# Requirement 1: Build and Maintain a Secure Network

# Firewall Configuration

# OfficeSupply shall implement a formal process for approving and testing all network connections

# and changes to the firewall and router configurations. (PCI Requirement 1.1.1)

# A network diagram identifying all connections between the cardholder data environment and other

# networks, including any wireless networks, must be maintained. (PCI Requirement 1.1.2)

# A cardholder data-flow diagram identifying the location of all cardholder data that is stored,

# processed, or transmitted within the network must be maintained. (PCI Requirement 1.1.3)

# OfficeSupply’s network will be configured with a requirement for a firewall at each Internet

# connection and between the internet-facing demilitarized zone (DMZ) containing the in-scope web

# server and the internal network zone that contains systems not directly involved in the payment

# process. (PCI Requirement 1.1.4)

# The network administrator shall maintain documentation which details use of all services,

# protocols, and ports allowed into the internal network zone. This list will include business

# justification for any traffic allowed in or out of the network. It will also include documentation of

# security features implemented for those protocols considered to be insecure. Examples of insecure

# services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1

# and v2. (PCI Requirement 1.1.6)

# Review firewall and router rule sets at least every six months. (PCI Requirement 1.1.7)

# Firewalls must restrict connections between untrusted networks and any system in the cardholder

# data environment. An “untrusted network” is any network that is external to the networks

# belonging to the entity under review, and/or which is out of the entity’s ability to control or

# manage. Access to the internet must be through a firewall, as must any direct connection to a

# vendor, processor, or service provider. (PCI Requirement 1.2)

# Inbound and outbound traffic must be restricted by the firewalls to that which is necessary for the

# cardholder data environment. All other inbound and outbound traffic must be specifically denied.

