Use of Tofino SA with HIMA products

1 Aim of this Report

The bigger networks are the more vulnerable they get. To use the advantages of Ethernet infrastructures it is important to limit the traffic to the required protocols and to the required communication relations. A lot of customers use, or plan to use, firewalls. One available industrial solution is the **Tofino** SA (security appliance) from byres-security. This is a software solution integrated into products from MTL, Hirschmann and Honeywell. This document doesn’t describe the use of this firewall, it describes the knowledge required to use it with HIMA products.
It is also not the aim to crack the Tofino or to test all the possible settings or all the different combinations of IP-Addresses. Also the performance in big applications can’t be estimated from the small scale test.

2 Test design

The first test was performed with a HIMatrix F20 with a connected PADT and a Modbus TCP Client running on the same computer to learn how the system works. The next step was to test the HIMA products with all HIMA specific protocols (safeethernet) see Chapter 3.

2.1 Test settings

All the tests are performed in the default settings of the protocols.

2.2 Test performing

All the tests of the different protocols are performed as following:

1. Access denied by Tofino
2. Access allowed by Tofino
3. Access denied by Tofino

After each step the access is controlled and should match the configured state.
The Direction is configured as “BIDIRECTIONAL”.

⚠ Please be aware that the configuring PC should not be the PC that also performs the communication. In that case the communication through Tofino has to be stopped for about 3 minutes or power cycled until the “deny” is valid.

3 Protocol matrix

	Used Protocol and related Ports	HIMax	HIQuad	HIMatrix PES	HIMatrix RIO	A number of X-OPC could be used per PC (default)	PADT Controlpanel
Controller / HIMA	**HIMax**	UDP 6010 /		UDP 6010 /	UDP 6010 + UDP 8004 UDP 123 NTP		
	HIQuad		UDP 6005 / UDP 6010 UDP 6012				
	HIMatrix PES	UDP 6010 /		UDP 6010 /	UDP 6010 + UDP 8001 (E) UDP 8004 (S) UDP 123 NTP		
	HIMatrix RIO	UDP 6010 + UDP 8004 UDP 123 NTP		UDP 6010 + UDP 8001 (E) UDP 8004 (S) UDP 123 NTP			
Computer / HIMA	**SILworX**	UDP 8000 +		UDP 8000 +	UDP 8000 +		
	ELOP II		TCP 6034 +				
	ELOP II Factory			UDP 8000 +	UDP 8000 +		
	X-OPC Server DA	UDP 6010 /		UDP 6010 /		UDP 15138 +	UDP 25138 +
	X-OPC Server AE	UDP 6010 /				UDP 15138 +	UDP 25138 +
	OPC-Server DA		UDP 6005 / UDP 6010 UDP 6012	UDP 6010 /			
	OPC-Server AE		Modbus TCP 502				
	COMeth		UDP 6011 UDP 6031 UDP 6032				
	safeethernet Token		UDP 6005 UDP 6010 UDP 6012	UDP 6005 UDP 6010 UDP 6012			
	Modbus	TCP 502 UDP 502 (nFix)	TCP 502 TCP 8896	TCP 502 UDP 502 (nFix)			
	ProfiNet	UDP 49152 UDP 59153 UDP 34964					
	Ethernet IP			TCP 44818 UDP 2222			
	Send Receive	TCP (nFix)		TCP (nFix)			
	CUT	TCP (nFix) UDP (nFix)		TCP (nFix) UDP (nFix)			

Not all combinations were tested just a spot test was executed.

