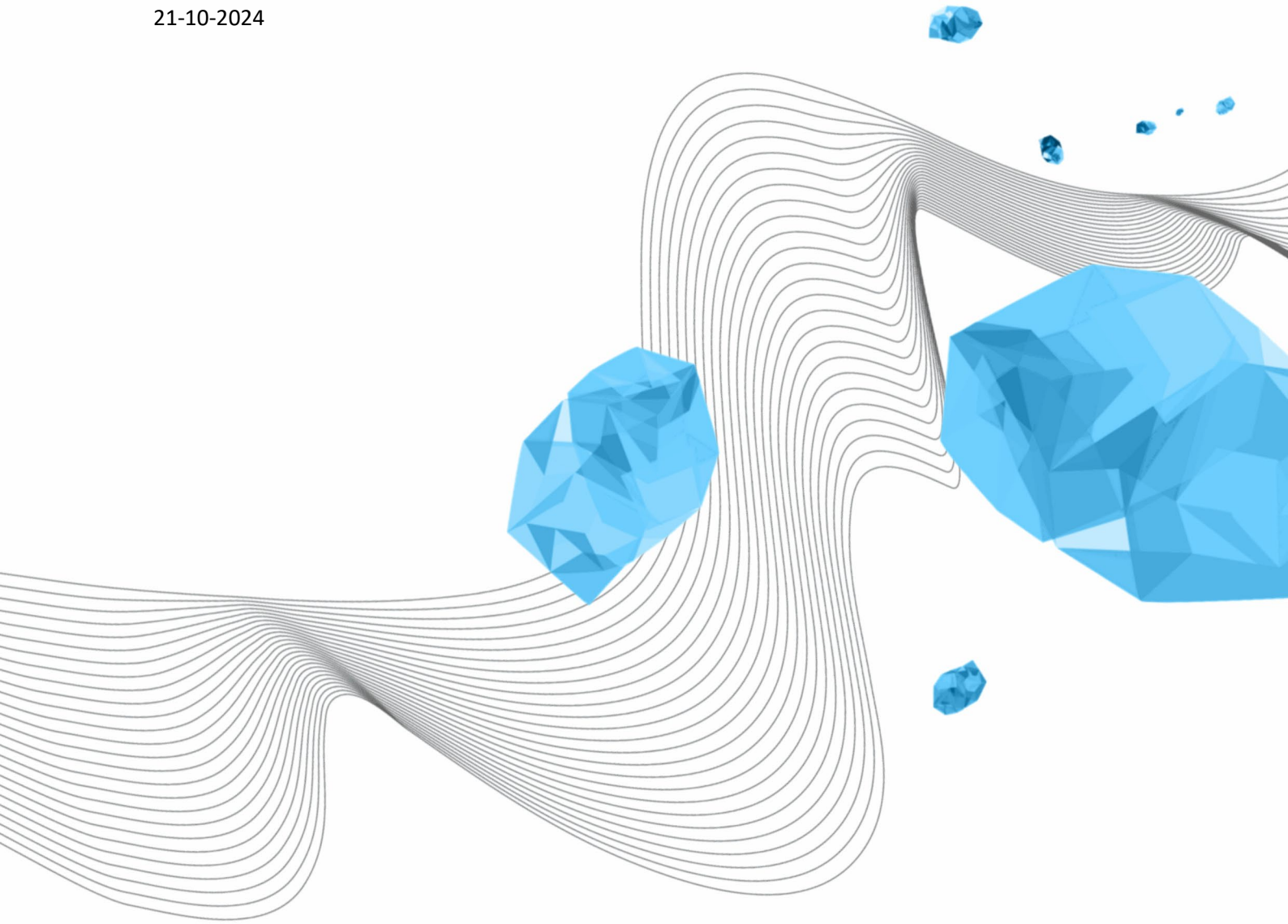
GUIDELINES ON BLOCKING NETWORKING PROTOCOLS

Peter Peters

Versie 1.7

21-10-2024



UNIVERSITY OF TWENTE.

