

NSI CSv2 Proposal

Synchronous Query Operation Support

John MacAuley

The Facts

- The current NSI CSv2 protocol only supports asynchronous communication
 - Requesting NSA sends a request operation to the provider NSA's SOAP endpoint.
 - Requesting NSA receives the resulting confirm, failed, or event message as a callback to the SOAP endpoint it has exposed.
- Why did we use asynchronous communications?
 - Requirement for long durations (minutes to days) between original request and a reply to that request.
 - Web services as a transport uses asynchronous callbacks or polling to support messaging behavior.
 - Polling performs poorly in a large scale messaging environment, so asynchronous callbacks were the obvious choice.

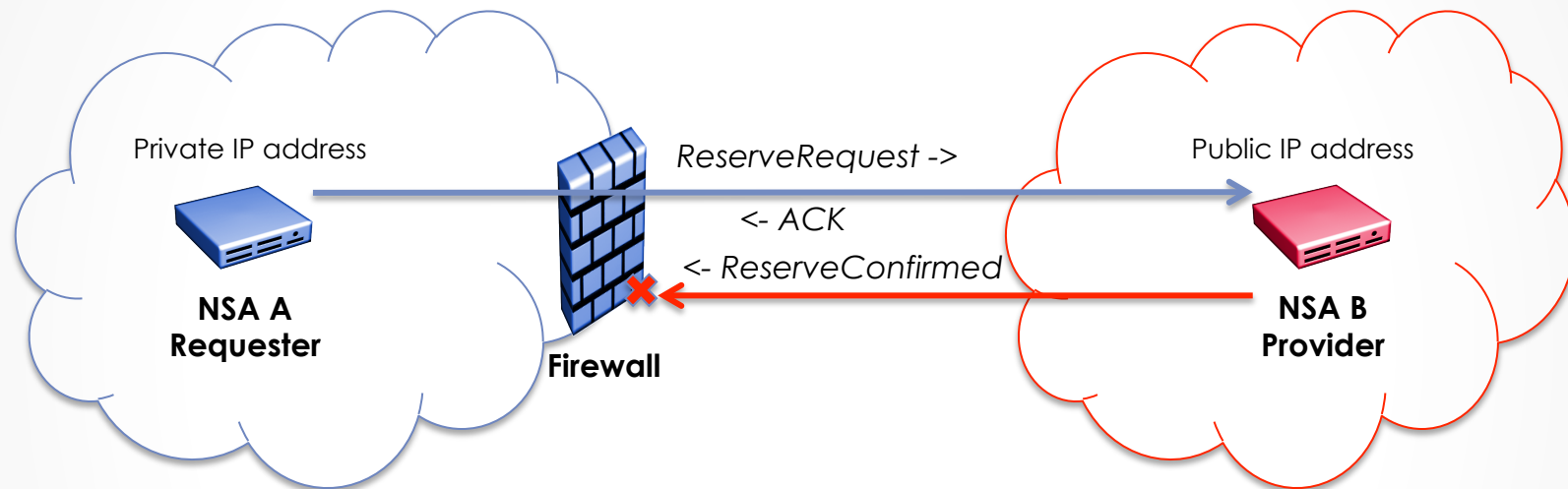
Current Behaviors

- As a result of the current transport protocol definition:
 - Provider NSA must be publically accessible – it must have a publically accessible interface to receive request messages from Requester NSA.
 - Requester NSA must also be publically accessible – it must have a publically accessible interface to receive response messages (confirm, failed, or event) from Provider NSA.
- Today we make supplying the callback “replyTo” field optional when the requesting NSA is not interested in receiving a confirmed/failed reply relating to the operation
 - There is no way to get the current status of a reservation without supplying the callback “replyTo” field in the query request.
 - As a result, the ability to support operations without the “replyTo” field provides no value unless we fix the query issue, and allow clients a way to get the current reservation status back synchronously.

