GUIDE

Establishing Access to SOIL

Version	Date	Change description
1	15.04.2016	Initial version

Contents

1 Definitions and Abbreviations

Below definition of some important terms used in this guide.

Term	Definition
Participant	Companies connected to SOIL for consumption and/or provisioning of applications/services.
SOIL	Secure Oil Information Link (Oil & Gas Industry extranet)
SOIL Service Provider (SSP)	A company approved by EPIM for provisioning of SOIL connection and security services to Participants. A SOIL Service Providers acts on SOIL in many ways in the same way ISPs act on the internet for providing access to Internet, but provide some additional mandatory services like SOIL firewall, routing ++
SOIL Core Operator	EPIM's Contractor for delivering the SOIL Core services
VPN	Virtual Private Network

2 Introduction

2.1 Purpose of this document

This guide aims to provide guidance to companies:

- In the process of preparing connection to SOIL for the first time.
- Currently connected to SOIL, but considering modifying their current SOIL connection

The guide provides guidance on three main aspects:

- Contractual alternatives
- Connection alternatives
- Technical aspects of being connected to SOIL

The guide is organised using patterns, which should not be considered as the only truth, but more as examples of acknowledged good practice.

2.2 Intended audience

Intended readers of this guide includes, but are not limited to

- Technical staff in Participants own organization
- Technical staff in Participants chosen IT provider (in case of outsources IT functions)
- Contract specialists and Managers in Participant organization, but then mainly limited to content provided in section *3 Contract alternatives*.

2.3 Relation to other important SOIL information sources

This document should be read together with the following other important information resources

1) The "Service Access Agreement for SOIL" to be concluded between the Participant and EPIM **before** the Participant is allowed to procure SOIL Access Services from SSP(s)

2) The step by step procedure for how to connect to SOIL as available on EPIM's homepage via link https://www.epim.no/epim/main/services/infrastructure-technology/soil/how-to-get-access

2.4 Purpose and criticality of SOIL

The SOIL network, is a secure and reliable extranet, supporting secure intercompany communication between Operators, business partners and suppliers, involved in NCS operations, and is designed to work independent from Internet.
The design and operation of SOIL will support this criticality.
SOIL acts primarily as an alternative delivery channel for information not desirable to transfer or publish via the Internet from a security and/or stability perspective. SOIL is currently the delivery channel for several applications/services in use by the NCS Oil & Gas industry.

3 Contract alternatives

After having entered into a Service Access Agreement with EPIM, the Participant's next step is to establish the actual physical access to SOIL. This involves subscribing to some mandatory SOIL Access Services from one or more of the EPIM approved SSPs. For more details on these services reference is made to section *5 Technical properties of SOIL*.

The complete list of EPIM approved SSPs can be found on EPIM's homepage https://www.epim.no/epim/main/services/infrastructure-technology/soil/approved-soil-service-providers

IMPORTANT! The contracts you as Participant conclude with SSP(s), for connecting to SOIL, should mirror your organisation's needs.

Following sub sections in this Chapter explains various possible contractual arrangement towards SSPs and some of their properties.

3.1 Contract Pattern A – Access line included in SSP contract

Participants:

- Without an existing line to SOIL and/or a desire to simplify number of contracts.
- Without an internal policy directing to use a specific line provider

Such Participants should consider to procure the line as part of the SSP contract.

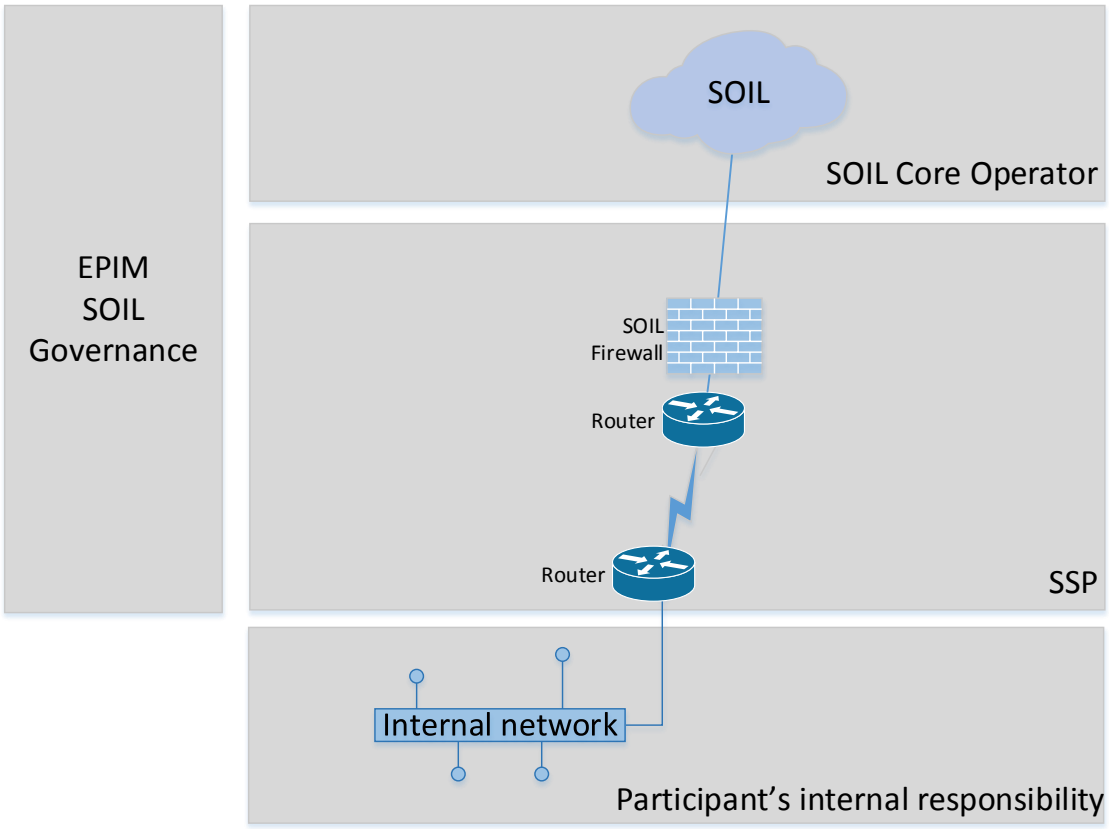
Pros	One less contract to manage.
Cons	If you later want to change to another SSP you will probably have to re-establish the line instead of just moving the termination point at the SSP side.

