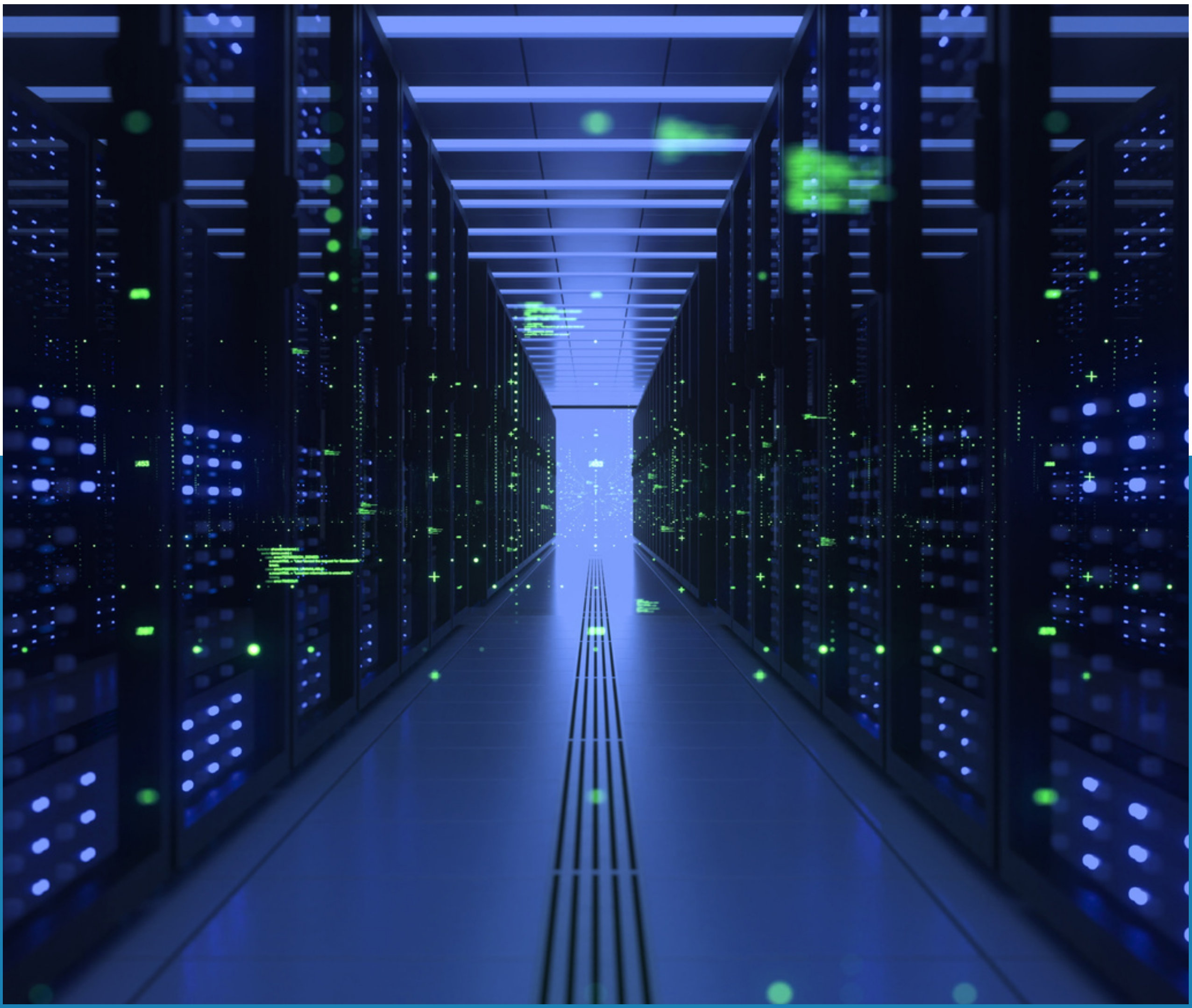
February 2023

EASEE-gas

Streamlining the gas business

Cloud endpoints for communication



EASEE-gas
Streamlining the gas business

Content Index

01. Executive summary

02. Introduction

03. Objective of this document

04. IP filtering

05. Other solutions

1. Executive summary

Moving communication systems to the cloud can give some supplemental challenges in terms of impact it can cause for parties with whom you have operational document exchanges.

It could require changes to the security context of these counterparties. This document aims at giving some contextual elements which can help your organization in evaluating such move. It focusses on elements that could influence interoperability.

2. Introduction

Trend: Setting up AS2/AS4 handlers in the cloud has impact on market communication.

When a company uses cloud endpoints it has an impact on counterparties. There should be awareness about the issues caused by this. Below is an explanation about the possible issues and solutions.

We are focusing on secure document exchange, using a cloud endpoint has impact on the underlying security level (network). In a message exchange there are always two parties.

We must consider that not all parties can deal with solutions which are available at cloud providers. Interoperability must be maintained.

This is a general trend; in this document we are focusing on the EASEE-gas communication using document exchange.

2.1 Cloud endpoints

Cloud solutions are getting more and more used by Message Brokers in several businesses around the world, and slowly but surely also will affect our work.

This may change the way we setup AS2/AS4 connections between partners. As of today, we depend on IP addresses whitelisted in firewalls, while cloud solutions depend more on dynamic endpoints.

3 Objective of this document

Currently flows between EASEE-gas partners are mostly secured with IP filtering for both incoming and outgoing flows. The objective of this document is to assess if this is still appropriate, notably in the context of cloud hosting which is becoming increasingly prevalent, and to suggest other options.

This document is certainly not intended to be a comprehensive or definitive study but rather informational.

