SAISON INFORMATION SYSTEMS CO, LTD.
HULFT Technical Support Center

Title

Firewall Settings Upon Using HULFT

Document Information

Technical Document ID:	1-HULx-xx007-E-04
OS:	ALL
Product Name/Version:	HULFT Ver.5
	HULFT Ver.6
	HULFT Ver.7
	HULFT Ver.8
Last Updated:	2019/1/31

～ HULFT Communication Flow① ～

The following are the send source and the destination port no. of each communication directions packet upon the file transferring.
You need to open these communications in the FireWall:

※The field name in the [System Environment Settings] is used for each port no.
For the actual port no., please verify the settings in your environment.
Also, since the port number is not dynamic (due to it being allocated by OS) when connecting using a send process or a send request, "any" is used in the following:

☆Send Process

Packets from a Sending side to a Receiving side	Send Source Port No.: any	Destination Port No.: [Receive Port No.]
Packets from a Receiving side to a Sending side	Send Source Port No.: [Receive Port No.]	Destination Port No.: any

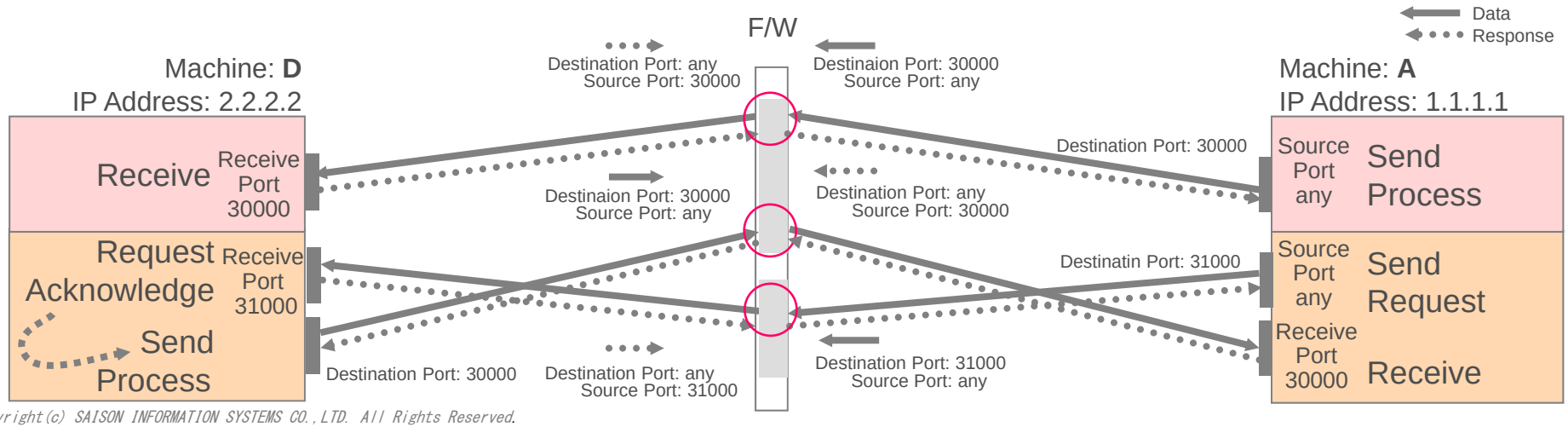
☆Send Request in addition to the above communication

Packets from a Sending side to a Receiving side	Send Source Port No.: any	Destination Port No.: [Request Acknowledge Port No.]
Packets from a Receiving side to a Sending side	Send Source Port No.: [Request Acknowledge Port No.]	Destination Port No.: any

< Display Example of Packet >

Send Source IP	Address IP	Send Source Port No.	Address Port No.	Data Area
1.1.1.1	2.2.2.2	any	30000	HULFT Data

< ex.) Upon Passing through Firewall >



～ HULFT Communication Flow ② ～

In HULFT, you can monitor the operation of an opposite side in addition to the file transfer.
The following are the send source and the destination port no. of each communication directions packet upon the operation monitoring.
You need to open these communications in the FireWall.

※The field name in the [System Environment Settings] is used for each port no.
For the actual port no., please verify the settings of your environment.
Also, since the port number is not dynamic (due to it being allocated by OS) when connecting using a monitoring process, "any" is used.

