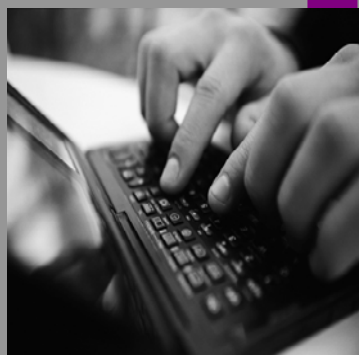

How-to Guide

SAP NetWeaver 7.0

How to…

Set Up the Landscape for a Federated Portal Network

Version 6.00 – January, 2008

Applicable Releases:
SAP NetWeaver 7.0 SPS 13 and higher

Contents

Document History

Version	Description
1.00	First release
2.00	Scenario 4: Internal Network Reverse Proxies removed
3.00	Scenarios tested; opening qualification note removed; note on location of limitation descriptions maintained
4.00	Scenario added specifically for Remote Delta Link usage of FPN
5.00	Change in title (from *How to… Set up Federated Portal Network Scenarios with Reverse Proxies*), with the intention of widening the scope of the guide New section, *Selected Network Scenarios*, relating to alternative configurations and features in network setup
6.00	Integration of distributed minor corrections

1. Introduction

The IT landscape environments at customer sites can be varied and complex network scenarios, which are likely to consist of multiple domains, networks and sub-networks. Adding the implementation of a federated portal network may involve additional network components and further complicate setup and configuration.

The scope of this guide includes the following:

- The presentation of several network scenarios with the main purpose of illustrating the components that may comprise them
- An emphasis on the configuration of reverse proxies with a federated portal network, also illustrated by several different scenarios

Purpose and Audience

Considering the multitude of possibilities for network configurations in different organizations, the aim of this document is to provide such information and instruction as will aid IT personnel in analyzing setup requirements of their systems more easily when implementing a federated portal network.

This document is intended for IT personnel and system administrators and assumes professional knowledge of network systems and their configurations, including such elements as DNS servers, firewalls, load balancing, just to name a few.

More Information

To find out more about the implementation of a federated portal network, including concepts and related business scenarios, go to the SAP Help Portal at *http://help.sap.com/nw70* → *SAP NetWeaver Library* → *EN.* In the documentation structure, navigate to *SAP Library* → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *People Integration by Key Capability* → *Portal* → *Portal Scenarios (Running an Enterprise Portal)* → *Implementing a Federated Portal Network*.
Link:
http://help.sap.com/saphelp_nw70/helpdata/en/5b/9f2d4293825333e10000000a155106/frameset.htm

For a detailed limitation statement, see **SAP Note 853509**, the central limitation note for NetWeaver 2004s.

Also see the central note for federated portal nework issues, **SAP Note 880482**.

2. Selected Network Scenarios

This section presents, in order of complexity, four scenarios selected to illustrate some of the variety of features it is possible to introduce and configure into an organizational network system that implements federation.

The figures included are high-level illustrations, primarily relating to interserver communication. They are not intended to reflect existing real-time scenarios.

Performance and Maintenance

It must be said in advance that for best performance, and to facilitate installation and maintenance, it is recommended to keep the federated portal setup as simple as possible. For example:

- Evaluate your SSL strategy in advance. Analyze what data is being passed between the federated instances.
- Identify your network domain and distances between the federated instances. Where and how can you improve on network speed?
- Reduce network latency between components to a minimum

However, since real-life scenarios may require more complex network setups driven by demanding security policies, configuration possibilities are shown below to illustrate some of the features that are available and may need to be taken into consideration.

This does not imply that the inclusion of these features, or their configuration in the illustrations, are recommendations. The intention is, rather, to show possibilities that may be used or varied as best suits the customer.

2.1. Direct Connection

Figure 1 shows the simplest scenario, using HTTP client protocol with additional appliances that often exist at customer sites. Though not a likely example for most organizations it serves as a starting point from which systems can become incrementally more complex.