COLOPHON

ORGANISATION
Library, ICT Services & Archive

TITLE
Guidelines on Blocking Networking Protocols

SUBJECT
Identification

PROJECT
[Project]

REFERENCE
LISA-0368

VERSION (STATUS)
1.7

DATE
21-10-2024

AUTHOR(S)
Peter Peters

DOCUMENT HISTORY

VERSION	DATE	AUTHOR(S)	REMARKS
1.0	18-11-2022	Peter Peters	Final version with change list added
1.1	1-3-2023	Peter Peters	Clarification about the networks these guidelines are implemented on. Other clarifications in the text. Removed some protocols.
1.2	17-3-2023	Peter Peters	Added some procotols
1.3	14-4-2023	Peter Peters	Added some protocols
1.4	5-1-2024	Peter Peters	Added a new category to high risk protocols (location services) Corrected some ports Added some protocols Added procedure for exceptions
1.5	19-1-2024	Peter Peters	Protocols corrected. Protocols added.
1.6	16-9-2024	Peter Peters	Protocols corrected. Protocols added.
1.7	18-10-2024	Peter Peters	Protocols added

CONTENT

1 INTRODUCTION

In the evaluations of cyber incidents within higher education, we often read that the security of the ICT network is a challenge due to the nature of these organisations. Educational institutions are open learning environments with many users, such as students, researchers, lecturers, employees and guest users. As a result, there are many different needs and wishes concerning ICT facilities. That is often the image within our university, which makes us reluctant to block protocols between the Internet and UTnet. However, our Information Security policy is based on Zero Trust, i.e. providing access to information systems and information facilities in a controlled manner. The open environment is at odds with Zero Trust, but we can take steps in a safer direction here.

Many ICT services (protocols) were designed to be used purely within a local network. Making them accessible via the Internet makes them a target for cybercriminals. Those criminals actively scan for these protocols. This blocking can happen for the entire network at the university or only parts of it.

These protocols will still be available from within the network, including eduVPN. Doing your everyday work will still be possible.

These guidelines describe the process and procedures for blocking high-risk or insecure protocols. The following groups of protocols will be considered for blocking.

1. Protocols with a high risk for abuse
2. Protocols that show high-risk vulnerabilities
3. Protocols for Operational Technology (OT)
4. Protocols that show high amplification rates when used to stage a DDoS attack

The following chapters will describe the different kinds of protocols and the specifics of the guidelines. The appendix will contain a list of all blocked protocols and the relevant part of the network it impacts.

The CISO decides on the protocols to be blocked. He will do that after consulting with the security teams and relevant administrators.

2 HIGH-RISK PROTOCOLS

Cybercriminals constantly target some protocols. Mainly because the impact, when compromised, is immense. These protocols fall into a few categories.

1. Remote access protocols are protocols designed to give high-level access to a computer. Examples are Secure Shell (SSH) and Remote Desktop Protocol (RDP)
2. File-sharing protocols are protocols which provide access to files and printers. Examples are SMB and Apple Filing Protocol.
3. Database protocols offer access to databases without the standard checks an application provides. Examples are DB2, Hadoop and MongoDB.
4. Device access protocols are usually specific protocols to access devices sold by one manufacturer. Examples are Cisco Smart Install, Android Debug Bridge and Ubiquity.
5. Messaging protocols are protocols used by devices from different manufacturers to exchange messages between them. This category does not include Instant Message Protocols. Examples are AMQP and MQTT.

6. Location Service protocols that are intended to locate services and devices in local networks. These protocols can leak internal information key to an attacker. An example is Service Location Protocol (SLP, srvloc).
7. Other protocols provide services that can be easily abused and don't fall into the above categories. Examples are SOCKS and mDNS.

3 VULNERABLE PROTOCOLS

Sometimes protocols were designed for use over the Internet but are not considered secure enough anymore. As with amplification protocols, sometimes only part of the protocol or a specific configuration is vulnerable. Depending on the situation, we will commit to education instead of blocking these protocols.

Protocols can also be vulnerable for a limited time until a solution is available, either as a patch or a workaround. If that is the case, the CISO will have the protocol blocked pending a resolution.

4 SCADA / ICS / OT PROTOCOLS

Supervisory control and data acquisition (SCADA), Industrial Control Systems (ICS) and Operation Technology (OT) all refer to systems used to control physical environments or systems. They control building management systems, robots, and manufacturing systems. Most protocols are simple conversions of serial protocols designed without any security considerations.

If compromised, they can cause physical damage and injury.