Review of the firewall issue

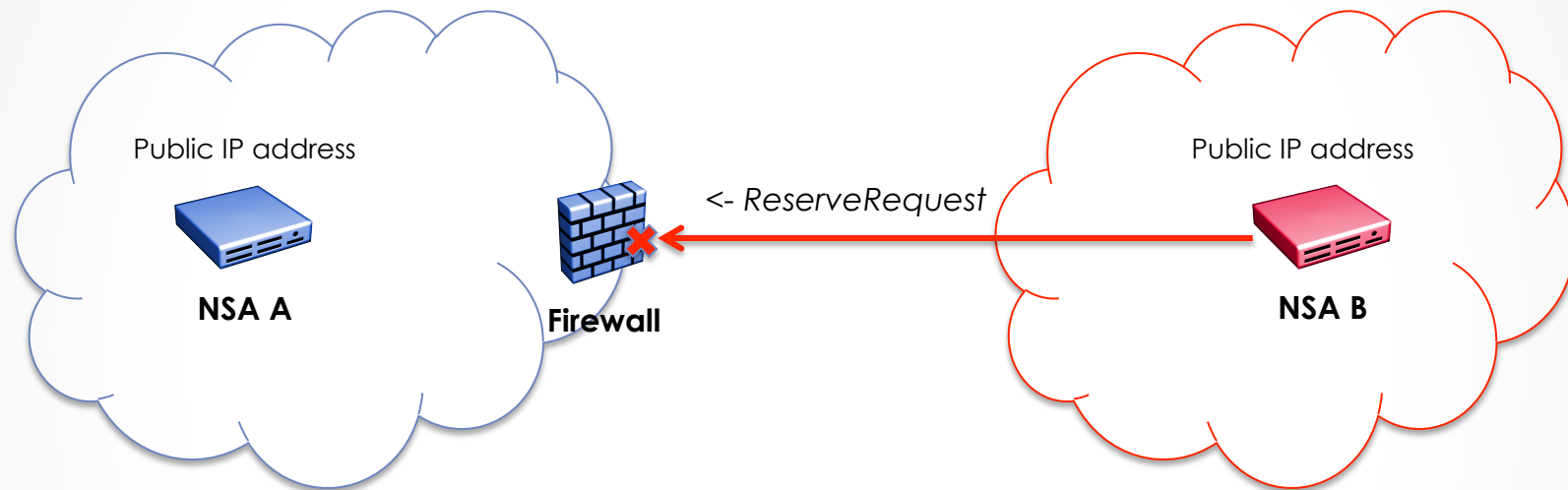
...

The Firewall Problem



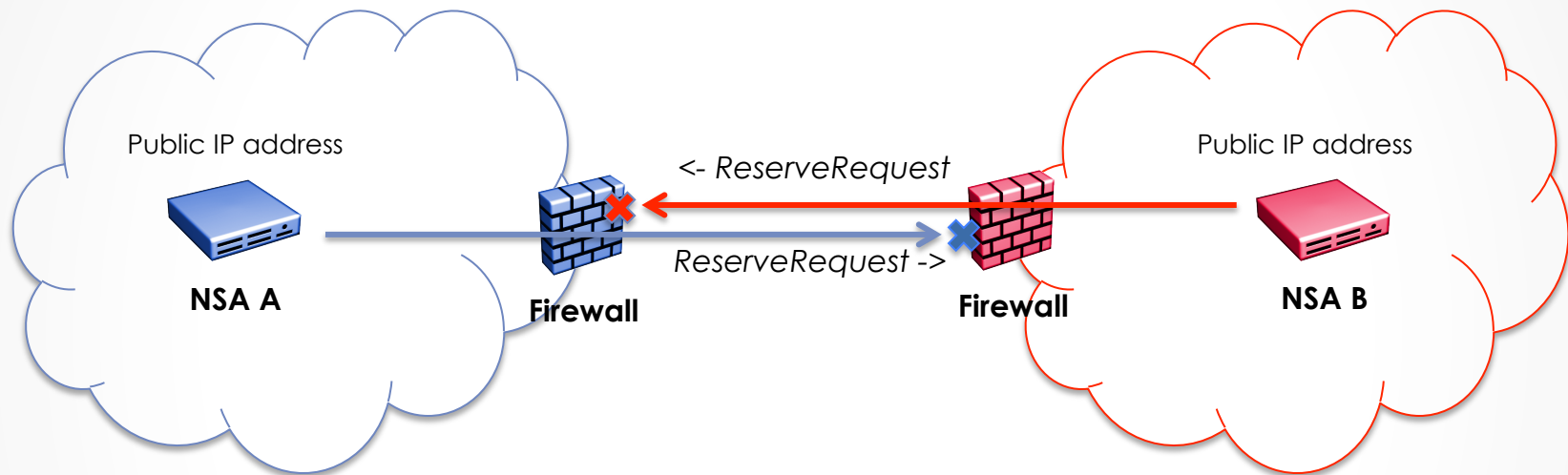
- "NSA A" behind firewall issues HTTP ReserveRequest to "NSA B" on the public network.
- "NSA A" populates private IP address into replyTo field for response.
- Firewall NATs HTTP request and passes on to "NSA B" but does not NAT the private IP address since this is embedded in the SOAP message.
- "NSA B" cannot reach the private IP address to deliver the ReserveConfirmed message.