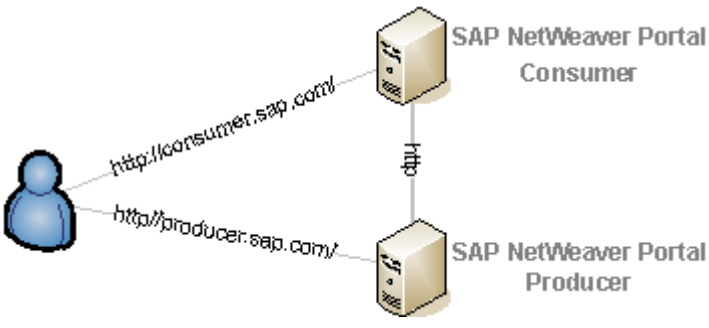

Figure 1

2.2. Direct Connection with Internal Load Balancing

Figure 2 adds to the direct connection the load balancing at the connection between the consumer and producer portals.

Here communication is by means of an SAP Message Server and load balancing is achieved internally, with the software residing on the portal server, or more than one server, if in a clustered environment. This is an alternative to having load balancing taking place on an additional intermediate machine.

Figures 1, 2, and 3, show the consumer-producer connections, whether direct, via SAP Message Server, firewalls, or reverse proxy, implemented by HTTP. If you are using a P4 connection with a firewall between the consumer and producer, be sure to configure the firewall accordingly. See the section Configuration for Remote Delta Link Usage about using P4 connections with a federated portal network.

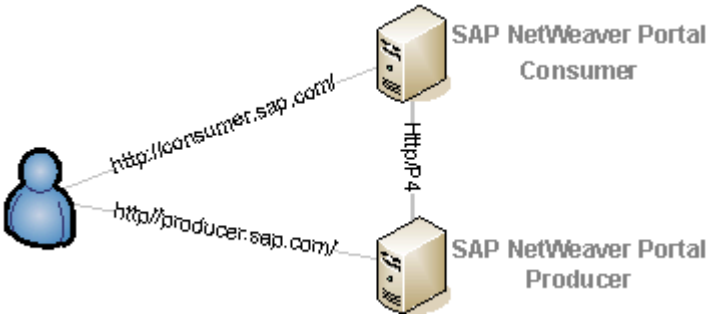

Figure 2

2.3. Adding Firewalls and Reverse Proxies

In the example in figure 3, firewalls, using SSL termination on front-end reverse proxies, and using reverse proxy for the consumer-producer connection are added. (**SAP Note 812901** offers hints about dealing with SSL termination.)