☆Send Monitoring

Packets from a Monitoring side to a Monitored side	Send Source Port No.: any	Destination Port No.: [Send Request Acknowledge Port No.]
Packets from a Monitored side to a Monitoring side	Send Source Port No.: [Send Request Acknowledge Port No.]	Destination Port No.: any

☆Receive Monitoring

Packets from a Monitoring side to a Monitored side	Send Source Port No.: any	Destination Port No.: [Receive Port No.]
Packets from a Monitored side to a Monitoring side	Send Source Port No.: [Receive Port No.]	Destination Port No.: any

☆Request Acknowledge Monitoring

Packets from a Monitoring side to a Monitored side	Send Source Port No.: any	Destination Port No.: [Request Acknowledge Port No.]
Packets from a Monitored side to a Monitoring side	Send Source Port No.: [Request Acknowledge Port No.]	Destination Port No.: any

☆Service Monitoring *the monitoring target is "HULFT for Windows Ver.7.2.0 or later versions" only

Packets from a Monitoring side to a Monitored side	Send Source Port No.: any	Destination Port No.: [Service Process Port No.]
Packets from a Monitored side to a Monitoring side	Send Source Port No.: [Service Process Port No.]	Destination Port No.: any

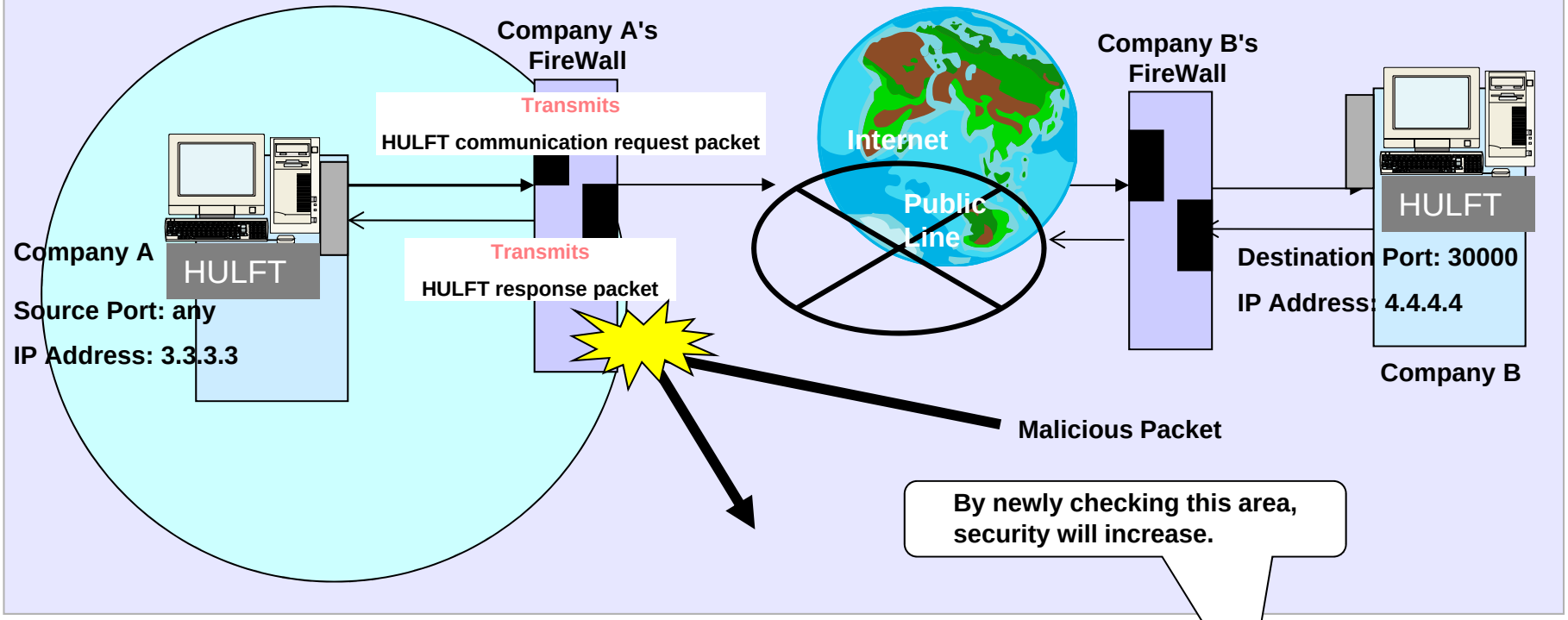
☆Scheduler Monitoring *the monitoring target is "HULFT for Windows Ver.7.2.0 or later versions" only