The router at the Participant-side can either be

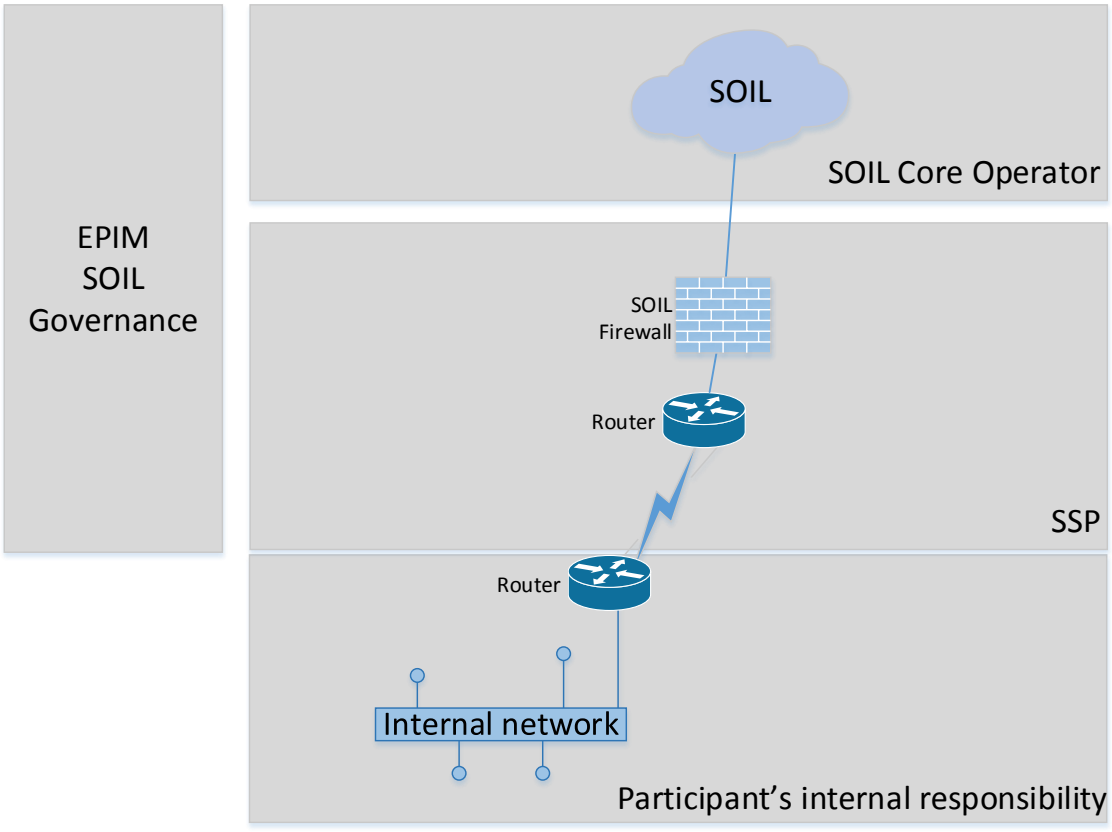
- Delivered by the SSP
- Provided by the Participant, and may include reusing an existing router.

The following sections in this chapter display the difference and domains of responsibilities.

3.1.1 SSP responsible for line, router and firewall



3.1.2 SSP responsible for line, but not for router on the Participant's side



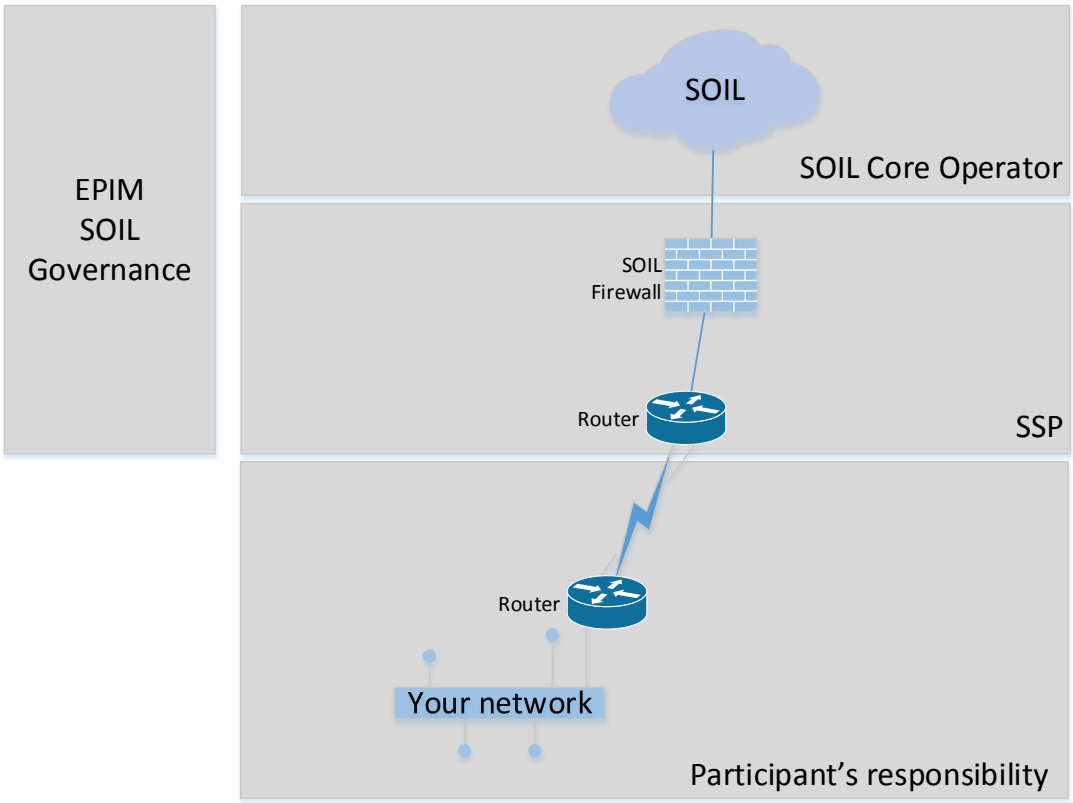
3.2 Contract Pattern B – Line contract separate from SSP contract

Participants:

- With an existing line to SOIL
- With an internal policy directing use of a specific line provider.

Should consider to procure the line as a separate contract.

Pros	You can just move the termination point at the SSP side if you later choose to change SSP.
Cons	An extra contract to manage if you do not have a portfolio contract with the line provider.



3.3 Contract Pattern C – SOIL connection as part of another contract

Participants:

- With an existing contract with one or more of the SSPs.

Should consider to procure the SOIL connection as an implicit part of such a contract.

Pros	• Easy to manage commercial and practically. • The SSP will normally gain more insight into your organisation's needs if they handle more services than just SOIL.
Cons	• Possibility for less competition.