It Gets Worse



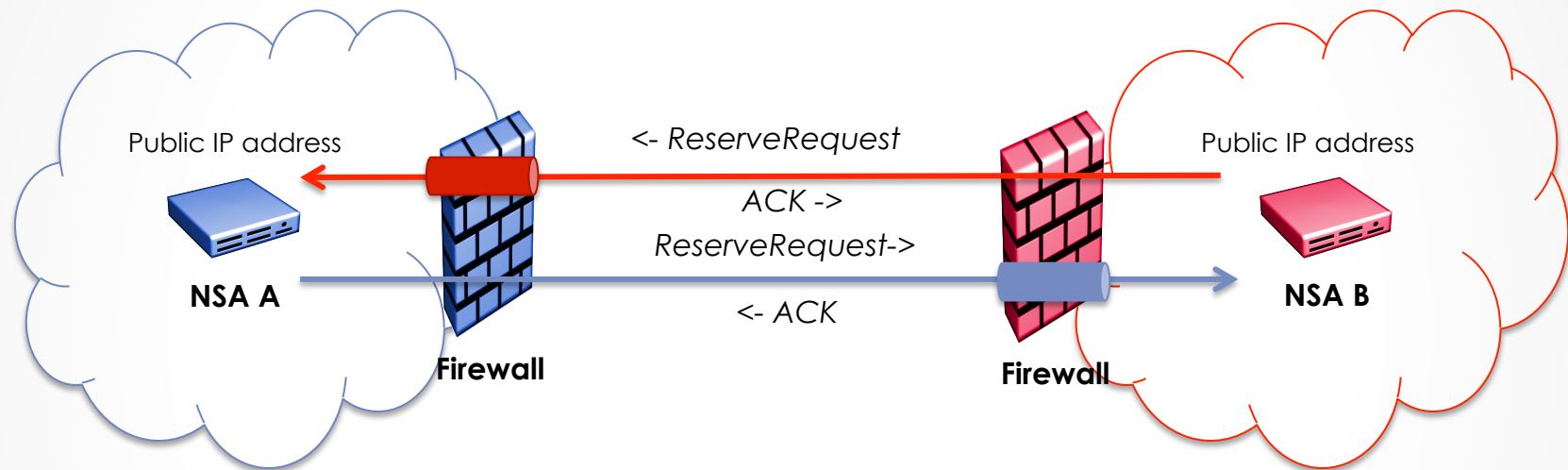
- The problem exists even when public IP addresses are assigned to an NSA behind a firewall, if that firewall is blocking HTTP requests.

Pathological Case



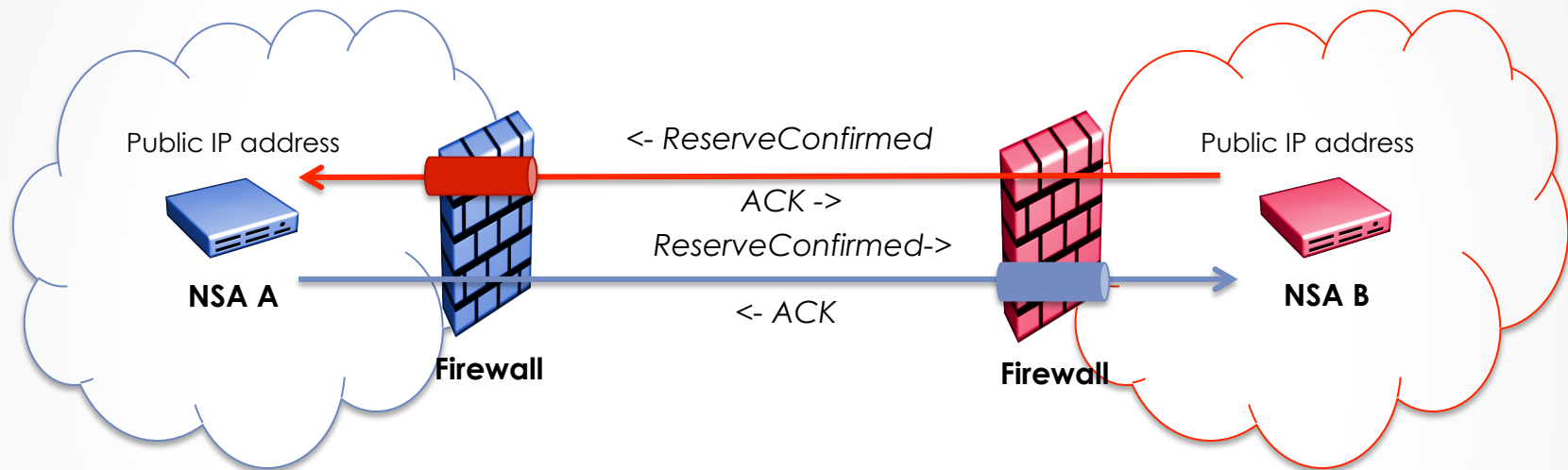
- "NSA A" cannot reach "NSA B" behind the firewall to issue request.
- "NSA B" cannot reach "NSA A" behind the firewall to issue request.