5 AMPLIFICATION PROTOCOLS

Specific application-layer protocols that rely on the User Datagram Protocol (UDP) have been identified as potential attack vectors. By design, UDP is a connection-less protocol that does not validate source Internet Protocol (IP) addresses. Unless the application-layer protocol uses countermeasures such as session initiation in Voice over Internet Protocol, an attacker can easily forge the IP packet datagram to include an arbitrary source IP address[1]. When many UDP packets have their source IP address forged to the victim's IP address, the destination server (or amplifier) responds to the victim (instead of the attacker), creating a reflected denial-of-service (DoS) attack.

Specific parts of the UDP protocols elicit much larger responses than the initial request. Previously, attackers were limited by the linear number of packets directly sent to the target to conduct a DoS attack. Now, a single packet can generate between 10 and 50.000 times the original bandwidth. This is called an amplification attack. When combined with a reflective DoS attack on a large scale, using multiple amplifiers and targeting a single victim, DDoS attacks can be conducted relatively easily.

An amplification protocol is not inherently high risk for the university's network. Some protocols, like Memcached, can impact part of the network.

Blocking these protocols also improves the university's standing in the international networking community.

[1] https://tools.ietf.org/html/rfc3261

As mentioned, only specific commands or configurations will trigger the response with some UDP protocols. We will want to commit to education instead of blocking these protocols.

6 APPENDIX – CHANGES TO THE BLOCKED PROTOCOLS

This appendix contains a list of changes to the blocked protocols. For details about the protocol, we refer to Appendix – List of blocked protocols.

Protocol Name	Description	Change	Document version
CouchDB	Apache CouchDB is an open-source document-oriented NoSQL database.	Protocol added.	1.0
MS-RDP	Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft®.	Protocol deleted. This was a duplicate for RDP.	1.1
DVR DHCP Discover	DHCPDiscover is a UDP-based JSON protocol that manages multiple networked digital video recorders (DVRs) variants.	Protocol did not indicate a blocked network.	1.1
WS Discovery	Web Services Dynamic Discovery is a technical specification that defines a multicast discovery protocol to locate services on a local network.	Protocol added.	1.2
MS Message Queuing	MSMQ is a messaging infrastructure and a development platform for creating distributed, loosely-coupled messaging applications for the Microsoft® Windows® operating system.	UDP added.	1.3 1.4[2]
MS-SQL	Microsoft SQL Server is a relational database management system developed by Microsoft.	TCP added. Ports added.	1.4[3]
SLP	The Service Location Protocol (SLP, srvloc) is a service discovery protocol that allows devices to find services in a local area network.	Protocol added.	1.4[4]
BACNET	BACnet is a communication protocol for building automation and control networks using the ASHRAE, ANSI, and ISO 16484-5 standards.	Changed network.	1.5[5]
General Electric	A series of General Electric PLC protocols, especially GE Fanus Series 90-30, GE SRTP and GE QuickPanels.	Protocols added.	1.5[6]

[2] Initially only TCP port 1801 was mentioned. MSMQ also uses UDP port 1801. The information in chapter 7 now reflects that fact.
[3] Initially only UDP was mentioned. MS-SQL also uses the TCP protocol on the same ports. The information in chapter 7 now reflects that fact.
[4] The protocol is defined to be used on a local network and not over the internet. The UDP port is prone to be used for reflective DDoS attacks with an amplification of 2200:1.
[5] BACNET was erronously set for specific networks only. As a SCADA protocol it should be blocked for all networks.
[6] GE SRTP is a replacement for GE Fanus. It also adds some ports.

CoAP	Constrained Application Protocol (CoAP) is a protocol for constrained devices.	Corrected wrong port number. Added description of CoAPS. Added TCP protocol for both CoAP and CoAPS.	1.6
CUPS-browsed	A daemon for browsing the Bonjour broadcasts of shared, remote CUPS printers	Protocol added	1.6
mSQL	Mini SQL (abbreviated mSQL) is a lightweight database management system from Hughes Technologies.	Protocol added	1.7[7]
uPNP	UPnP is a service that allows devices on the same local network to discover each other.	Protocol added	1.7[8]

[7] Mini SQL is a database application, and therefore, it should be blocked.
[8] uPNP is mostly used in home networks to detect other devices and open ports in the firewall. Both uses are unsafe in a network like ours.