# (PCI Requirement 1.2.1)

# Examine router configuration files to verify they are synchronized and secured from unauthorized

# access. (PCI Requirement 1.2.2)

# Verify that there are perimeter firewalls installed between all wireless networks and the cardholder

# data environment, and that the firewalls deny or, if traffic is necessary for business purposes,

# permit only authorized traffic between the wireless environment and the cardholder data

# environment. (PCI Requirement 1.2.3)

# Firewall configuration must prohibit direct public access between the Internet and any system

# component in the cardholder data environment as follows:

#  Implement a DMZ to limit inbound traffic to only system components that provide

# authorized publicly accessible services, protocols, and ports. (PCI Requirement 1.3.1)

#  Limit inbound Internet traffic to IP addresses within the DMZ. (PCI Requirement 1.3.2)

#  OfficeSupply will install controls that implement anti-spoofing measures to detect and block

# forged source IP addresses from entering the network. (For example, block traffic

# originating from the Internet with an internal source address.) (PCI Requirement 1.3.3)

#  Outbound traffic from the cardholder data environment to the Internet must be explicitly

# authorized by management and controlled by the firewall. (PCI Requirement 1.3.4)

#  Ensure the firewall allows only established connections into the network and denies any

# inbound connections not associated with a previously established session. (PCI Requirement

# 1.3.5)

#  Use network techniques (such as NAT or RFC 1918 addressing) so as not to disclose private

# IP addresses and routing information to unauthorized parties. (PCI Requirement 1.3.7)

#  Use personal firewall software or hardware to protect any devices (including company

# and/or employee-owned) that connect to the Internet when outside the network (for

# example, laptops used by employees). (PCI Requirement 1.4)

# Ensure that security policies and operational procedures for managing firewalls are documented, in

# use, and known to all appropriate personnel. (PCI Requirement 1.5)

# FTP RPC

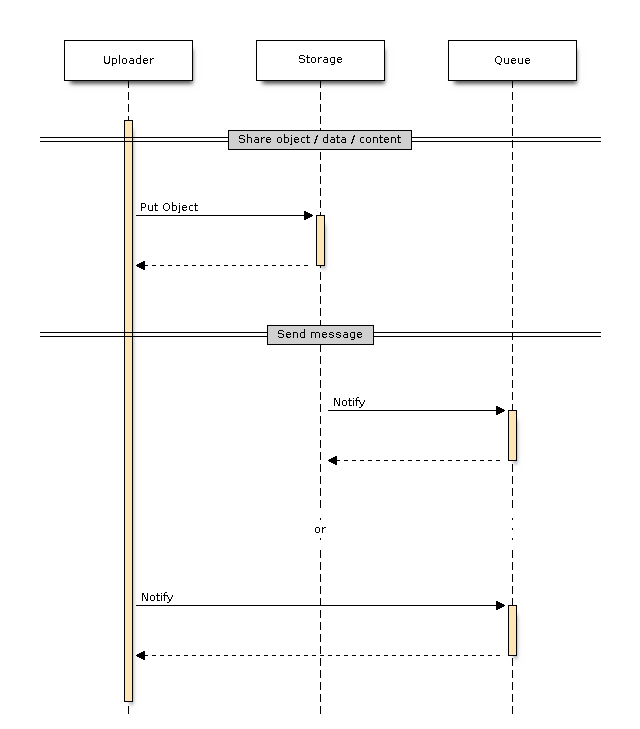
FTP via remote procedure call

Due to technical details of how the FTP and FTPS protocol are defined, systems that transfer files via FTP require a firewall with mostly open egress rules.

FTP RPC segregates the open egress requirement from the rest of the system(s).

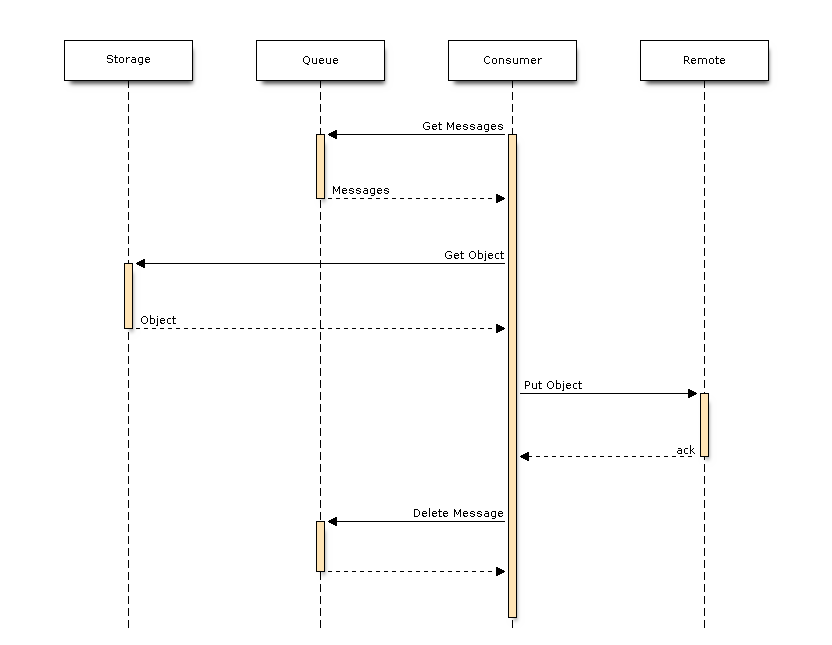
The system is asynchronous and does not return a response to the initiator.

## Outbound



| Name | Description |
| --- | --- |
| Uploader | Outbound initiator |
| Storage | Shared storage |
| Queue | Message queue |

### From Open Egress



| Name | Description |
| --- | --- |
| Storage | Shared storage |
| Queue | Message queue |
| Consumer | Message consumer |
| Remote | Remote / Vendor FTP |

