Server database connections	Forcam Database Server	1433	TCP	Database configuration
	ActiveMQ	Forcam Application Server	61616	TCP	Activemq configuration
	Ignite	Forcam Application Runtime Ignite	48100, 48500- 48520	TCP	Configure in context.xml
	http/remote/runtime/server/port	Forcam Application Runtime	10080	TCP	Configure in context.xml
	rmi/remote/server/port	Forcam Application Runtime	1199	TCP	Configure in context.xml
	rmi/exporter/server/port	Forcam Application Runtime	1299	TCP	Configure in context.xml
	ffdnc WorkBench Genral Configuration	Forcam Application Server	14080- 14084	TCP	Configure in workbench
	Machine Access	Machines...	Varies by machine	TCP	See list below
Application Server	ffdnc Java JMX remote access	Forcam DNC Server	8092	TCP	Configure on install
	ffdnc server.xml access	Forcam DNC Server	14005, 14009, 14080, 14443	TCP	Configure in server.xml
	ffdnc WorkBench Genral Configuration	Forcam DNC Server	14080- 14084	TCP	Configure in workbench

4 Tracing Acquisition Server Isolation (i.e. on DCU/DACQ Server)

Source	Description	Destination	Port	Protocol	Comment
Tracing Server	SQL Server database connections	Forcam Database Server	1433	TCP	database configuration
	Mongo DB	Forcam Mongo Database Server	27017 or 27024 or 37028	TCP	configure in context.xml
	ActiveMQ	Forcam Application Server	61616	TCP	ActiveMQ configuration
	Artifactory	Forcam Artifactory	8081	TCP	configure in context.xml
	Ignite	Forcam Application Runtime Ignite	48100, 48506, 48507	TCP	configure in context.xml
	http/remote/runtime/server/port	Forcam Application Runtime	10080	TCP	configure in context.xml
	influxdb/db/port	Influx DB Server	25086	TCP	configure in context.xml
	Emailing	Company Mail Server	25	TCP	configure in context.xml
	Machine Access	Machines...	Varies by machine	TCP	See list below. Is this needed?

Source	Description	Destination	Port	Protocol	Comment
Application Server	ffacquisition Java JMX remote access	Forcam Tracing Server	18091	TCP	configure on install
	ffacquisition server.xml access	Forcam Tracing Server	17005, 17009, 17080, 17443	TCP	configure in server.xml
	ffprocessing Java JMX remote access	Forcam Tracing Server	18095	TCP	configure on install
	ffprocessng server.xml access	Forcam Tracing Server	18005, 18009, 18080, 18443	TCP	configure in server.xml

5 Data Acquisition Server (DCU/DACQ) Isolation

Source	Description	Destination	Port	Protocol	Comment
Data Acquisition Server	SQL Server database connections	Forcam Database Server	1433	TCP	Database configuration
	ActiveMQ	Forcam Application Server	61616	TCP	Activemq configuration
	http/remote/runtime/server/port	Forcam Application Runtime	10080	TCP	Configure in server.xml/javis.ini
	rmi/remote/server/port	Forcam Application Runtime	1199	TCP	Configure in context.xml
	rmi/exporter/server/port	Forcam Application Runtime	1299	TCP	Configure in context.xml
	Internal DACQ to DCU on server	Forcam Data Acquisition Server	8765	TCP	Only if separate services
	Remote Restart of DACQ-scripting	Forcam Data Acquisition Server	8775	TCP	

6 Shop Floor Isolation

Source	Description	Destination	Port	Protocol	Comment
Shop Floor Terminals	Access to FORCAM FORCE™ Shop Floor Terminal	Forcam Application Server	11080	TCP	Configure in server.xml
	Access to FORCAM FORCE™ Shop Floor Terminal	Forcam Application Server	11443	TCP	Configure in server.xml
Data Acquisition Server	Allen Bradley/Rockwell (EtherNet/IP™, new)	Machines with ...	44818	TCP/UDP	
	Allen Bradley/Rockwell (PLC5E, SLC5/05, old)	Machines with ...	2222	TCP/UDP	
	Allen Bradley/Rockwell (Peer to Peer)	Machines with ...	4000	TCP/UDP	
	Fanuc FOCAS 1&2 / Ethernet	Machines with ...	8193	TCP	Configure on controller
	Fanuc CIMPLICITY i CELL	Machines with ...	8192	UDP	
	Fanuc FOCAS2/Ethernet	Machines with ...	8195	UDP	
	Fanuc Unsolicited Message Server	Machines with ...	8196	TCP	
	Heidenhain (for newer controls, TNC640)	Machines with ...	19003	TCP	
	Heidenhain (for older controls, iTNC530)	Machines with ...	19000	TCP	
	Heidenhain (NFS)	Machines with ...	111	TCP	
	Heidenhain (SMB)	Machines with ...	445	TCP	
	Heidenhain (default)	Machines with ...	5000	TCP	
	Heidenhain (LSV2, for serial COM)	Machines with ...	9000	TCP	
	IBH-Link S5++ (IBHNet, read/write)	Machines with ...	2002	TCP	
	IBH-Link S5++ (Programming Unit - PU)	Machines with ...	10010	TCP	
	IBH-Link S5/S7 RFC1006	Machines with ...	102	TCP	
	IBH-Link S7 Standard	Machines with ...	1099	TCP	
IBH-Link S7++ (Search for IBHLink device)	Machines with ...	25383, 25384	UDP		
Makino MML	Machines with ...	8193 or 11212	TCP		