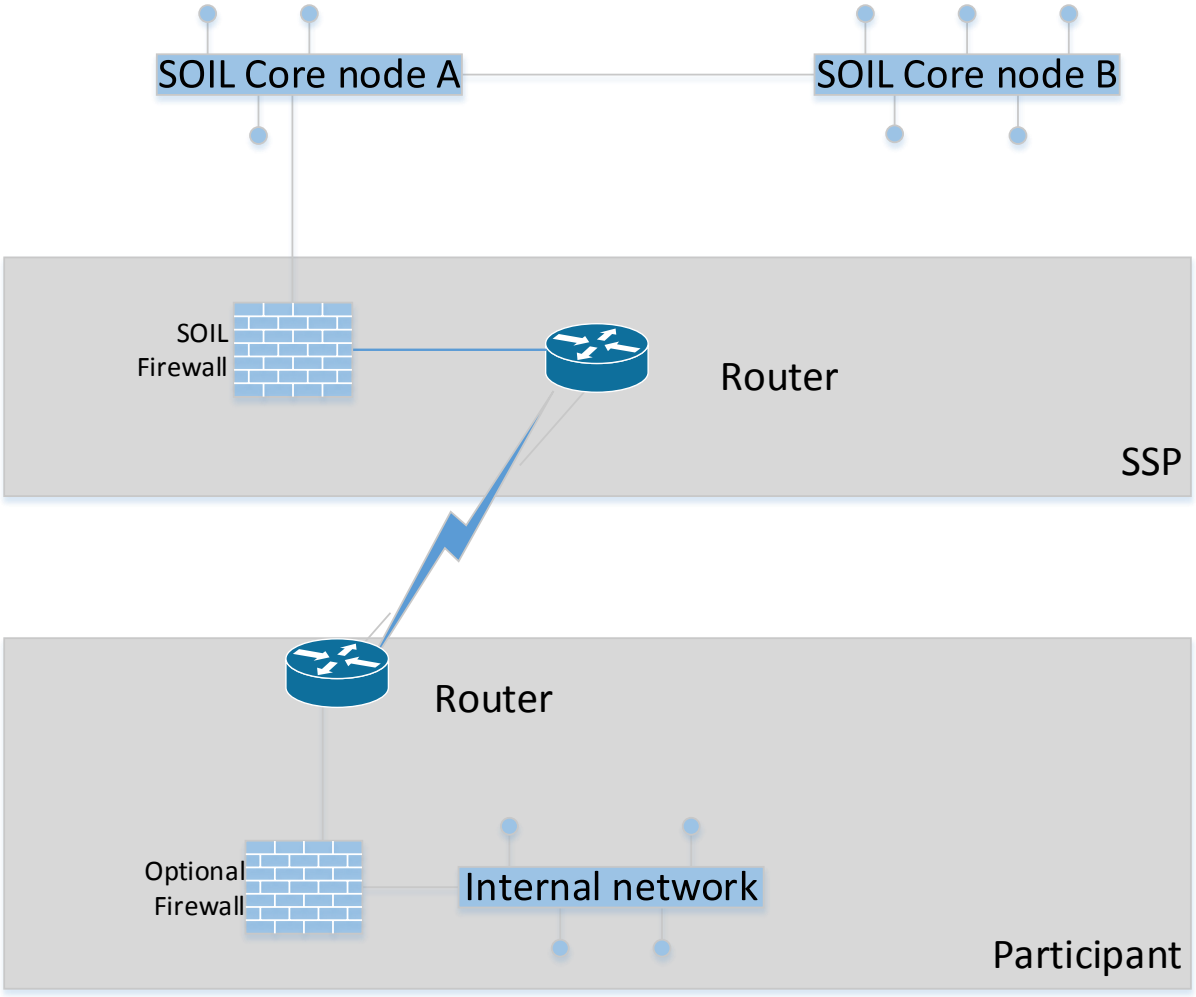
4 Connection alternatives

The Connection Patterns described in this Chapter are examples of possible ways to connect to SOIL via a SSP.

Fine grained technical properties of your internal network is not covered by this Guide, who aims to assist in the choice of SOIL main connection configuration between your network and SSP(s). Distributed SOIL routing to your organisation's various locations is an internal matter.

4.1 Connection Pattern 0 – Typical

The typical connection for SOIL access is high-speed fibre or access via a MPLS network to your chosen SSP.



4.2 Connection Pattern 1 – Low cost

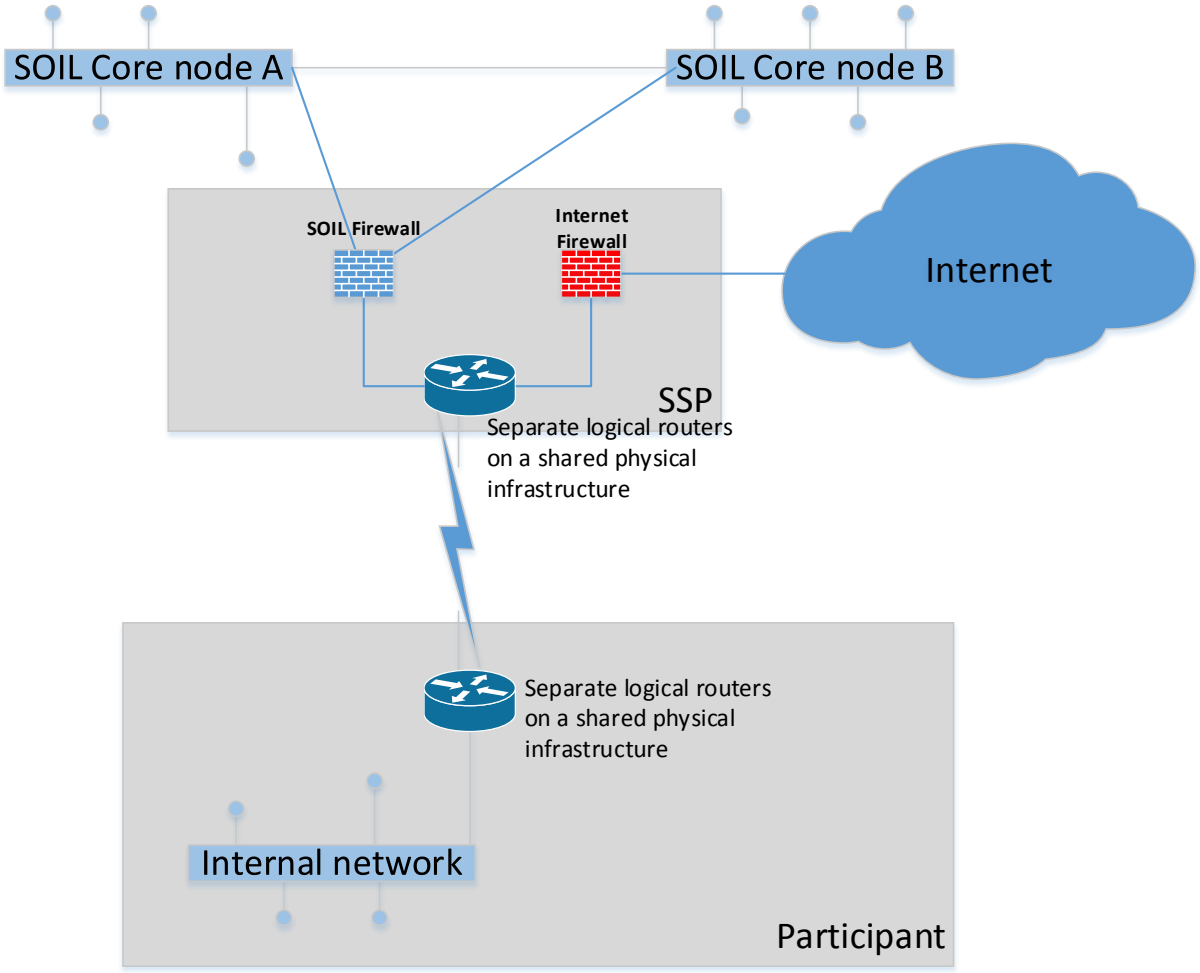
Participants in need of a low cost solution should consider:

1) Can we combine the line for SOIL connection with delivery of Internet access? (Requires logical barriers between SOIL and Internet traffic)
2) Do we need an SLA?
3) What is the bandwidth we normally need, and peak level?

Bandwidth requirements drive price on both line and mandatory SOIL firewall service provided by SSP. SOIL usage normally has relatively low concurrency rate.