Packets from a Monitoring side to a Monitored side	Send Source Port No.: any	Destination Port No.: [Scheduler Port No.]
Packets from a Monitored side to a Monitoring side	Send Source Port No.: [Scheduler Port No.]	Destination Port No.: any

[Caution] Targets that can be monitored will vary depending on the host type and the version of HULFT installed on the monitored host.
For details pertaining to monitoring target, please refer to “Remote Heartbeat Function” in the “administration manual”.

～Effective FireWall Setups Suggestion①～

You can filter malicious communication request packet by allowing only the response packet (ACK) from HULFT to transmit.

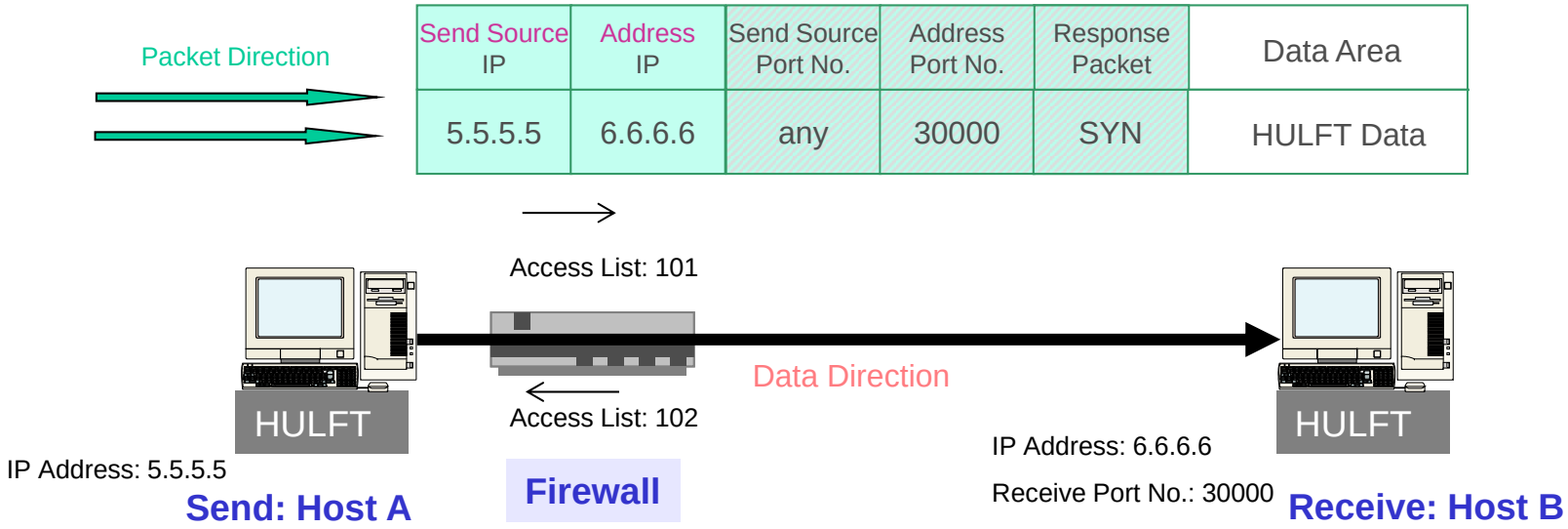


< Display Example of Packet >

Send Source IP	Address IP	Send Source Port No.	Address Port No.	Response Packet	Data Area
3.3.3.3	4.4.4.4	30000	any	ACK	HULFT Data

< ex.) Upon Passing through Firewall >

~How to Setup Effective FireWalls①~



If you would like to increase the security of Host A using the firewall, you must set up an access list that filters packets of A to B (in this case, access list 101) and an access list that filters packets of B to A (in this case, access list 102).