Proper Configuration of Firewall



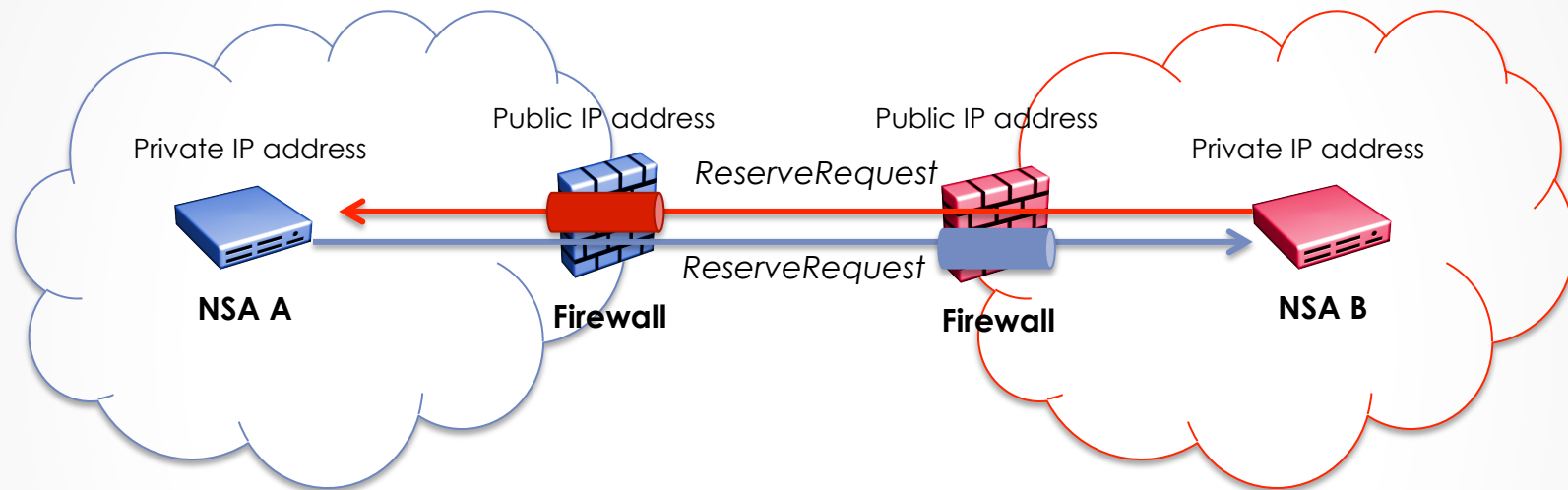
- For NSA with public IP addresses behind the firewall:
 - Access control lists can be set for peer NSA in combination with port filtering to allow an NSA behind a firewall to have traffic to it's HTTP server port passed through.

Proper Configuration of Firewall



- With proper configuration the ReserveConfirmed messages delivered through the callback mechanism can also be properly delivered to the requesting NSA.

Proper Configuration of Firewall



- For NSA with private IP addresses behind the firewall:
 - Firewall will need to act as public entity for NSA.
 - Access control lists can be set for peer NSA in combination with NAT and port forwarding to allow the requesting NSA to be mapped through to the provider NSA's HTTP server port within the DMZ
 - A requesting NSA behind a firewall will need to provide the public facing IP address and port of the firewall within the replyTo field of the SOAP request.