7 APPENDIX – LIST OF BLOCKED PROTOCOLS

This list contains the protocol name and a short description of the protocol. The next column contains the IP protocol and port(s). For reference, the next column shows pointers to the chapter(s) describing the danger of the protocol. The last three columns represent the part of the network for which the protocol should be blocked. An "X" in the first column denotes a network block for all IP ranges in use at the university. An "X" in the next column indicates a block for UTnet. Users of the campus network can still use the protocol in this case. The third column shows whether there will or can be exceptions to the rules governed by the previous two columns.

Protocol Name	Description	UDP / TCP Port	Reason[9]	Blocking		
				All networks [10]	All networks, except student dorms	Only specific networks or exceptions[11]
AMQP[12]	Advanced Message Queueing Protocol is an open internet protocol for business messaging. It is often used for IoT device management.	TCP 5672	3 4		X	X
Android Debug Bridge	ADB is a command-line tool that lets you communicate with an Android device.	TCP 5555	2 (4)	X		
Apple Filing Protocol	AFP is a protocol for sharing files over a network.	TCP 548	2	X		
Apple Remote Desktop	Apple Remote Desktop is a Macintosh application that allows users to use the computer's desktop remotely.	UDP 3283	2 5	X		

[9] Pointer to the chapter where the reason is explained.
[10] Networks used for network research are considered equal to “internet”. They are excluded from “All networks” by default.
[11] In case an “X” appears in this column as well as in one of the other columns this means that exceptions are possible on the blocking rules.
[12] As with other messaging protocols this one can be used in research. They are also often used on the campus network.

BACnet	BACnet is a communication protocol for building automation and control networks using the ASHRAE, ANSI, and ISO 16484-5 standards.	TCP 47808[13]	4	X		
Cassandra	Cassandra is a free, open-source, distributed, wide-column store, NoSQL database management system designed to handle large amounts of data across many commodity servers, providing high availability with no single point of failure.	TCP 7000 – 7001, 7199	2		X	
CharGEN	The Character Generator Protocol is intended for testing, debugging, and measurement. The protocol is rarely used, as its design flaws allow misuse.	UDP 19	3 5	X		
Cisco Smart Install	Smart Install is a plug-and-play configuration and image-management feature that provides zero-touch deployment for new switches.	TCP 4786	2 3	X		
CoAP[14]	Constrained Application Protocol (CoAP) is a protocol for constrained devices. CoAP is designed for use between devices on the same constrained network (e.g., low-power, lossy networks), between devices and general nodes on the Internet, and between devices on different constrained networks joined by the Internet. This includes the DTLS-secured version, CoAPS.	UDP 5683 TCP 5683 UDP 5684 TCP 5684	4 5		X	X
CODESYS	CODESYS is an integrated development environment for programming controller applications according to the international industrial standard IEC 61131-3.	TCP 1200, TCP 2455	4	X		
CouchDB	Apache CouchDB is an open-source document-oriented NoSQL database implemented in Erlang. CouchDB uses multiple formats and protocols to store, transfer, and process data. It uses JSON to	TCP 5984	2		X	

[13] This is an ephemeral port. An ephemeral port is a communications endpoint (port) of a transport layer protocol of the Internet protocol suite that is used for only a short period of time for the duration of a communication session. Such short-lived ports are allocated automatically within a predefined range of port numbers by the IP stack software of a computer operating system. Blocking these ports can give unexpected results in day-to-day operation of the network.

[14] As with other messaging protocols this one can be used in research. They are also often used on the campus network.

	store data, JavaScript as its query language using MapReduce, and HTTP for an API.					
Crimson V3	Crimson® 3.0 is programming software for G3, G3 Kadet and Graphite® HMI operator panels, Graphite Edge and Core Controllers, Modular Controllers and Data Station Plus.	TCP 789	4	X		
CUPS-browsed	CUPS browsed allows access to shared, remote CUPS printers	UDP 631	2	X		
CWMP	CPE WAN Management Protocol was for remote management of customer-premises equipment (CPE) connected to an Internet Protocol (IP) network.	TCP 7547, TCP 30005	2	X		
DB2	Db2 is a family of data management products, including database servers, developed by IBM.	UDP 523	2 5	X		
DHCP	Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information, such as the subnet mask and default gateway.	UDP 67 - 68	2	X		
DNP3	Distributed Network Protocol 3 is a set of protocols used between components in process automation systems.	TCP 20000	4	X		
DNS	The Domain Name System is the hierarchical and decentralised naming system that identifies computers reachable through the Internet or other Internet Protocol networks.	UDP 53	5			X[15]
DVR DHCP Discover	DHCPDiscover is a UDP-based JSON protocol that manages multiple networked digital video recorder (DVR) variants.	UDP 37810[16]	5	X		

[15] To prevent abuse of open resolvers. Access to registered nameservers will be allowed.