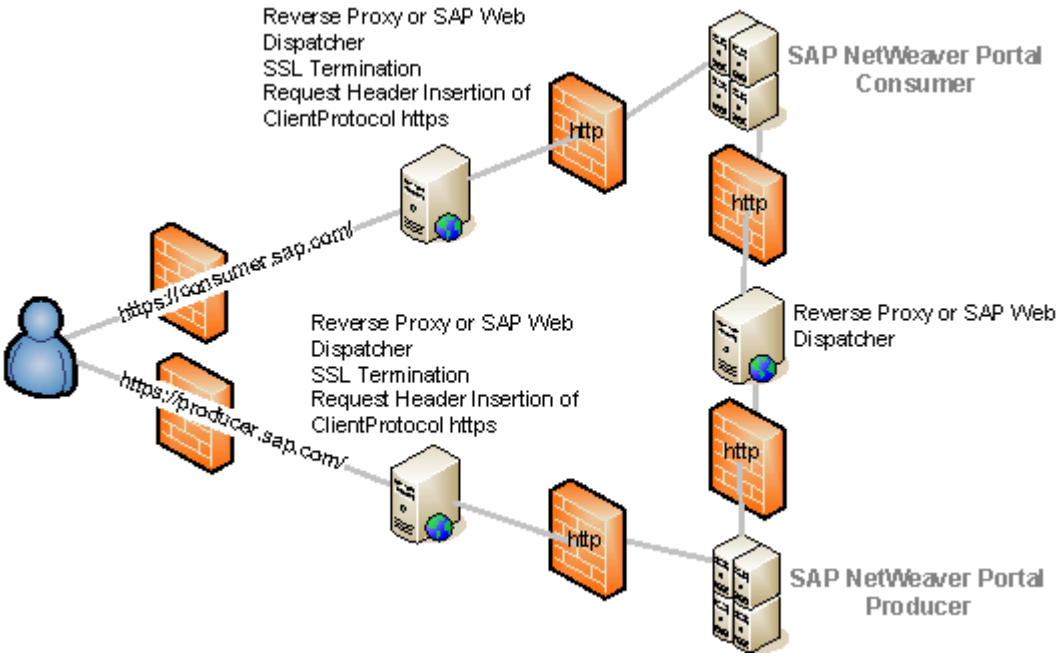

Figure 3

2.4. Early SSL Termination and External Load Balancers

The following illustration, figure 4, introduces a number of additional elements: SSL Termination via Load Balancer, followed by a virus scanner appliance and intrusion detection sensors, combined with firewalls and load balancer for the connection between the consumer and producer portals.

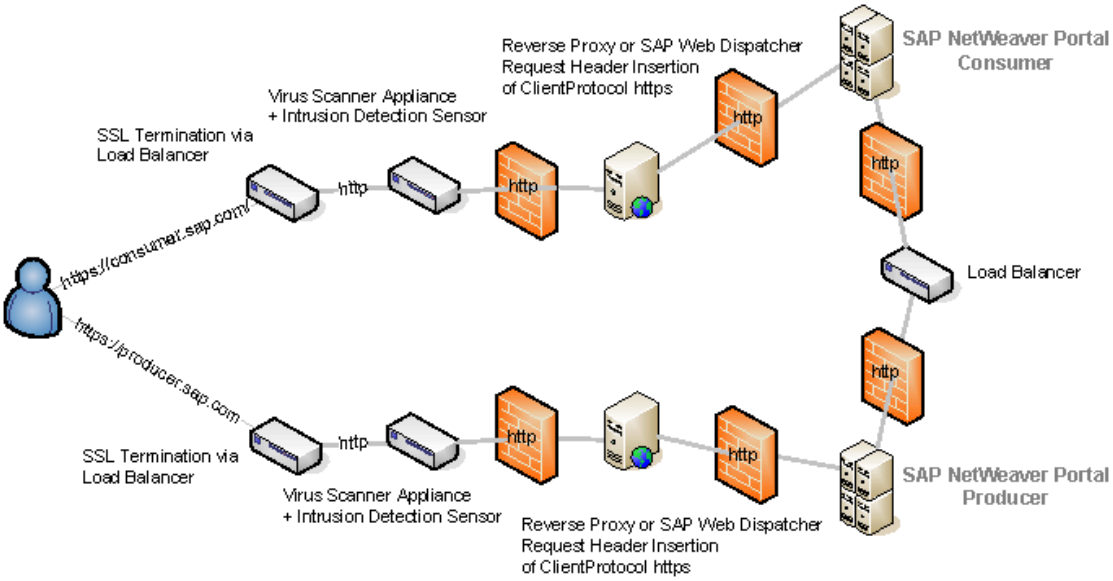

Figure 4

3. Setting up Federated Portal Network Scenarios with Reverse Proxies

Use

For reasons of security, load distribution and the caching of static content, reverse proxies are a common and generally necessary part of the network scenario in large organizations. The configuration of proxy parameters in a standard SAP NetWeaver Portal scenario is straightforward and is described in the portal administration documentation on the SAP Help Portal at *http://help.sap.com/nw70* → *SAP NetWeaver Library* → *EN.* In the documentation structure, navigate to *SAP Library* → *SAP NetWeaver Library* → *SAP NetWeaver by Key Capability* → *People Integration by Key Capability* → *Portal* → *Portal Administration Guide* → *System Administration* → *System Configuration* → *Service Configuration* → *System Properties for Proxy Server*.
Link:
http://help.sap.com/saphelp_nw70/helpdata/en/33/8abf9e0ce011d7b84900047582c9f7/frameset.htm

Purpose

This section provides information about three network scenarios involving reverse proxies. Though none of the scenarios may define a real-life network environment, such an environment would encompass a combination of all or some of the scenarios presented here. Furthermore, it is assumed that in a scenario with one portal, there is an existing reverse proxy in use; here, the implementation of a federated portal network broadens scope of configuration and setup issues in the network involved. The aim here is that the following descriptions and instructions will help to facilitate analyzing the setup and configuration requirements of their systems.