Source	Description	Destination	Port	Protocol	Comment
	MCIS-RPC	Machines with ...	3010	TCP	Host port
	MCIS-RPC	Machines with ...	3011	TCP	Machine (listening) port
	MOXA telnet communication	Machines with ...	23	TCP	
	MOXA Web UI	Machines with ...	80	TCP	
	MOXA Data port	Machines with ...	950-965	TCP	
	MOXA Command port (for transferring data)	Machines with ...	966-981	TCP	
	MOXA Data port (for transferring data)	Machines with ...	4001	TCP	
	MOXA Broadcast search	Machines with ...	4800	UDP	
	MOXA Firmware Upgrade	Machines with ...	4900	TCP	
	MQTT.fx server	Machines with ...	2783	TCP	
	MQTT (default)	Machines with ...	1883, 1885	TCP	
	MQTT (SSL/TLS)	Machines with ...	8883	TCP	
	MTConnect Agent	Machines with ...	5000, custom	TCP	Configurable
	MTConnect Adapter	Machines with ...	7878	TCP	Configurable
	Okuma THINC Listening	Machines with ...	8888	TCP	
	Omron (FINS)	Machines with ...	9600	UDP	
	OPC DA (Binary/DCOM, read)	Machines with ...	5000	TCP	
	OPC DA (Binary/DCOM, write)	Machines with ...	6000	TCP	
	OPC DA-XML	Machines with ...	80	TCP	
	OPC DA-XML (HTTPS)	Machines with ...	443	TCP	
	OPC UA (SOAP-XML)	Machines with ...	80	TCP	
	OPC UA (SOAP-XML, HTTPS)	Machines with ...	443	TCP	
	OPC UA (Binary)	Machines with ...	4840, 4843	TCP	
	OPC UA (Binary, DataFEED OPC)	Machines with ...	4980	TCP	
	OPC UA (SOAP-XML, KEPServerEX)	Machines with ...	49320	TCP	
	OPC-Server (DCOM, Service Contr. Manager)	Machines with ...	135	TCP	

Source	Description	Destination	Port	Protocol	Comment
	Siemens Control with CP (IPS7Link/RFC1006)	Machines with ...	102	TCP	
	Siemens MCIS-RPC (RPC, Host)	Machines with ...	13010	TCP	
	Siemens MCIS-RPC (RPC, Machine)	Machines with ...	3011	TCP	
	Simatic S7 IPS7LNK	Machines with ...	502, 2000	TCP	
	WAGO http access	Machines with ...	80	TCP	WAGO configuration page
	WAGO https access	Machines with ...	443	TCP	WAGO configuration page
	WAGO CodeSys Software	Machines with ...	2455	TCP	
	WAGO Controller - FORCAM I/O-Box	Machines with ...	3002	UDP	
	WAGO (Modbus, polling/send)	Machines with ...	502	UDP/TCP	

7 External Access

Source	Description	Destination	Port	Protocol	Comment
External access	Access for: 1. Customer system for support 2. Customer access GUIs 3. Cloud environment	Forcam Application Server	80, 443, 1998, 3389, custom, 10080, 10443, 11080, 11443, 15080, 15443, 16080, 16443, 19080, 19443, 21080, 21443, 24080, 24443, 25080, 25443	TCP	Customer defined Access Runtime Worker Client WorkBench MDESimulator Office Client Scheduler Webservices Authentication
		Forcam Database Server	80, 443, custom		Customer defined Access
		Forcam Data Acquisition Server	80, 443, custom		Customer defined Access
ERP System	ERP "Download" interface	Forcam Application Runtime	10080	TCP	Configure in server.xml
	ERP secured "Download" interface	Forcam Application Runtime	10443	TCP	Configure in server.xml
	ERP "Upload" interface from Application Server	ERP - System	8002	TCP	Configurable

8 History of Changes

The following table describes the changes as of release version 5.10:

Date	Changes
2019-08-08	Updated picture
2019-08-08	Added access for new interfaces like MDESimulator, Webservices, Authentication AND for 443 access
2019-08-08	Added Mongo DB access
2019-08-08	Added ActiveMQ/Artemis to top area
2019-08-08	Added ignite access
2019-08-08	Added http and other Runtime access
2019-08-08	Moved DNC isolation up so DACQ and machines together
2019-08-08	Rearranged some order in DNC but added recent findings
2019-08-08	In DACQ section, added http access
2019-08-08	Machine section added MQTT at end
2019-08-08	Expanded external access line 1 to include cloud settings
2019-08-08	Added note at begin (was requested as a column but should apply to ALL)
2019-08-26	Added Mongo component if used
2020-01-31	Added Chapter 4 Tracing Acquisition Server Isolation
2020-03-06	Added MOXA Data port in chapter 6
2020-07-29	Added Port 48520 for DNC Server in chapter 3