[16] This is an ephemeral port. An ephemeral port is a communications endpoint (port) of a transport layer protocol of the Internet protocol suite that is used for only a short period of time for the duration of a communication session. Such short-lived ports are allocated automatically within a predefined range of port numbers by the IP stack software of a computer operating system. Blocking these ports can give unexpected results in day-to-day operation of the network.

Elastic Search	Elasticsearch is a search engine based on the Lucene library. It provides a distributed, multitenant-capable full-text search engine.	TCP 9200	2		X	X
EtherNet/IP	EtherNet/IP (IP = Industrial Protocol) is an industrial network protocol that adapts the Common Industrial Protocol (CIP) to standard Ethernet.	TCP 44818[17]	4	X		
Firebird	Firebird is an open-source SQL relational database management system that supports Linux, Microsoft Windows, macOS and other Unix platforms.	TCP 3050	2		X	
GE SRTP	The protocol is an implementation of the "Service Request Transport Protocol" developed by General Electric Automation and Controls[18] for communication with PLCs. This includes the Quickpanel port.	TCP 18245 – 18246, TCP 57176	4	X		
Hadoop	Apache Hadoop provides a software framework for distributed storage and processing Big Data using the MapReduce programming model.	TCP / UDP 50070[19]	2 5		X	X
HART	The HART Communication Protocol is a hybrid analog+digital industrial automation open protocol.	TCP 5094	4	X		
IEC 60870-5-104	IEC 60870 part 5 is one of the IEC 60870 standards defining systems used for remote control in electrical engineering and power system automation applications.	TCP 2404	4	X		
IPMI	The Intelligent Platform Management Interface (IPMI) is a set of computer interface specifications that provides management and	UDP 623	2 5	X		

[17] This is an ephemeral port. An ephemeral port is a communications endpoint (port) of a transport layer protocol of the Internet protocol suite that is used for only a short period of time for the duration of a communication session. Such short-lived ports are allocated automatically within a predefined range of port numbers by the IP stack software of a computer operating system. Blocking these ports can give unexpected results in day-to-day operation of the network.

[18] Formerly GE Fanuc, that used only port 18245.

[19] This is an ephemeral port. An ephemeral port is a communications endpoint (port) of a transport layer protocol of the Internet protocol suite that is used for only a short period of time for the duration of a communication session. Such short-lived ports are allocated automatically within a predefined range of port numbers by the IP stack software of a computer operating system. Blocking these ports can give unexpected results in day-to-day operation of the network.

	monitoring capabilities independently of the host system's CPU, firmware and operating system.					
IPP	The Internet Printing Protocol (IPP) is a protocol for communication between client devices and printers (or print servers).	TCP 631	2	X		
ISAKMP[20]	Internet Security Association and Key Management Protocol is a protocol for establishing Security association (SA) and cryptographic keys in an Internet environment.	UDP 500	2 3			X
Kad	Kademlia is a distributed hash table for decentralised peer-to-peer computer networks.	UDP 6429	5	X		
LDAP	The Lightweight Directory Access Protocol is an open, vendor-neutral, industry-standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol network.	TCP / UDP 389	2 5[21]		X	X[22]
mDNS	The multicast DNS (mDNS) protocol resolves hostnames to IP addresses within small networks that do not include a local name server.	UDP 5353	3 5	X		
MELSEC-Q	MELSEC is a communication protocol for Mitsubishi Electric PLCs.	TCP 5007	4	X		
Memcached	Memcached is a general-purpose distributed memory-caching system.	TCP / UDP 11211	2 5	X		
Modbus	Modbus is a data communications protocol for use with programmable logic controllers.	TCP 502	4	X		
MonetDB	MonetDB is an open-source column-oriented relational database management system initially developed at the Centrum Wiskunde	TCP 50000[23]	2			X

[20] This is used by IPsec for establishing virtual Private Networks.

[21] UDP only

[22] Both TCP and UDP are blocked on UTnet. On campus TCP can be allowed.