Some points to keep in mind are:

- When configuring a scenario with a reverse proxy, there are likely to be issues to consider, which are required for that scenario but are not specific to the federated portal network implementation.

  For example, there may be a requirement of some back-end applications to be in the same network zone as the producer and consumer, and, indeed, that the producer and consumer be in the same network zone. This, however, would not be a requirement specific to the federated portal.

- The opposite may also be the case, that some back-end technologies are affected by federated portal network limitations.

  For example, using object-based navigation within a federated portal network is supported, but federation places limitations on OBN technology. Refer to *Using Object-Based Navigtion* in the federated portal documentation referenced earlier.
  Link:
  http://help.sap.com/saphelp_nw70/helpdata/en/fe/cb40b1e98f4e69b9af0077c79b67c3/frameset.htm

In any event, it is not within the scope of this document to cover all the possibilities.

3.1. The Environment

Figure 5 illustrates a basic scenario of network zones, starting with the end user in the Internet zone, through the DMZ, including firewalls and reverse proxy, and on to the federated portal consumer and producer portals, communicating with each other in the internal zone.[1]

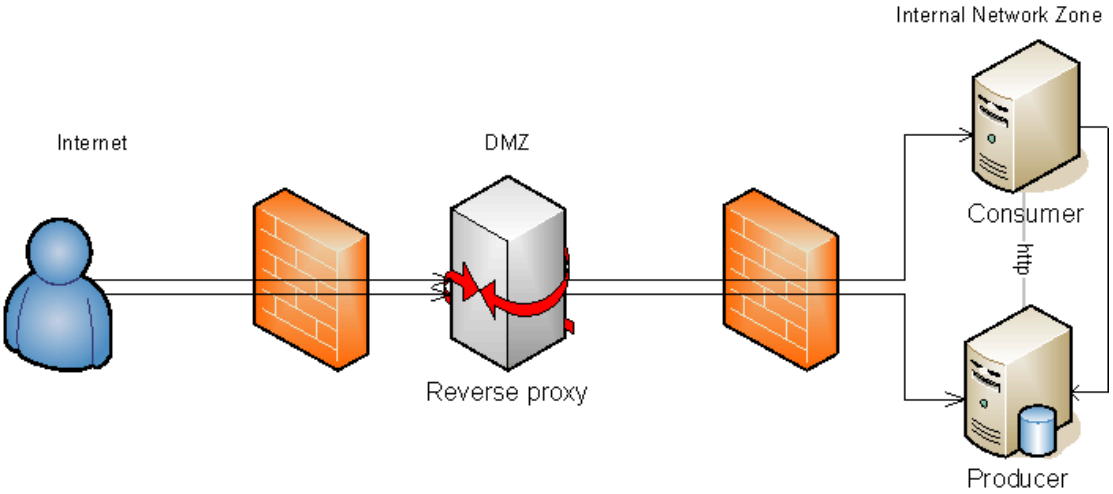

Figure 5

This basic environment serves also as the model for Scenario 1 below.

The Basic Flow

1. The end-user request is directed via the reverse proxy to the consumer portal.
2. The consumer portal returns HTML content.

   However, if some of the requested content is not available from the consumer portal, the HTML content returned by the consumer portal will be redirected (either as HTML or, possibly, some JavaScript activated from the browser) to the producer portal to complete the content.

What to Configure

The common deployment scenario of the SAP NetWeaver portal consists of a consumer portal, a producer portal, a DMZ between them, and the client browsers (end users). Often, in real-world scenarios, a consumer portal communicates with a number of producer portals. For the sake of simplicity, we will look at a single consumer-producer scenario.

The general configuration requirements are:

1. Adding names to the DNS in the Internet zone
2. Setting rules on the reverse proxy
3. Configuring firewalls to support reverse proxy rules
4. Configuring the consumer portal

The consumer and producer machines do not have to be in the same domain.

[1] Using one reverse proxy to access two portals is only supported using dedicated virtual hostnames (using http), or even dedicated IP addresses (for SSL termination).

The following sections contain descriptions of the procedures involved for the above-mentioned configuration requirements (1-4) for four different scenarios.

Because of the vast diversity in firewall technologies on the market, and in use at different organizations, it is assumed here that the reader has the knowledge, or access to the knowledge, required to configure the firewalls onsite.