Advice:

- Make sure your bandwidth requirements are quite moderate to begin with, as increasing bandwidth later should be relatively strait forward
- Make sure your contract for line and other SOIL access services include details on how to handle adjustments in bandwidth/capacity requirements.
- Remember to ask for price for later adjustment of data rate for line and SOIL-firewall.
- The SSP is obligated to handle critical Incidents 24x7, but otherwise they are only required to give technical support 8-16 on Norwegian working days.
- Make sure you do not state any requirements beyond this if you want to keep the price as low as possible.



4.3 Connection Pattern 2 – High availability and resilience

If you need as high availability and resilience as possible, 24x7, you need to consider:

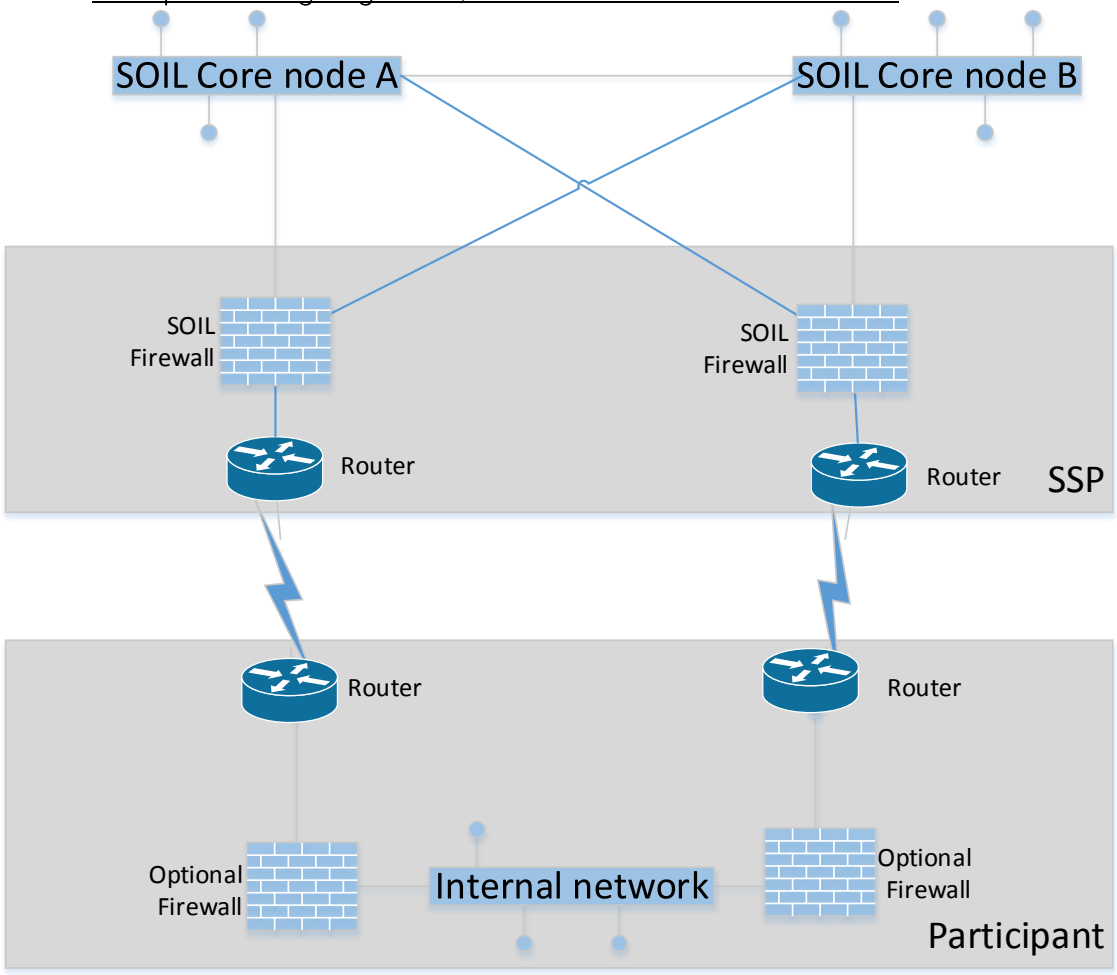
1) Will you benefit from using more than one SSP, so that issues at one SSP do not stop your SOIL connection?
2) Are you capable of utilising more than one SSP connection?
3) What is the cost/benefit?

If you answer positive to the questions above then you should probably use more than one SSP. Some precautions for the design:

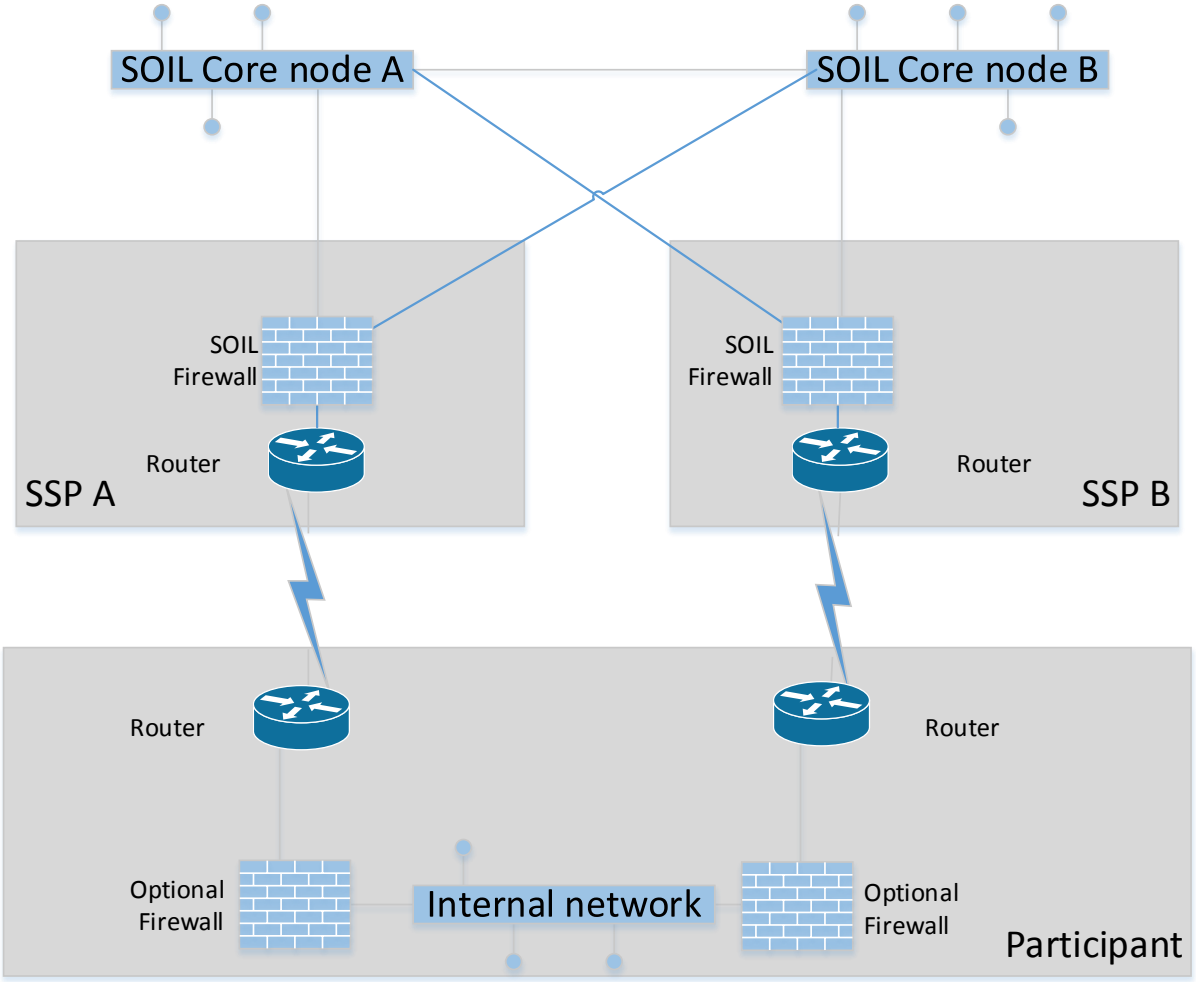
A) Make sure lines follow **separate physical paths**, and do not share infrastructure at your end. This is relevant both for lines between your infrastructure and the SSPs, and the lines between SSPs and the SOIL Core nodes.
B) Evaluate use of redundant routers at your side.
C) If you use firewalls at your end in addition to the SSP's SOIL firewall, should you make these redundant?
D) Is your IT organisation capable of utilising two SSPs or do you need to add some capabilities (i.e. skills)?