[23] This is an ephemeral port. An ephemeral port is a communications endpoint (port) of a transport layer protocol of the Internet protocol suite that is used for only a short period of time for the duration of a communication session. Such short-lived ports are allocated automatically within a predefined range of port numbers by the IP stack software of a computer operating system. Blocking these ports can give unexpected results in day-to-day operation of the network.

	& Informatica in the Netherlands. It is designed to perform highly on complex queries against large databases, such as combining tables with hundreds of columns and millions of rows.					
MongoDB	MongoDB is a cross-platform document-oriented database program. Classified as a NoSQL database program, MongoDB uses JSON-like documents with optional schemas.	TCP 27017 – 27019, TCP 28017	2		X	
MQTT[24]	MQTT is a machine-to-machine network protocol. It is designed for connections that have devices with resource constraints or limited network bandwidth.	TCP 1883, TCP 8883	2 4		X	
~~MS-RDP~~	~~Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection.~~	~~TCP / UDP 3389~~	~~2~~ ~~5~~	~~X~~		
MS-SQL	Microsoft SQL Server is a relational database management system developed by Microsoft.	TCP 1433 - 1434, TCP 4022 UDP 1434	2		X	
MSMQ[25]	MSMQ is a messaging infrastructure and a development platform for creating distributed, loosely coupled messaging applications for the Microsoft® Windows® operating system.	TCP 1801 UDP 1801	2 3	X		
mSQL	Mini SQL (abbreviated mSQL) is a lightweight database management system from Hughes Technologies.	UDP / TCP 1114	2 3		X	
MySQL	MySQL is an open-source relational database management system.	TCP 3306	2		X	
NAT-PMP	NAT Port Mapping Protocol is a protocol for automatically establishing network address translation settings and port forwarding configurations without user effort.	UDP 5351	2 5	X		

[24] As with other messaging protocols this one can be used in research. They are also often used in the campus network.
[25] It is considered a legacy protocol. See https://particular.net/blog/msmq-is-dead.

NetBIOS	NetBIOS is an acronym for Network Basic Input/Output System. It provides services related to the OSI model's session layer, allowing applications on separate computers to communicate over a local network.	TCP / UDP 137 – 139	2	X		
Netcore / NetisRouter	Netis is a brand of routers from Netcore. It is vulnerable to a backdoor attack on UDP 53413.	UDP 53413[26]	3	X		
NTP	The Network Time Protocol is a networking protocol for clock synchronisation between computer systems over packet-switched, variable-latency data networks.	UDP 123	5[27]			X
OMRON-FINS	FINS is used to control machines for industrial and manufacturing OMRON Global.	UDP 9600	4 5	X		
OPC UA Binary	OPC Unified Architecture (OPC UA) is a cross-platform, open-source IEC62541 standard for data exchange from sensors to cloud applications developed by the OPC Foundation.	TCP 4840	4	X		
Oracle BD	Oracle Database is a multi-model database management system produced and marketed by Oracle Corporation.	TCP 1521, 1830	2	X		
PC-Worx	PC WORX is the standard programming, debugging and operating software for the ILC, AXC, RFC, S-MAX, PC WORX RT and CPX (Festo) PLC ranges.	TCP 1962	4	X		
Portmapper	The port mapper is an Open Network Computing Remote Procedure Call service on network nodes that provide other ONC RPC services.	UDP 111	2 5	X		
PostgreSQL	PostgreSQL, or Postgres, is a free and open-source relational database management system emphasising extensibility and SQL compliance.	TCP 5432	2		X	

[26] This is an ephemeral port. An ephemeral port is a communications endpoint (port) of a transport layer protocol of the Internet protocol suite that is used for only a short period of time for the duration of a communication session. Such short-lived ports are allocated automatically within a predefined range of port numbers by the IP stack software of a computer operating system. Blocking these ports can give unexpected results in day-to-day operation of the network.