Hostnames

We will refer to the “internal” area of the network where the consumer portal and producer servers are located as the internal network; the user side of the DMZ is referred to as the external network.

The hostnames used for the portal machines (consumer and producer) on the internal network will be different from the hostnames used externally for these machines. The external hostnames may be dictated by branding or other issues and will generally be names recognizable and meaningful to the end user. On the other hand, it is the IT department that would be likely to dictate the internal names—recognizable to other servers on the network.

Focus on the Federated Portal Network (FPN)

Although much of the content in this document deals with what are general network-related issues, it is import to focus on those aspects that are essential for the federated portal network implementation to work successfully.

- Identifying, and ensuring access to, all the systems involved in the FPN.
- Setting additional remote content provider properties, if required
- Ensuring proper DNS resolution:
  - that each client knows its DNS
  - gets to the correct DNS server
  - avoids clashes with an identical DNS defined on another DNS server

3.2. Scenario 1: Simple Reverse Proxy Network

The simple scenario in Figure 6 is based on the generic illustration in Figure 1, with specific hostnames and IP address as examples.

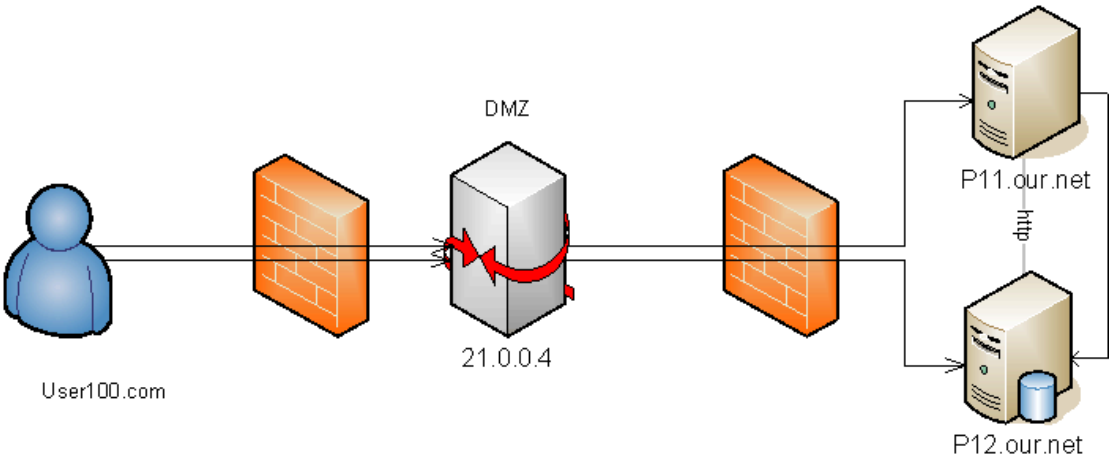

Figure 6

Configuration of the Network Devices

1. On the DNS server accessible to the end user, configure the world DNS of the "external network" hostnames both for the consumer and the producer portals to point to the IP address of the reverse proxy.

   For example:

   - **`consumer.myBusiness.com 21.0.0.4`**
   - **`producer.myBusiness.com 21.0.0.4`**

2. Configure the reverse proxy with rules to direct calls to the correct portal addresses.
   - **`consumer.myBusiness.com*`** => **`p11.our.net*`**
   - **`producer.myBusiness.com*`** => **`p12.our.net*`**
3. Configure the firewalls to support the reverse proxy rules.
4. Configure the consumer.
   a. On the consumer machine, navigate as follows: *System Administrator* → *Federated Portal* → *Myself as Content Consumer* → *Manage My Producers*.
   b. Double-click and deregister the producer portal so that it can be edited. (When it is registered its permission changes to read-only.)
   c. In the Property Editor, under the "Remote Content Provider" category, change the values of the following properties:
      - **`com.sap.portal.remotePortal.ExternalNetworkHostname`** to **`producer.myBusiness.com`** (for example)

        and

      - **`com.sap.portal.remotePortal.ExternalNetworkPort`** to the respective port

   d. Save and reregister the producer portal.
5. If there are multiple producer portals, repeat step 4 for each one.