“Lightweight” Requester- Only NSA ...

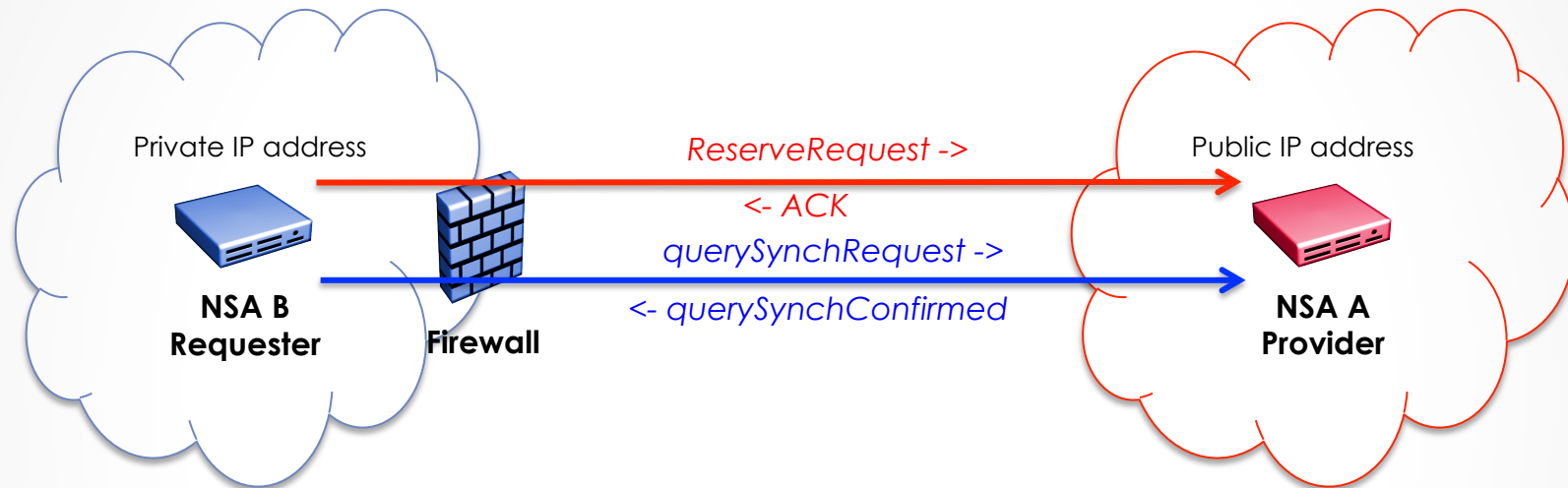
Discussion

- The NSI control plane “backbone” will consist of NSAs implementing both requester and provider roles (most likely aggregators)
 - These backbone NSAs will implement the full NSI protocol, always be present on the network, and use asynchronous communications.
 - There will be no issue with these NSA being publically accessible and firewall safe.
- But what about “lightweight” Requester-only NSA?
 - These typically represent the end user client and are delegates for end user requests.
 - These clients will come on and off the network as needed by the associated end user application.
 - There are end user requirements for these type of Requester NSA to be behind a firewall with private IP addresses, and with no ability to be firewall safe due to administrative policies.

Solution

- Continue to support the existing asynchronous communication model for those fully functional “backbone” NSA.
- Continue to allow for an optional “replyTo” field in the asynchronous operations (reserve, modify, provision, release, terminate, etc.).
- Implement an additional synchronous summary query operation that will return results in the SOAP response (200 OK) instead of the ACK message.
- This will allow a requester NSA to:
 - Issue all operations relating to a schedule lifecycle.
 - Use a firewall safe synchronous query to determine schedule status, and therefore, derive operation progress/results.

Synchronous Query



1. Provider "NSA A" exposes publically accessible NSI CSv2 SOAP endpoint.
2. Requester-only "NSA B" issues standard ReserveRequest SOAP operation to Provider "NSA A" but does not provide replyTo field.
3. Provider "NSA A" services ReserveRequest operation, but upon completion, does not issue the ReserveConfirmed due to lack of replyTo field.
4. Requester-only "NSA B" issues querySynchRequest to retrieve summary status of reservation.
5. Provider "NSA A" services querySynchRequest SOAP operation and returns resulting data in the SOAP response.