The following sections include examples of alternative setups to be considered.

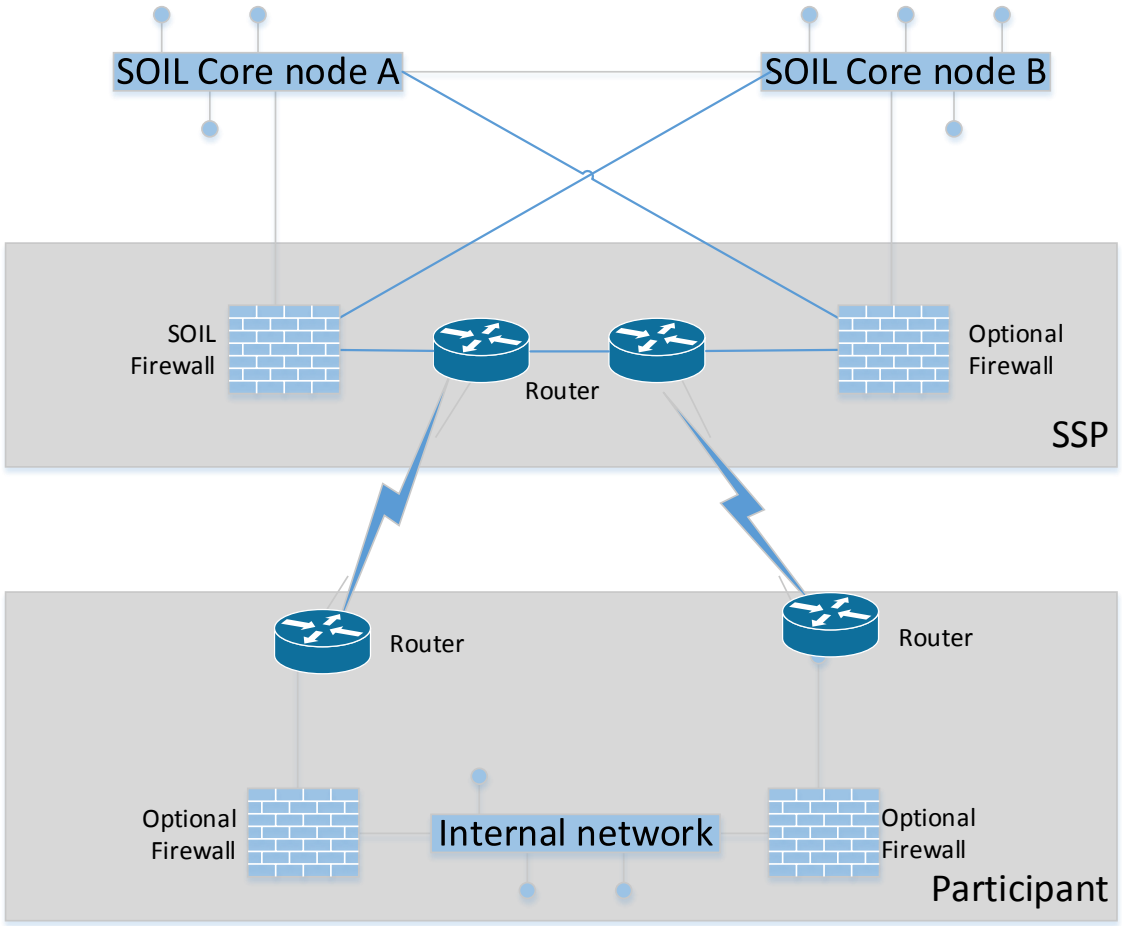
4.3.1 Example 1: Using single SSP, but with redundant lines and sites



