SAP NetWeaver '04

Security Guide

Network and Communication Security

Document Version 1.00 – May 11, 2004

THE BEST-RUN BUSINESSES RUN SAP

THE BEST-RUN BUSINESSES RUN SAP

SAP AG
Neurottstraße 16
69190 Walldorf
Germany
T +49/18 05/34 34 24
F +49/18 05/34 34 20
www.sap.com

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

Disclaimer
Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressively prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP's Support Services and may not be modified or altered in any way.

Documentation in the SAP Service Marketplace
You can find this documentation at the following Internet address:
`service.sap.com/securityguide`

Typographic Conventions

Type Style	Description
Example Text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, graphic titles, and table titles
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example text`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, *F2* or *ENTER*.

Icons

Icon	Meaning
⚠	Caution
🗨	Example
💡	Note
🧭	Recommendation
SYN	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help → General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

Contents

Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business and your needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the SAP System database or files. Additionally, if users are not able to connect to the server LAN, they cannot exploit well-known bugs and security holes in network services on the server machines.

Again, your strategy and your priorities are the most important factor in deciding which level of security is necessary for your network infrastructure. We do offer general recommendations when establishing your network topology, which include using a firewall and other intermediary devices, which include the SAP Web dispatcher and the SAProuter, to protect your local network. To protect SAP System communications at the transport layer, the SAP NetWeaver products support the use of the Secure Sockets Layer (SSL) protocol and Secure Network Communications (SNC).

> Depending on your current situation, you may not be able or willing to implement the described secure network setup. However, we do offer suggestions and recommendations at various security levels. If the plan described here does not fit your needs, contact our consultants, who are also available to assist you in the process of setting up your network securely.

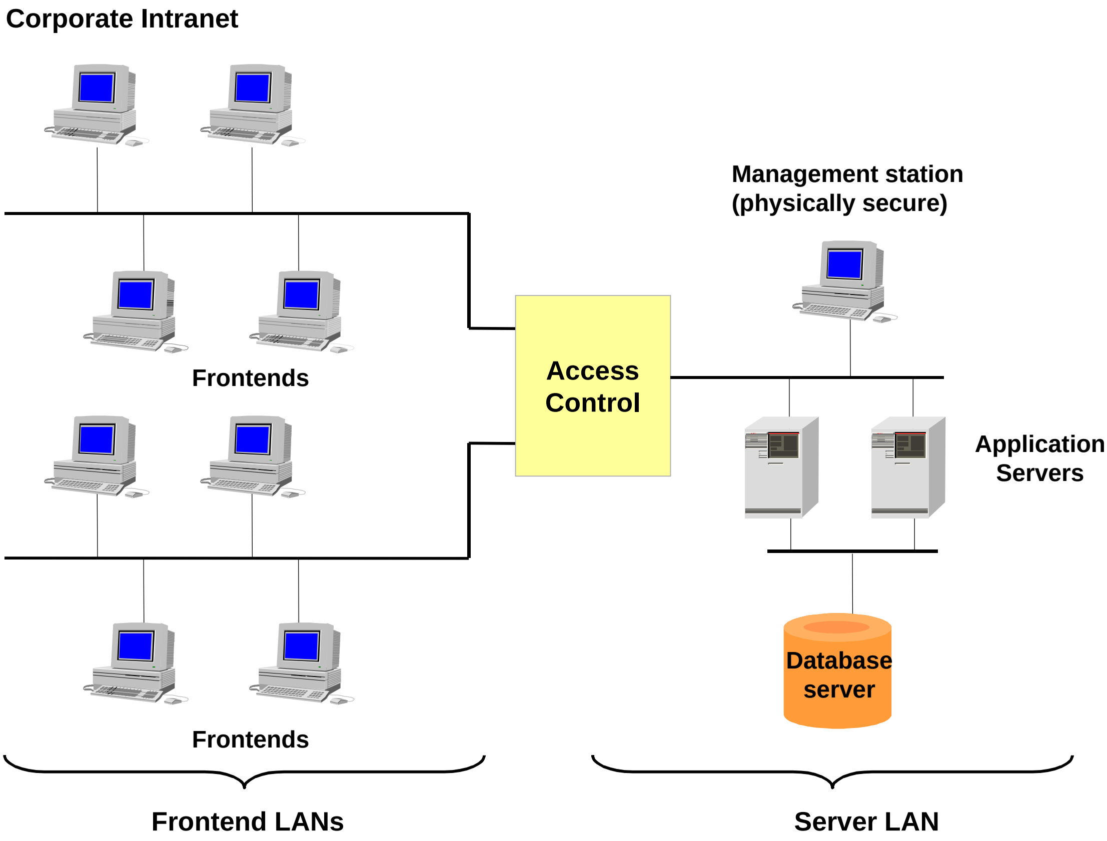
See the following topics:

1 Basic Network Topology for SAP Systems

SAP systems are implemented as client-server frameworks built in three levels: database server level, application server level and the presentation level (front ends). Depending on the size of your SAP system, your physical network architecture may or may not reflect this three-tier framework. For example, a small system may not have separate application and database server machines (the work processes run on the same machine as the database). The system may also only have a limited number of front ends in a single subnet connected to the server machine. However, in a large SAP system, several application servers usually communicate with the database server, as well as a large number of front ends. Therefore, the physical topology of your network can vary from simple to complex.