3.3. Scenario 2: Two or More Reverse Proxies

This scenario may be considered a subordinate possibility of scenario 1, since it would only be possible with the installation of usage type EP Core (EPC), and probably only for an Intranet. Its description is included here for those cases in which it is needed. For those running this scenario, the emphasis is on ensuring proper DNS resolution.[2]

Sometimes two or more reverse proxies are directed to the same internal network. In the scenario illustrated in Figure 7, there are two user groups. The scenario is as follows:

- Group A is represented here by user A.
- Group B is represented by user B.
- User A and B are in different locations in the IT landscape of the organization.
- Both user A and user B access the same consumer portal, on **`ufn30.net`**, but through different reverse proxies.
- The consumer portal consumes content from the producer portal **`ufn20.net`**.

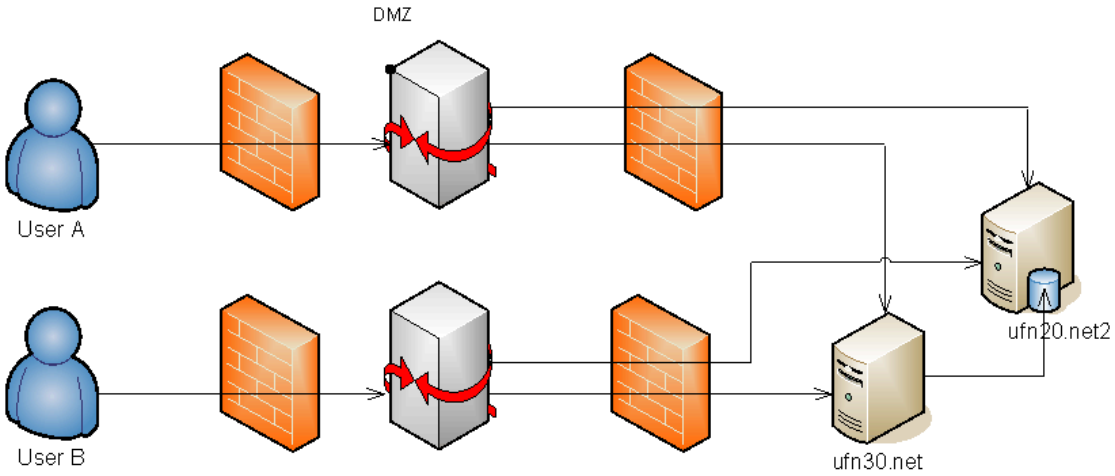

Figure 7

Configuration for Scenario 2

The configuration for this scenario is very similar to that of scenario 1 and the same network elements need to be configured for each user group:

1. Add names to the DNS on the user group domains.

   The main point in this scenario is that two separate reverse proxies are protecting the same consumer portal.

   - One alternative is to use two separate DNS servers for each user group.
   - It is also possible to define different "external network" hostnames for each user group, and to configure the world DNS of each, both for the consumer and the producer portals, to point to the IP address of the reverse proxy. (See scenario 1 for examples.)

2. Set rules on the reverse proxy.

[2] Using one reverse proxy to access two portals is only supported using dedicated virtual hostnames (using http), or even dedicated IP addresses (for SSL termination).

This is the same as described for scenario 1, for each reverse proxy.

Since the DNS configuration has the same names for some portals, some of the rules will be the same as well.

3. Configure the firewalls to support the reverse proxy rules.

   Same as scenario 1. Configuration to support the reverse proxy rules.

4. On the consumer portals.

   Do as described for the consumer for scenario 1.

3.4. Scenario 3: Internal Network Users

Scenario 3, illustrated in figure 8, describes a situation in which some users reside within the internal network. [3] Typically, these users are administrators.[4]