4.3.2 Example 2: Using two SSPs for redundancy

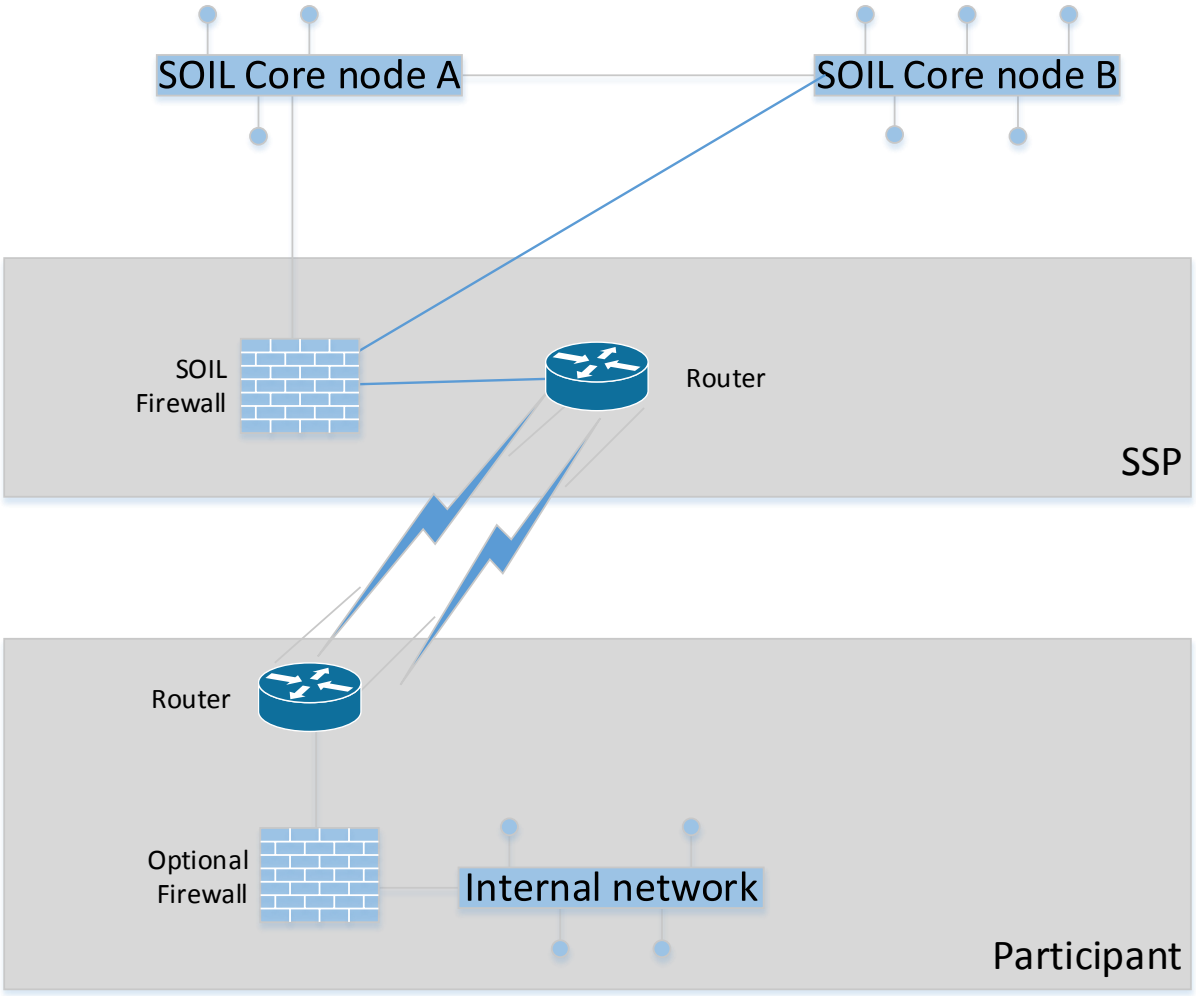


4.3.3 Example 3: Using single SSP with one site, but redundant infrastructure



4.3.4 Example 4: Using single SSP without redundant infrastructure, but with redundant lines

Make sure the redundant lines follow separate paths, and do not share infrastructure at your end, if practically possible.



4.4 Connection Pattern 4 – Connecting from a non-Scandinavian country

The intention of SOIL is an industry network independent of other networks, especially Internet. To support this intention you should pursue use of line circuits separate from Internet as the default choice. Some of the SSPs do have global networks, spanning most Oil & Gas related countries in the World.

The alternative is to request quotas from the SSPs for a VPN tunnel with fail-over.

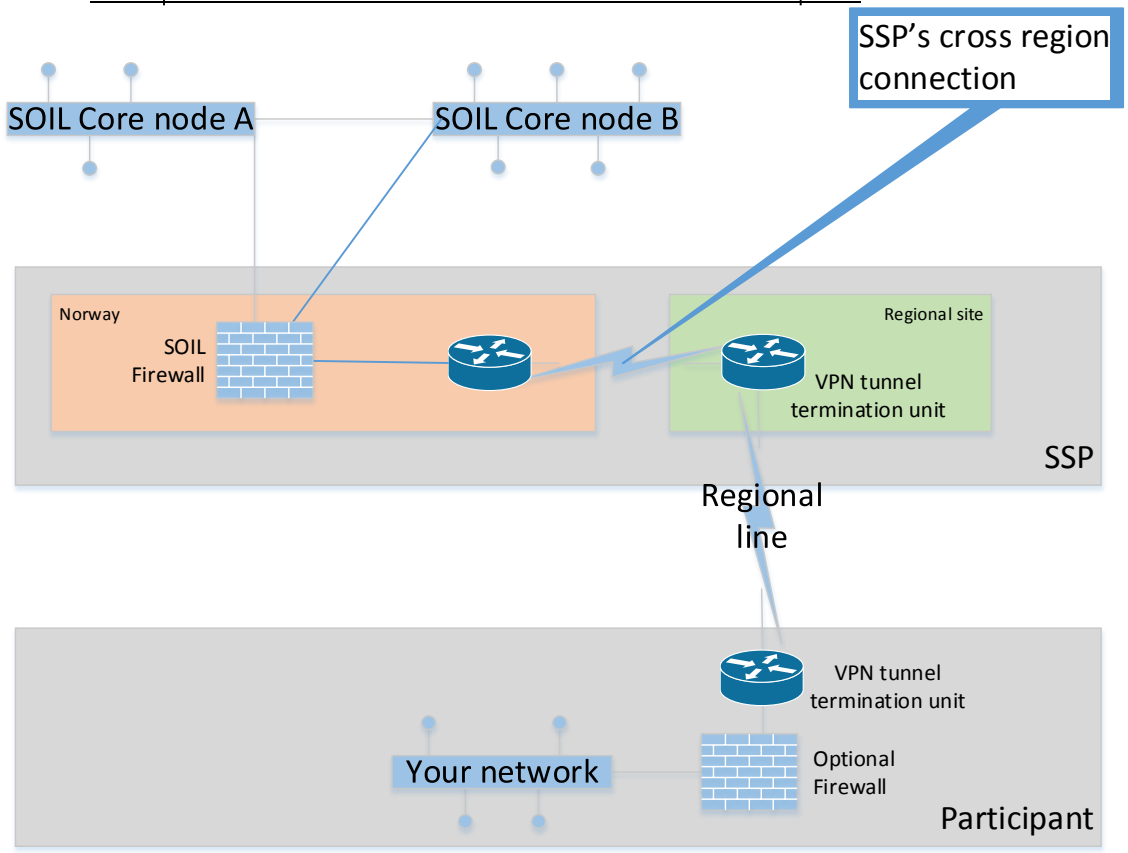
- The VPN must have two nodes on the SSP side:
  - One in Norway
  - One in another country, with route to SOIL independent of Internet, from the SSP's node in the other country than Norway.
- You should consider use of redundant connection equipment and locations at your side as well, but this is not mandatory.

VPN over Internet do not enable any specified Service Level Agreement for the connection!