[Caution] In "HULFT for Mainframe Type VOS Ver.5," ping is issued from VOS upon connection so you must additionally set up to allow the connection.
In "HULFT for Mainframe Type VOS Ver.6," you can select whether or not to issue ping upon connection.

～Effective FireWall Setups Suggestion②～

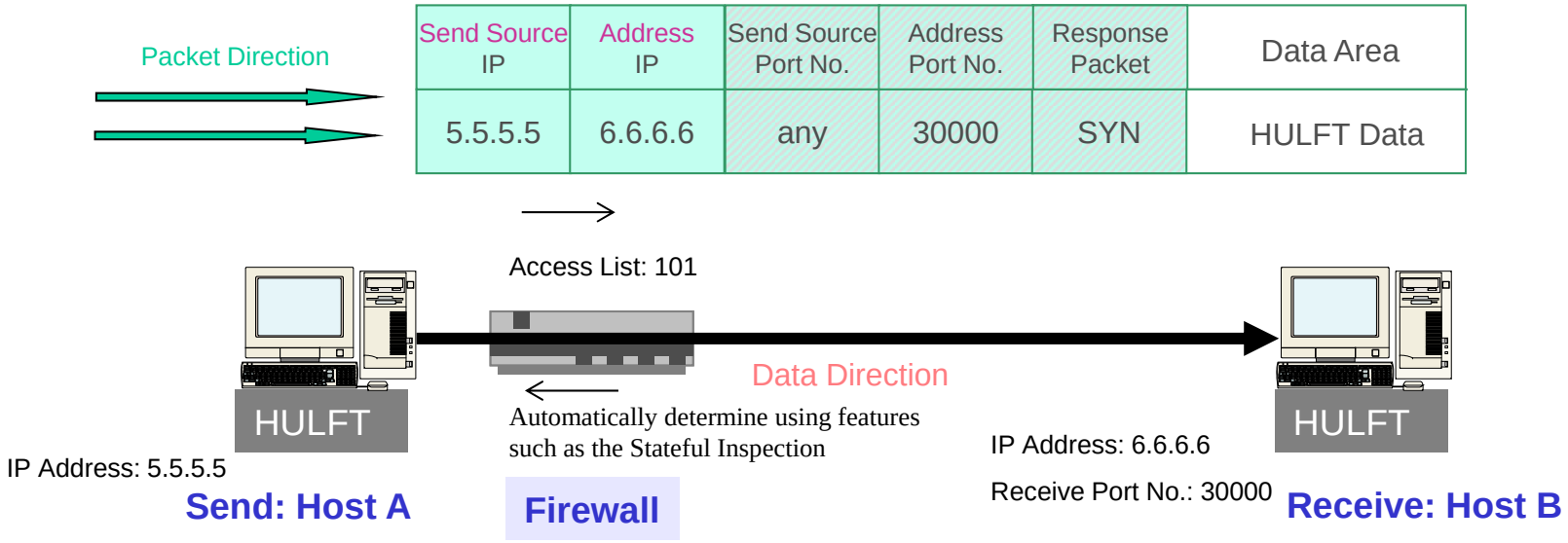
In the "~Effective FireWall Setups Suggestion①~," we suggested to check the response packet flag as a workaround, but we have recently seen a problem that abuses this setting to externally setup (ACK) to attack.

To be prepared for this kind of attacks, many products with the FireWall feature (such as Stateful Inspection) to check extensively up to session information to determine whether it is response packets are released so using this feature is the effective way to accept response packets.

There have been cases where it had no meaning to check this area.

	Send Source IP	Address IP	Send Source Port No.	Address Port No.	Response Packet	Data Area
< Display Example of Packet >						
< ex.) Upon Passing through Firewall >	3.3.3.3	4.4.4.4	30000	any	ACK	HULFT Data

~How to Setup Effective FireWalls②~



If you would like to increase the security of Host A using the FireWall, you will need to enable the feature to automatically determine response packets in addition to the access list (in this case, Access List 101) that controls the packets flowing from "A" to "B".

[Caution] In "HULFT for Mainframe Type VOS Ver.5," ping is issued from VOS upon connection so you must additionally set up to allow the connection.
In "HULFT for Mainframe Type VOS Ver.6," you can select whether or not to issue ping upon connection.