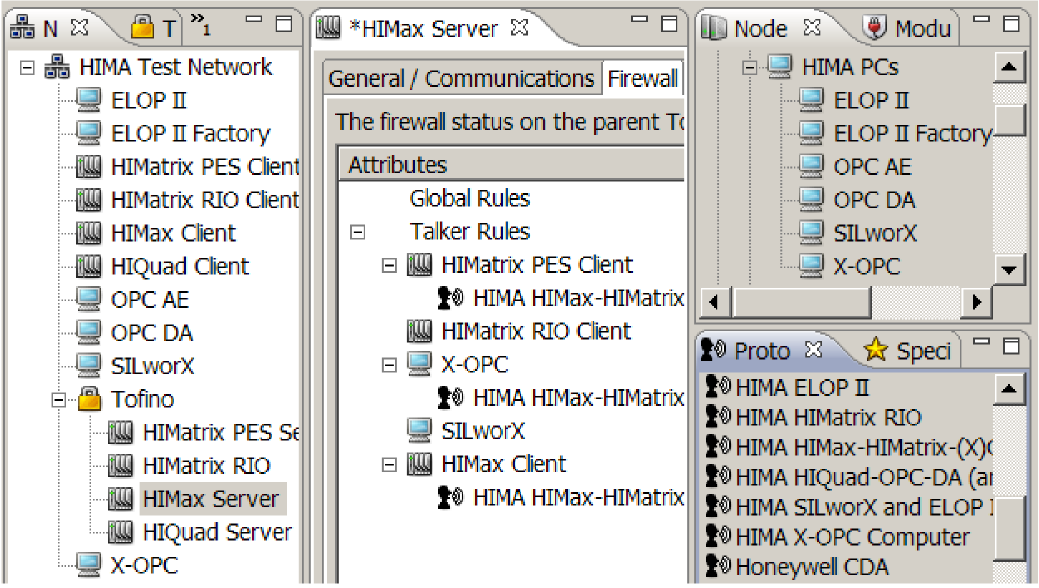
3.1 Implementation Rules

Controllers: HIMax, HIQuad, HIMatrix PES and HIMatrix RIO
Computer: SILworX, ELOPII, ELOPII Factory, (X) OPC-Server DA & AE

Protocols	Ports
HIMA ELOP II	6034
HIMA HIMatrix RIO	6010, 8001, 8004 + (NTP)
HIMA HIMax-HIMatrix-(X)OPC	6010
HIMA HIQuad-OPC-DA (and Token)	6005, 6010, 6012
HIMA SILworX and ELOP II Factory	8000
HIMA X-OPC Computer	15138, 25138

3.2 How to use Tofino with HIMA Products

Byres Security and HIMA agreed that it makes sense to use the **minimum** set of rules for the most secure implementation



The background is that the talker rules always take the Protocols used by both nodes. E.g. due to the “Protocol Matrix” from above

- SILworX uses “HIMA SILworX and ELOP II Factory”,
- HIMax uses “HIMA HIMatrix RIO”, “HIMA HIMax-HIMatrix-(X)OPC” and “HIMA SILworX and ELOP II Factory”

A connection HIMax to HIMax, with the complete set of rules, would open all the ports of the 3 mentioned Protocols, but just the Protocol “HIMA HIMax-HIMatrix-(X)OPC” is required. That would be a comfortable solution but not a secure one.
The way it is implemented now is that HIMax just uses the Protocol “HIMA HIMax-HIMatrix-(X)OPC”. Therefore a HIMax to HIMax communication also just uses the Protocol “HIMA HIMax-HIMatrix-(X)OPC”.
On the other hand a SILworX to HIMax configuration offers no identical protocol and therefore no protocol in the talker rules. The Protocol “HIMA SILworX and ELOP II Factory” has to be added with drag and drop to the talker rules.

The Protocol Matrix gives you information about where a protocol has to be added manually and where not. At the upper right corner of each table field you find a mark:
/…just drag and drop to the talker rules, nothing to be added
+…add the protocols manually

The external Protocols, e.g. to DCS Systems have to be added manually anyway.

These rules are implemented from V 1.5 of Tofino.

3.3 Additional testing

The Modbus TCP Enforcer was successfully tested with Honeywell as Master and HIMax as a Slave.

4 Remarks to Tofino

All Tests performed with the Hardware from MTL,
Software Version 1.4.1 and 1.5.2.

Technical Data:
Throughput with 20 FW Rules: 95.5 MBPS at 1500 Byte Frames
Throughput with 500 FW Rules: 90.0 MBPS at 1500 Byte Frames

All technical data above are from the Tofino CMP User's Guide
No Hardware or EMI tests have been performed. So HIMA can't give a statement regarding the behavior in harsh industrial environment.

4.1 Further development

At present an OPC-Classic enforcer is developed where HIMA participates. Then Tofino is able to protect the connection between OPC-Server and OPC-Client.