[27] Only in specific configurations

ProConOS	ProConOS is a high-performance PLC run time engine for embedded and PC-based control applications.	TCP 20547	4	X		
PowerShell Remoting	Windows PowerShell remoting lets you run any Windows PowerShell command on one or more remote computers.	TCP 5985 - 5986	2		X	
QOTD	Mainframe sysadmins used the Quote of the Day (QOTD) service to broadcast a daily quote on request by a user.	UDP 17	5	X		
Quake Network Protocol	The Quake Protocol was used in earlier generations of the industry-changing Quake first-person shooter video game.	UDP 26000, 27960	5		X	
Radmin	Radmin is a protocol for remote access to computers.	TCP 4899	2		X	
RDP	Remote Desktop Protocol is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection.	TCP / UDP 3389	2		X	
REDIS	Redis is an in-memory data structure store used as a distributed, in-memory key-value database, cache and message broker, with optional durability.	TCP 6379	2	X		
Rsync	rsync is a utility for efficiently transferring and synchronising files between a computer and a storage drive across networked computers by comparing file modification times and sizes.	TCP 873	2[28]		X	X
Secure Shell (SSH)	The Secure Shell Protocol is a cryptographic protocol for securely operating network services over an unsecured network. Its most notable applications are remote login and command-line execution.	TCP 22	2		X	
Siemens S7	With SIMATIC STEP 7 (TIA Portal), you can configure, program, test, and diagnose the Siemens Controllers.	TCP 102	4	X		
SLP	The Service Location Protocol (SLP, srvloc) is a service discovery protocol allowing computers and other devices to find services in a local network without prior configuration. SLP has been designed to	TCP / UDP 427	2 5	X		

[28] If used without a password

	scale from small, unmanaged networks to large enterprise networks.					
SMB	Server Message Block is a communication protocol that provides shared access to files and printers across nodes on a local network.	TCP 445	2	X		
SMTP	Protocol for delivering email messages to mail servers.	TCP 25	2		X	
SNMPv2	Simple Network Management Protocol is an Internet Standard protocol for collecting and organising information about managed devices on IP networks and modifying that information to change device behaviour.	UDP 161 - 162	2 4 5	X		
SOCKS 4/5	A SOCKS proxy allows you to hide your IP address from online services.	TCP 1080	2		X	
SSDP	The Simple Service Discovery Protocol is a network protocol for advertising and discovering network services and presence information.	TCP / UDP 1900	2 5	X		
Steam Protocol	The Steam protocol is a customised file transfer protocol. Steam:// URLs can contain Steam protocol commands to install or uninstall games, update games, start games with specific parameters, backup files, or perform other supported actions.	UDP 27015	5		X	
Telnet	Telnet is an application protocol used on the Internet or local area network to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. Information is transmitted in plain text.	TCP 23	2 3	X		
TFTP	Trivial File Transfer Protocol (TFTP) is a simple lockstep file transfer protocol that allows clients to get a file from or put a file onto a remote host.	UDP 69	2 3 5	X		
Tridium Niagara Fox	Niagara Fox Protocol is a building automation protocol used between the Niagara software systems by Tridium.	TCP 1911	4	X		

Ubiquiti	The Ubiquiti discovery protocol (UDP port 10001) is passive - devices will respond if they receive a directed or broadcast packet.	UDP 10001	25	X		
uPNP	UPnP (Universal Plug and Play) is a service that allows devices on the same local network to discover each other and automatically connect through standard networking protocols.	TCP 5000	2	X		
VNC	Virtual Network Computing (VNC) is a graphical desktop-sharing system to control another computer remotely.	TCP 5900	2		X	
WS-Discovery	Web Services Dynamic Discovery (WS-Discovery) is a technical specification that defines a multicast discovery protocol to locate services on a local network.	UDP 3702	25	X		
XDMCP	XDMCP is an unencrypted remote desktop protocol.	UDP 177	25	X		

8 APPENDIX – EXCEPTIONS PROCEDURE

This appendix describes the procedure for requesting an exception to the blocked protocols. A request has to follow the following rules:

1. Email the request to security-management-lisa@utwente.nl.
2. Include a detailed reason for the exception.
3. Provide the protocol to be excluded.
4. Provide the internal host or network to be excluded.
5. Provide the external host or network to be excluded.

The triple 3/4/5 needs to be as restrictive as possible.

LISA Security Management can ask for clarification.

When the exception is honoured, LISA Security Management will register the request and instruct LISA-ITO to add the exception.

At least once a year, LISA Security Management will verify whether the exceptions must remain active.

LISA Security Management has the responsibility and right to remove exceptions if they pose a threat to the University. LISA Security Management will try to inform the requestor beforehand but can not guarantee this. LISA Security Management will notify the requestor when an exception is removed.