4. IP filtering

IP filtering is rather cumbersome since IP filtering rules needs to be created and updated for every partner each time one of them changes either its outbound or its inbound IP. In a standard setup of systems in the cloud, counterparties would need to open up the whole IP range from the cloud provider. This weakens security associated to IP filtering.

The major cloud providers (i.e., AWS, Azure, Google Cloud) all offer firewalling services at reasonable cost; and they also sell fixed public IP for a reasonable fee.

Therefore, though not optimal in terms of maintenance, IP filtering is still a valid solution and should probably remain so in a foreseeable future.

```
-06-03T18:42:18.018", "deltaStartMillis":"0",
ager.handlers.RequestHandler", "method":"handle",
 "message":"Duration Log", "durationMillis":"508"
/analyze", "webParams":"null", "class":"com.orgman
e-afd8-46ac-9745-839146a20f09", "sessionID":"144o2
6"}{"timestamp":"2017-06-03T18:43:335.030","deltaS
hartdata_new.json", "class":"com.orgmanager.handle
520jm9trnd3s3n7wg0k", "sizeChars":"48455", "messa
'0", "level":"INFO", "webURL":"/app/page/report",
:b-bfa8-4e7d-8047-498454af885d", "sessionID":"144
}{"timestamp":"2017-06-03T18:46:921.000", "delta
ger.handlers.RequestHandler", "method":"handle",
 "message":"Duration Log", "durationMillis":"10"
json/file", "webParams":"file=chartdata_new.json
5-19e2-4a60-88d7-6ead86e273d1", "sessionID":"144
"}{"timestamp":"2017-06-03T18:42:18.018", "delta
ger.handlers.RequestHandler", "method":"handle",
"message":"Duration Log", "durationMillis":"508"
analyze", "webParams":"null", "class":"com.orgman
-afd8-46ac-9745-839146a20f09", "sessionID":"144o2
"}{"timestamp":"2017-06-03T18:43:335.030","deltaS
artdata_new.json", "class":"com.orgmanager.handle
20jm9trnd3s3n7wg0k", "sizeChars":"48455", "messa
0", "level":"INFO", "webURL":"/app/page/report",
b-bfa8-4e7d-8047-498454af885d", "sessionID":"144o
}{"timestamp":"2017-06-03T18:46:921.000", "deltaS
ger.handlers.RequestHandler", "method":"handle
```

5. Other solutions

Alternatives to IP filtering need to be distinguished as to whether they apply to outbound or to inbound flows.

5.1 Outbound flows

Several solutions may be considered. For each of them the principle is the same: filter on the FQDN (=the DNS name) of the partner rather than its IP address.

5.1 .1 Proxy

This is the most natural solution and probably the one that should be favored. Filtering outgoing http(s) flows based on FQDN is a native feature that they all support. Your company probably host such equipment.

The principle is that your network team adds the FQDNs of your partners to the whitelist of your company's proxy (or makes sure those FQDNs are not blacklisted, depending on the policy implemented on this proxy).

There are some constraints though:

- **Authentication**

Your AS2/AS4 software may not be compatible with proxy. In fact, AS2/AS4 software is itself quite often designed to act as proxy. Additionally, if the proxy of your company requires an authentication, you have to make sure that its authentication protocol is supported by your AS2/AS4 software.

- **Ports**

Proxies natively support standard http(s) ports (that is, 80 for http and 443 for https). Though, some of your AS2/AS4 partners probably use a different port than one of those standard ports. Your network team will need to implement rules on the proxy for your AS2/AS4 software to reach those partners. And this team is not likely to like it since maintaining those rules is quite a burden if there are too many of them.

5.1.2 FQDN filtering by firewalls

Firewall can filter outbound flows based on rules containing FQDNs. Generally, it works as follows:

- Your network team configures the FQDN of your partner in a firewall rule.
- The firewall periodically resolves this FQDN into an IP address (i.e., every 30 seconds).
- For every outbound flow, the firewall checks the target IP against the IP address in the rule, and allows or rejects the flow based the rule.

This solution is a valid solution in terms of security, but not all firewalls support it. Furthermore, the implementation may impact your DNS architecture: sometimes it is requested that the DNS and the firewall is the same equipment for the solution to work.

5.1.3 FQDN filtering by DNS

The principle is that the DNS of your company resolves the FQDN of your AS2/AS4 partners only if they are whitelisted.

The problem is that you can easily work this around by updating the local “hosts” file of the server of your AS2/AS4 software (if its http client supports this file for name resolution) and therefore your security team is not likely to agree to this solution.

5.2 Inbound flows

5.2.1. Web Application Firewalls (WAF)

WAF is the most natural alternative to IP filtering for inbound flows. The principle is that the filtering is done at the http layer: the WAF checks the URL, the http headers, the http body and blocks the flow if it detects some malicious usage (i.e., code injection).

The network team of your company can (and most likely will) use the same WAF to protect different servers (your AS2/AS4 software but also other http servers or your company), just as they already do with their TCP/IP firewalls. You may need a WAF rule dedicated to the FQDN of your service in order to disable the parsing of the http body, since it is encrypted by AS2/AS4.

The security assessment of this solution in the AS2/AS4 context still needs to be done by security team of your company. If necessary, for additional security, additional rules dedicated to AS2/AS4 may be implemented in the WAF, but it will require additional work and expertise, and not all WAF do support that kind of customization. Cloud providers provide WAF service at a reasonable cost, but they are not highly configurable.

EASEE-gas

Streamlining the gas business

Contact us

EASEE-gas, the European Association for the Streamlining of Energy Exchange

Join us and play an active part in the discussions shaping the future of the EU energy sector.

✉ easee-gas@kellencompany.com

🌐 easee-gas.eu

in EASEE-gas