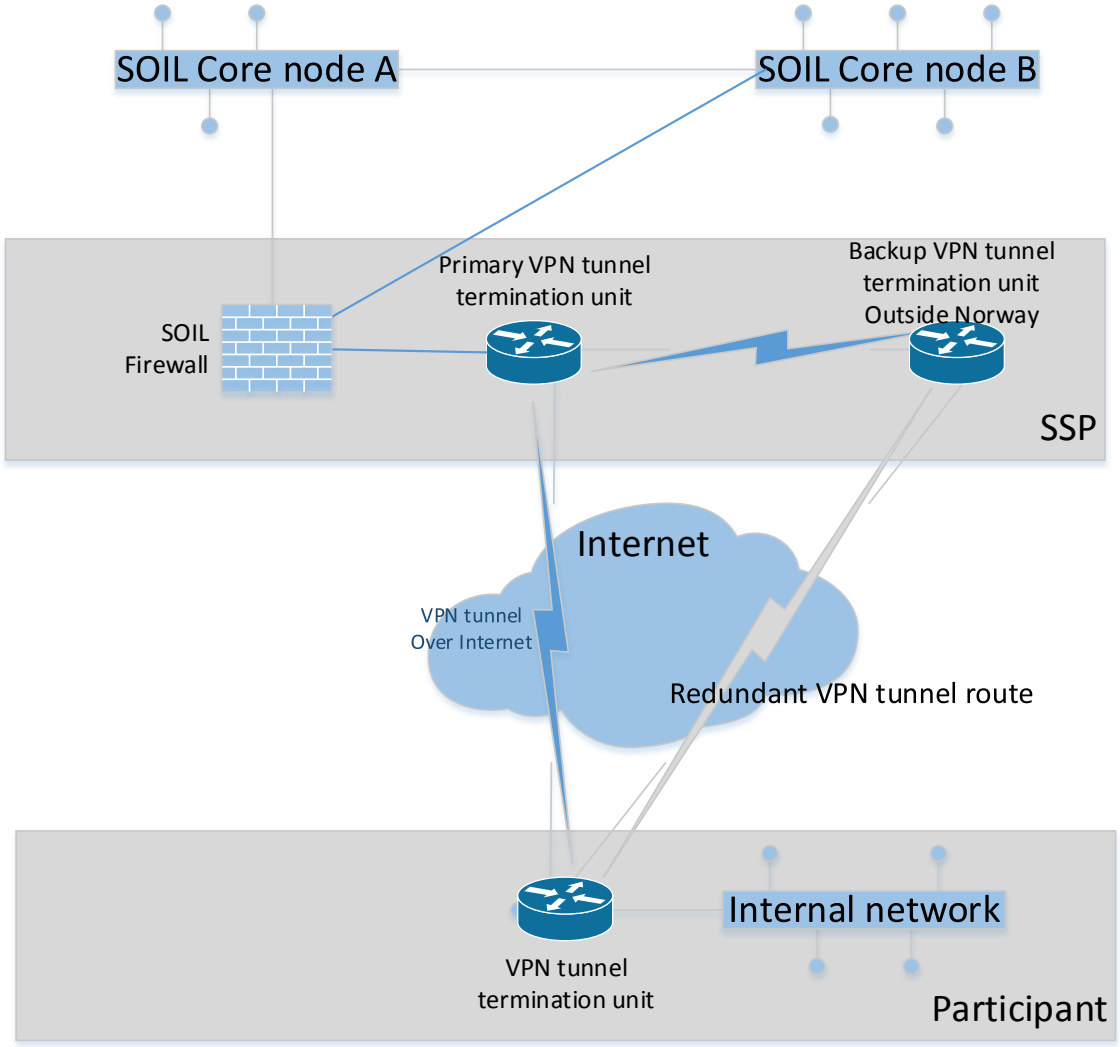
When delivering VPN based accesses to Participants the SSPs are enforcing a set of specific requirements as defined by EPIM. These requirements define the basis security level for connecting to SOIL using VPN over Internet. The Participant may state more strict requirements in the agreement with the chosen SSP(s) in addition, but not less.

As you probably are aware of the perceived quality of the SOIL connection depends on available bandwidth on your Internet connection.

4.4.1 Example 1: Leased line to an SSP's nearest connection point



4.4.2 Example 2: Use of VPN tunnel



5 Technical properties of SOIL

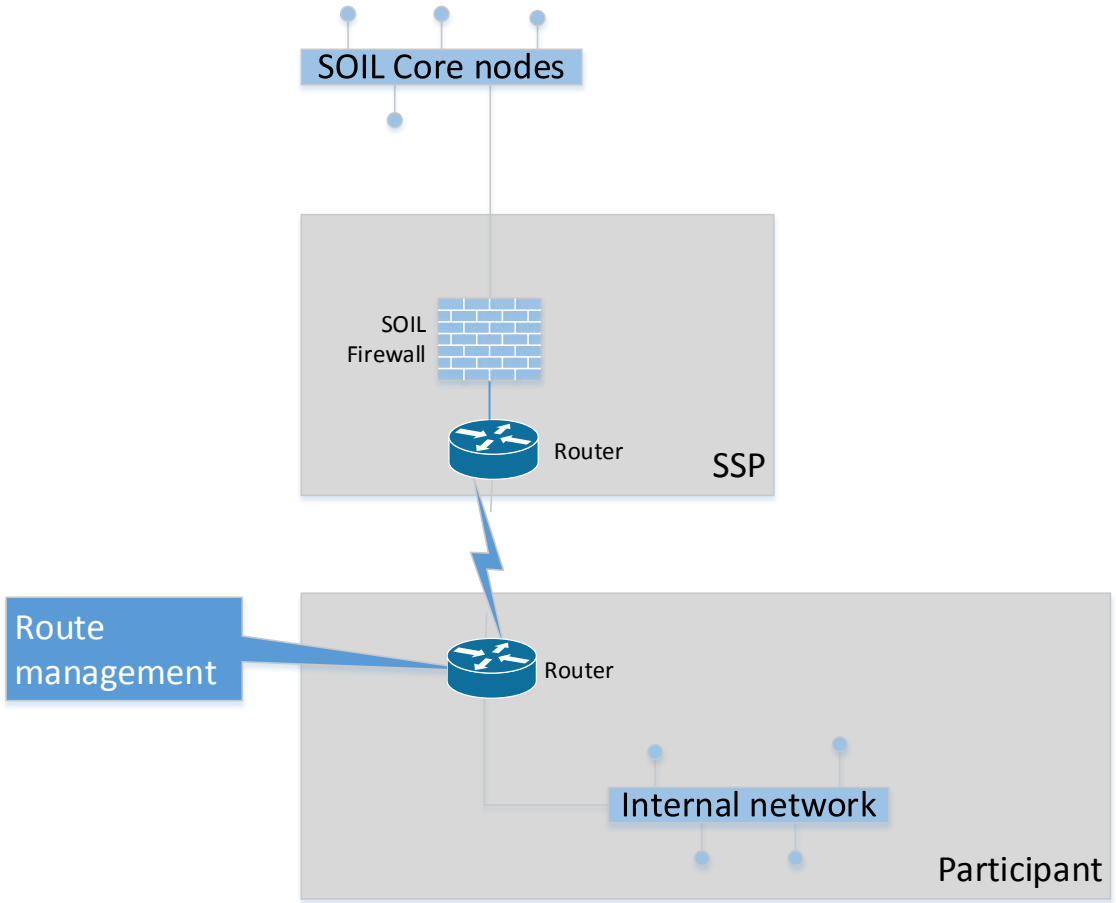
5.1 SOIL Firewall and Routing

All SOIL Participants must subscribe to the mandatory SOIL firewall service from SSP(s).
Due to internal policies in your company, you may still need to maintain your local SOIL firewall. This does not remove the need for subscribing to the mandatory SOIL firewall service from your chosen SSP(s), which is a requirement to ensure a predictable security level for all SOIL Participants and enable EPIM to audit and report the security level.

Consider the following as examples only, please discuss with SSP(s) for more details and alternatives.

5.1.1 Example 1: SOIL connection with only SSP mandatory SOIL Firewall

The Participant Router receives all relevant SOIL routing information from the SSP by either a dynamic routing protocol or automated/manual routines. Details of what is possible and how it is done may depend on SSP's SOIL firewall implementation, but as a general rule there will always be specific routing information for SOIL access present on the Participant's Router.