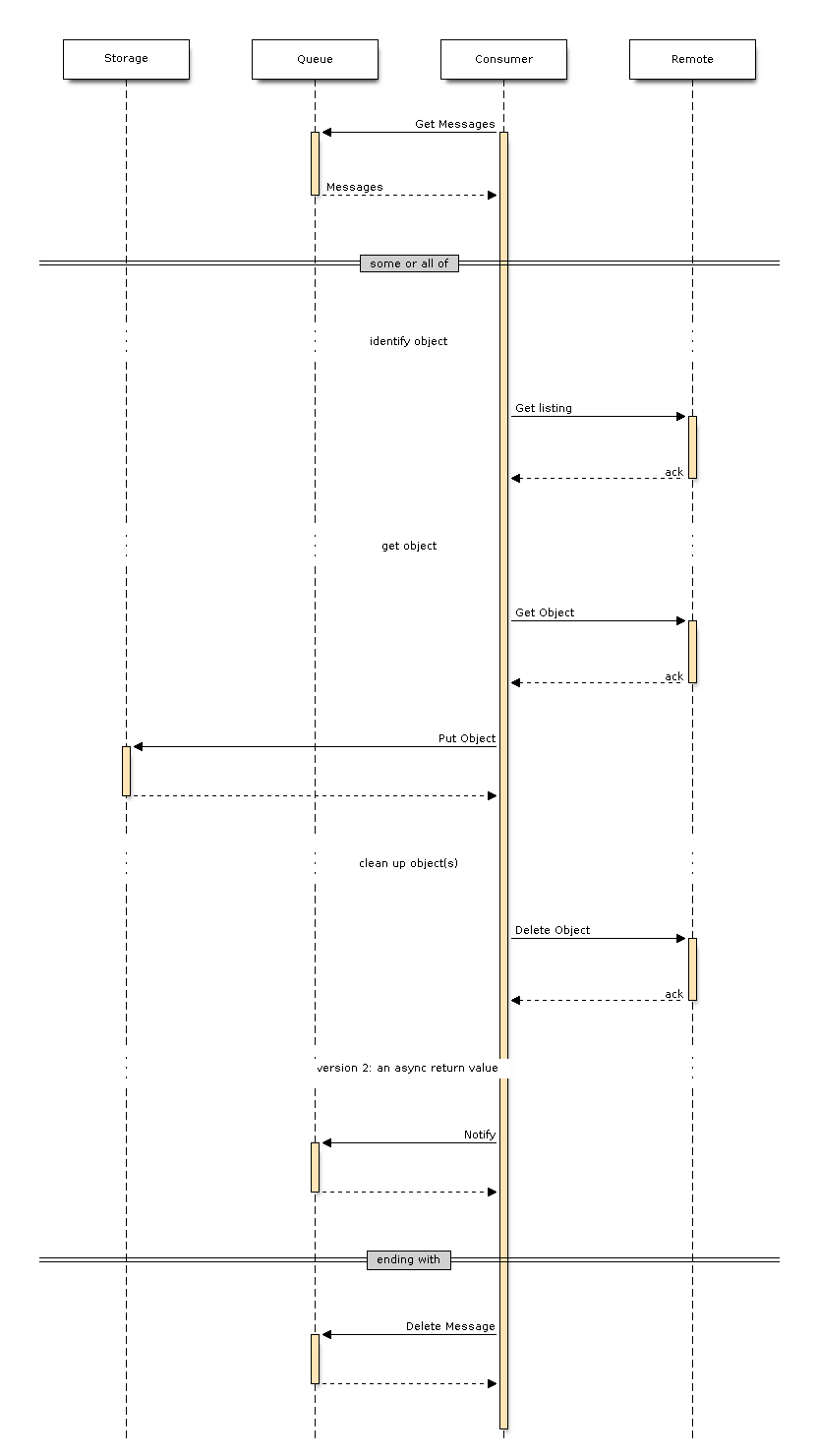
As of writing:

* “Shared storage” is AWS S3, which supports creating queue messages.
* “Message queue” is AWS SQS
* “Consumer” will be AWS Lambda

## Inbound

Starts with a request message sent describing the inbound request.

### From Open Egress



| Name | Description |
| --- | --- |
| Storage | Shared storage |
| Queue | Message queue |
| Consumer | Message consumer |
| Remote | Remote / Vendor FTP |

As of writing:

* “Shared storage” is AWS S3
  + AWS S3 supports creating queue messages on object creation events, delaying the need for consumer creating ack-notifications.
  + The use cases encapsulate the file-listing usages, meaning there is no need to send a “this is the file list” response.
* “Message queue” is AWS SQS
* “Consumer” will be AWS Lambda

For inbound requests, there is an expectation that there will be a later file-consumer that handles continuing the activates that happen after file has been acquired, either by queue-watching or storage-polling.

© Copyright OfficeSupply.com

Built with [Sphinx](http://sphinx-doc.org/) using a [theme](https://github.com/rtfd/sphinx_rtd_theme) provided by [Read the Docs](https://readthedocs.org/).