Firewall Configuration

Table of contents

1. Introduction

Our service may not function properly if firewalls prevent some of our own and/or merchant components from communicating.

All necessary information are provided in this document to help configure the merchant's firewalls and minimise communication errors between the merchant's network infrastructure and our payment gateways.

This document assumes that the merchant is familiar with the procedures for configuring firewalls, routers or any other devices used to block traffic on the merchant's network. The merchant should refer to his firewall configuration guide for instructions about creating and configuring firewall rules.

2. Firewall Port Information

The following table lists the destination ports that must be open to allow communication between the merchant's network infrastructure and our payment gateways.

Usage *	- Transaction feedback requests - Dynamic template page - XML page - Push reports via HTTP(S)	- Transaction confirmation e-mails - emails from our system to the merchant	- Web browsing in the back office - Application-specific connections to the back office (DirectLink, automated file uploads, AFTP, Fidelio, etc.)
Flow from the merchant system's perspective	Incoming	Incoming	Outgoing
Protocol/port	TCP 80 (HTTP) TCP 443 (HTTPS)**	TCP 25 (SMTP)	TCP 443 (HTTPS) UDP 53 (DNS)
Source	185.8.52.254 185.8.53.254 185.8.54.254 212.23.45.97 212.35.124.164	185.8.52.254 185.8.53.254 185.8.54.254 212.23.45.97 212.35.124.164	<u>HTTPS:</u> 62.72.112.128/28 84.233.249.96/27 185.8.54.0/24 185.8.53.0/24 185.8.52.0/24 212.23.45.96/28 212.35.124.160/27 <u>DNS:</u> 185.8.52.99 185.8.53.99 185.8.54.99
Destination	Merchant system(s) IP address(es)	Merchant mail server(s) IP address(es)****	185.8.52.254 185.8.53.254 185.8.54.254 212.23.45.97 212.35.124.164

<u>Important:</u> All merchant systems communicating with our payment gateways must be able to resolve the public hostname.

* The lists are non-exhaustive.

** Depending on protocols supported by the merchant's application servers and the merchant configuration in the back office and/or hidden parameters (HTTPS recommended).

*** If the merchant maintains a list of IP addresses authorised to send emails on his behalf, our IP ranges should be added to this list. As the owner of a public domain, a merchant could use SPF records, for example, to prevent sender-address spoofing. Please refer to http://www.openspf.org for more information or check with the merchant's DNS and/or mail server administrator if any action is required.

**** Depending on the merchant's email system architecture, the server could be hosted by the merchant ISP or inside the merchant's network.