The Participant has several options:

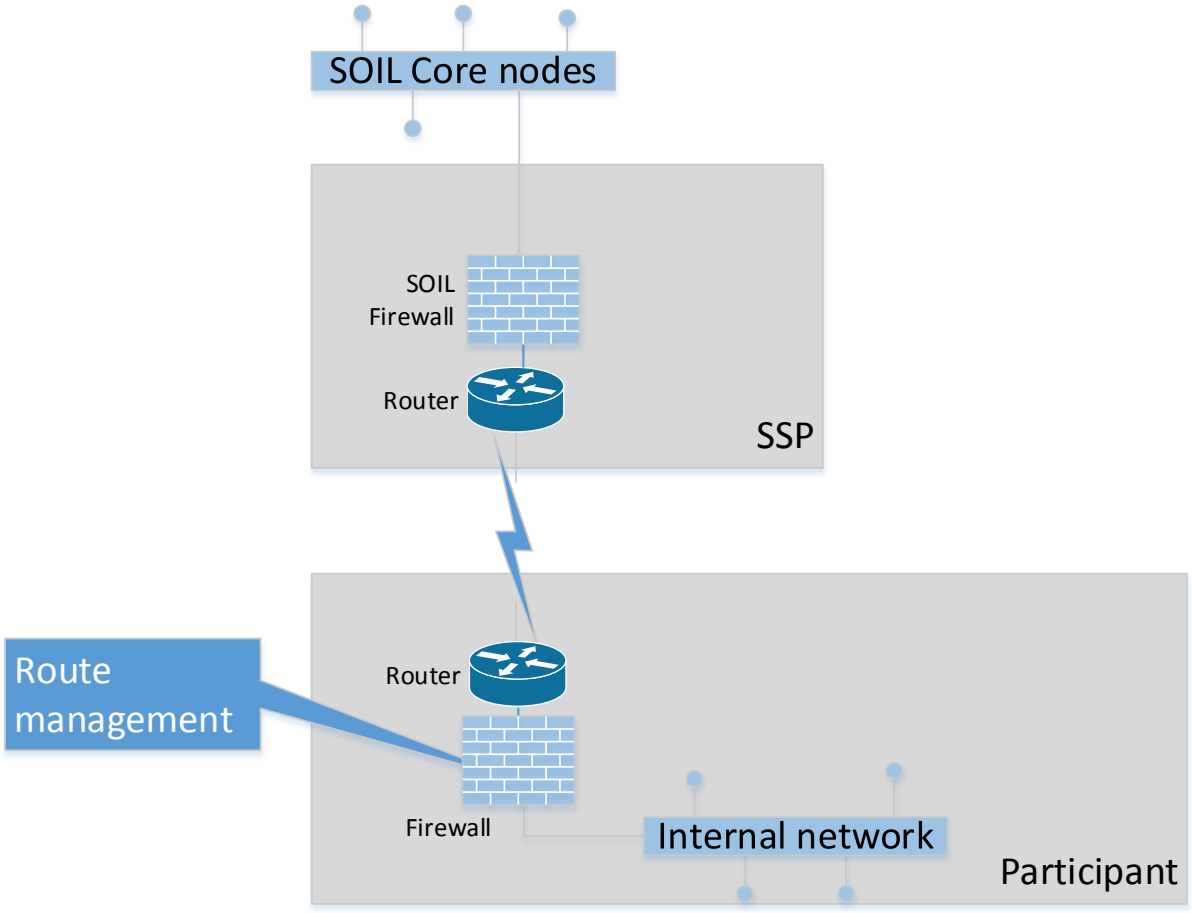
a) Establish dynamic routing between its internal routers/L3 switch and the Participant Router, so that the internally routers learn SOIL route entries for everything you need to access on SOIL.

b) Use the Participant Router as default-gateway for clients on the local subnet. This requires that Participant Router have a default-route to your Internet Firewall, and specific entries for what is needed on SOIL.
c) Manually add static route entries to internal routers/L3 switch for SOIL route entries for everything you need to access on SOIL.

With option a) and b), there is no need for manual updates to access SOIL. The Participant Router holds the specific route entries needed for SOIL access, and the SOIL-GW get updated from the SSP.
With option c) you need to add the necessary routing yourself to the core router or L3 switch, and point routing to the Participant Router.

5.1.2 Example 2: SOIL connection with SSP firewall, plus local SOIL Firewall

Your optional extra local SOIL firewall may be single/redundant/distributed, we name it "Participant-FW" for the rest of this example.
The Participant-FW may be either a dedicated SOIL firewall or the same firewall you use for Internet. There is not a requirement that the your local SOIL firewall is dedicated or separate, since there is already a dedicated mandatory SOIL firewall provided by the SSP.



The Participant Router will connect to "Participant-FW" on a dedicated SOIL interface or VLAN.
In this scenario, you need to maintain local firewall rules in addition to routing to SOIL on your Participant-FW.
Some Firewalls support dynamic routing, if true in your case:
a) Either establish dynamic routing between the internal routers/L3 switch and the Participant Router, so that the internally routers learn SOIL route entries for everything you need to access on SOIL.

b) Or use the Participant Router as default-gateway for clients on the local subnet. This requires that Participant Router have a default-route to Participant's Internet Firewall.
c) Or manually add static route entries to internal routers/L3 switch for SOIL route entries for everything the Participant need to access on Soil.

With option a) and b), there is no need for manual updates to access SOIL. The Participant Router holds the specific route entries needed for SOIL access, and the Participant Router gets updated from the SSP.
With option c) you need to add the necessary routing yourself to the core router or L3 switch and point routing to Participant Router.

5.2 IP addresses

SOIL supports IPv4 and IPv6. Currently the only use is IPv4, but be prepared for supporting IPv6 in the future, as the lack of available IPv4 addresses needs to be addressed for SOIL.

Only public IP addresses are allowed to be used on SOIL. You will need at least one address for your users' access to SOIL, using NAT (Native Address Translation). Services you may want to offer to the SOIL community also needs one or more public IP addresses.

The public IP addresses can come from various sources:

1) From the SSP.
2) The Participant may own IP address ranges.
3) From the Participant's Internet provider, but then separate address segments should be allocated for SOIL use only.
4) From the Line provider.

5.2.1 Change of IP addresses

Some actions are necessary if you want to change public IP address from the original configuration.

If you want to change the address used for consumption of SOIL applications/services, by your organisation's users, you need to collaborate with your SSP. Your collaboration partners on SOIL needs to open their SOIL firewall for the new address or segment to be used, and close the old one. Ask your SSP for assistance or advice for communicating the change. Your SSP needs to execute the changes on your side anyway.

For services you provision to SOIL, you need to inform the consumers of the service (i.e. other Participant organisations) in collaboration with your SSP. You will also need to change the DNS record for your service accordingly. Some of the consumers might have a local IP configuration pointing to your service, as a mean to ensure availability also in case Internet-DNS is unavailable. Ensure the consumers, of your service, are informed about the new IP address accordingly.

5.3 DNS

You need to consider how your users will resolute URLs to IP addresses for SOIL in case Internet is unavailable. The intention of SOIL is to offer a resilient alternative to Internet, to ensure NCS-operation do not suffer from a large scale Internet attack/failure. To ensure this you need to consider the easiest way to ensure your users/machines can reach critical SOIL services independent of Internet DNS.

Ask the SSPs for alternatives in the selection process or request support from your SSP.

5.4 Technical support

During the process of choosing one or more SSPs you may contact the SOIL Core Operator for technical advice. This is a payable service by your company.

Contact information for SOIL Core Operator service desk via email.

E-mail: gmdc@atea.no

Important!
Include the following in the email **Subject field**:
"Request for assistance: SA0011864 – EPIM SOIL – [#COMPANY#]"
, where you replace #COMPANY# with the name of your company.

After concluding contract with an SSP you should rely on the SSP to give technical support. SOIL Core does not provide a common service desk to all Participants.