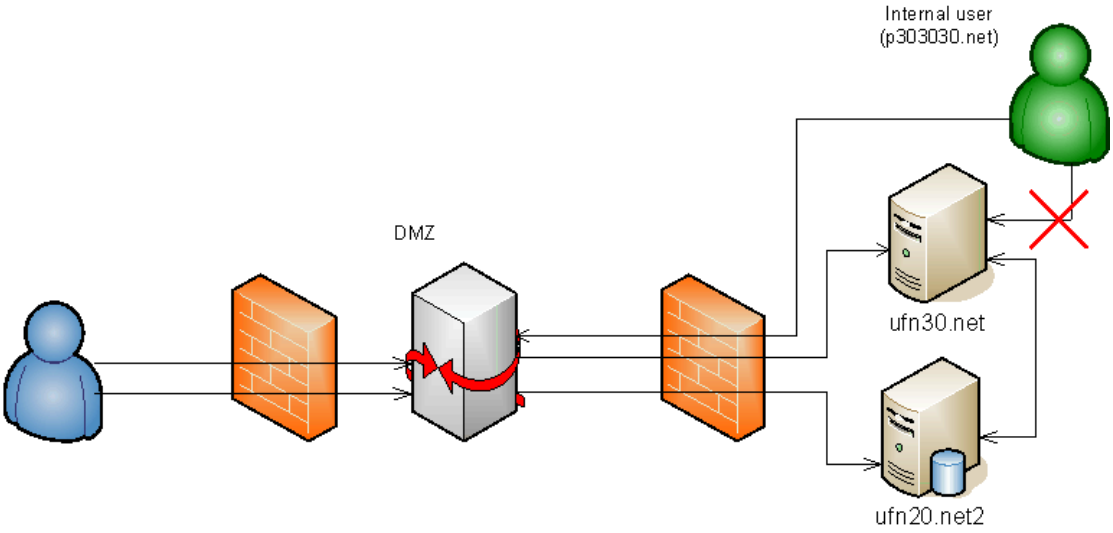

Figure 8

Configuration for Scenario 3

The configuration issues in this scenario are as follows:

- The internal user must also, just as the external user, access the portals in the internal network through the reverse proxy and therefore also requires DNS mapping to the reverse proxy, the same as in scenario 1.

  If the internal user accesses the portals directly, the portals will still generate URLs with the external network hostname, which would not be recognized by servers in the internal network.

  In a closed organization, the internal user may use the same DNS name from the same DNS server. This depends on the local landscape.

[3] Using one reverse proxy to access two portals is only supported using dedicated virtual hostnames (using http), or even dedicated IP addresses (for SSL termination).

[4] It would also be possible to access the portal directly from the internal user, without going through the DMZ, by proper internal DNS resolution.

- This scenario requires configuration of the firewall to allow internal users access to the reverse proxy from the internal network.

3.5. Configuration for Remote Delta Link Usage

The P4 port of the producer must be used in all configuration settings when both of the following are true (figure 9):

- The consumer portal obtains content from the producer by the remote delta link usage type
- The network landscape requires communication through a reverse proxy, not only between the user and consumer, but also between the consumer and producer machines.

Configuration may include:

- Setting reverse proxy rules
- Configuring firewalls to support reverse proxy rules
- Configuring load balancing
- Configuration settings made on the consumer

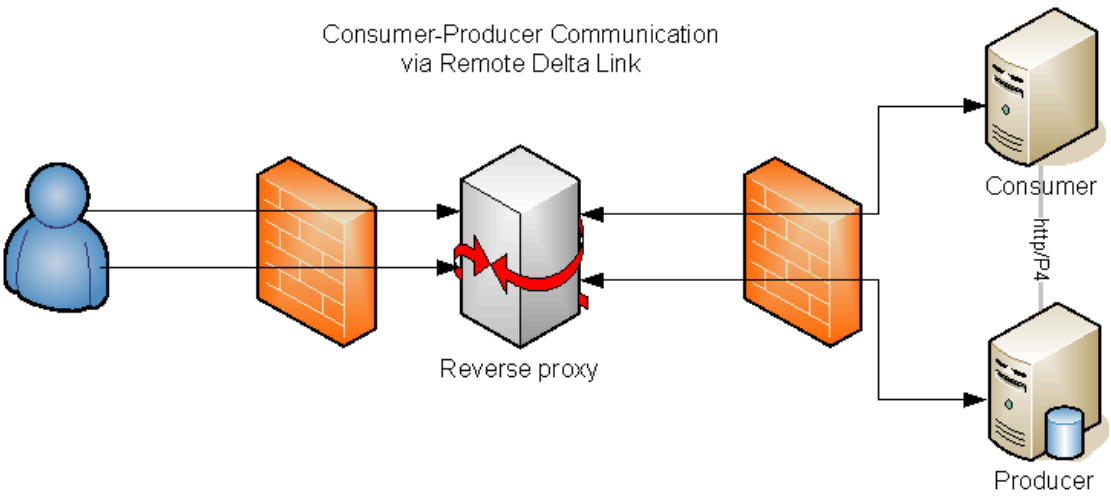

Figure 9

For SAP NetWeaver Portal SPS13 and Higher

Beginning with SPS13, configuration of the P4 port for both consumer and producer are performed on the consumer portal in two locations:

- When adding a producer (for entering P4 port of the producer)

  For creating a producer, see *http://help.sap.com/nw70 → SAP NetWeaver Library → EN.* In the documentation structure, navigate to *SAP Library → SAP NetWeaver Library → SAP NetWeaver by Key Capability → People Integration by Key Capability → Portal → Portal Scenarios (Running an Enterprise Portal) → Implementing a Federated Portal Network → Activities for Content Consumers → Adding Producers → Adding NetWeaver Producers*.

  Link:
  http://help.sap.com/saphelp_nw70/helpdata/en/43/222fc40bb93fece10000000a11466f/frameset.htm

- When registering a consumer with a producer (for entering P4 port of the consumer)

  For editing a producer instance and registration, see *http://help.sap.com/nw70 → SAP NetWeaver Library → EN.* In the documentation structure, navigate to *SAP Library → SAP NetWeaver Library → SAP NetWeaver by Key Capability → People Integration by Key Capability → Portal → Portal Scenarios (Running an Enterprise Portal) → Implementing a Federated Portal Network → Activities for Content Consumers → Configuring Producer Instances on Your Consumer Portal → Registering and Unregistering Your Consumer Portal*.

  Link:
  http://help.sap.com/saphelp_nw70/helpdata/en/43/223b360b413fe1e10000000a11466f/frameset.htm

For SAP NetWeaver Portal SPS12 and Below

In SAP NetWeaver Portal SPS12 and below, the portal by default takes the HTTP port and replaces the last digit with the digit 4.

Conversion Examples:

- HTTP: 50000 → converted to P4: 50004
- HTTP: 50007 → converted to P4: 50004
- HTTP: 51002 → converted to P4: 51004

If the resultant value is not the same as the P4 port on the producer (which may be the case as a result of load balancing or changes made by a system administrator, for example), you must update the `AliasToPorts` property of the portal service `ProducerInformationService` on both the consumer and producer portals according to the procedure described below.

Examples for when manual update of AliasToPorts service is necessary:

- HTTP port is 50000; producer P4 port is 50005 (however, the portal updates the P4 port to 50004 based on the existing HTTP port)
- HTTP port is 51000; producer P4 is 50004 (however, the portal updates the P4 port as 51004 based on the existing HTTP port)

Editing the Service on the Consumer

1. In the portal, navigate to *System Administration → System Configuration → Service Configuration* and, in the Portal Catalog, choose *Applications*.

   Step 1 applies to both the consumer and the producer respectively.

2. Find `ProducerInformationService`, right-click and choose *Configure*.
3. Update the port according to the format:

   `<producer_alias>=<producer_P4port_number>`

   For example:

   `alias1=50004;alias2=56004`

4. Save and restart the service.

   To restart the service:

   a. Right-click the service, choose *Administrate*, and click *Restart* for `ProducerInformationService`.

   b. Next to *Action*, click *Restart*.

Editing the Service on the Producer

Repeat steps 1-4 on the producer portal; however, in step 3 enter the P4 port of the consumer portal according to the format:

<consumer_name>=<consumer_P4port_number>

For example:

consumer1=50004;consumer2=56004

3.6. General Rule/Limitation

No scenario works with mixed http/https protocols. Although it is possible, when registering multiple producers, to use either protocol in the producer definition, it must be clear that when a request is made to the consumer using HTTP, the subsequent request to the producer must also use HTTP. Likewise, if the request to the consumer uses HTTPS, the consumer must be registered with the producer using HTTPS. Mixing protocols may interfere with proper implementation of the federated portal network.

http://www.sdn.sap.com/irj/sdn/howtoguides