There are several possibilities to consider when organizing your network topology. The topology can vary from a single LAN segment to multiple IP subnets. We highly recommend you install your application server and central database server on separate machines and place them in a separate subnet as indicated in the graphic below:

Separating Frontend LANs from the Server LAN



By placing your SAP system servers in a separate subnet, you increase the access control to your server LAN, thereby increasing the security level of your system.

> We discourage placing SAP system servers into any existing subnet without first considering the appropriate security issues.

If you have several systems (or groups of systems) with varying security levels, then we recommend you create separate server LANs for each "group" of related systems. Determining these system "groups" and the security levels that they require, is a very individual process. We do have consultants available for assistance.

2 Network Services

The servers are the most vulnerable part of your network infrastructure and you should take special care to protect them from unauthorized access. However, there are a number of network services that do allow server access, and you should take appropriate precautions when using these services.

General Network Services

A typical Unix or Windows server machine runs many network services of which only a few are actually needed for running a SAP system. The names of these services are contained in the file `/etc/services`. This file maps the symbolic name of the service to a specific protocol and numeric port number. (Under Windows, the file is located at: `/winnt/system32/drivers/etc/services`.)

> Disable any of these network services on the server net that you do not need. Sometimes these services contain known errors that unauthorized users may be able to take advantage of to gain unauthorized access to your network (for example, `sendmail`). In addition, by disabling unused network services, you also decrease the vulnerability of your network to denial-of-service attacks. For an even higher level of security, we also recommend that you use static password files and disable any unnecessary access services on the application and database servers.

> You can list the active services and open ports on a UNIX or Windows NT server with the command `netstat –a`.

SAP Network Services

SAP systems also offer a variety of network services in their own infrastructures. As with general network services, we also recommend disabling any SAP services that you do not need with your installation. For a complete list of the ports used by SAP NetWeaver products and their default assignments, see the document *TCP/IP Ports Used by SAP Server Software* which is available on the SAP Service Marketplace at http://service.sap.com/network.

Additional Information

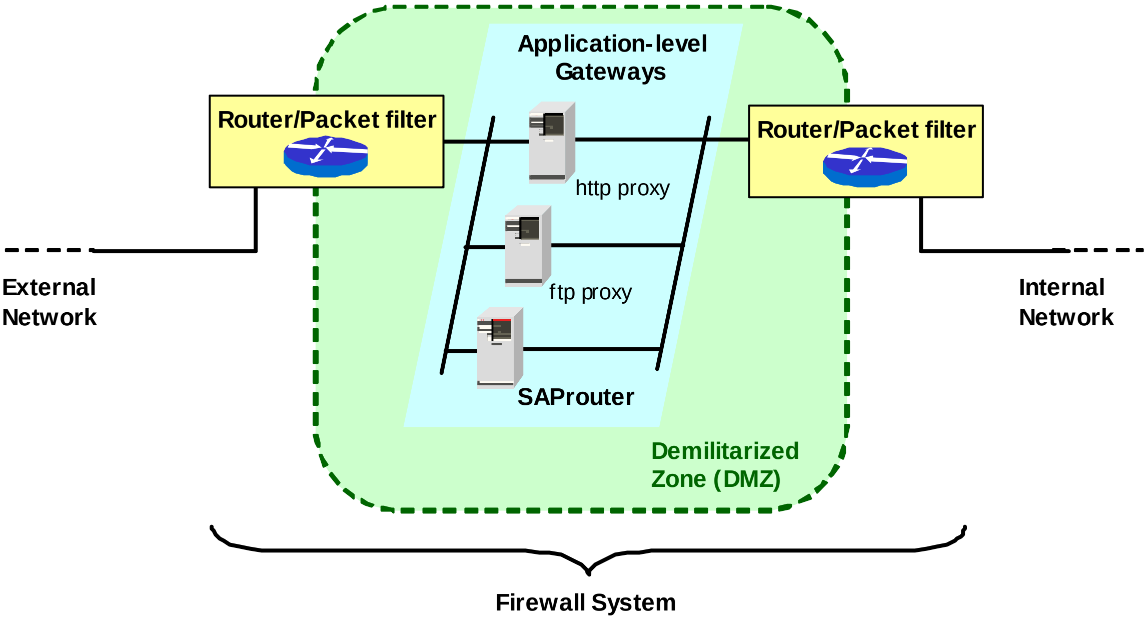
For a list of well-known port numbers, see the list provided by the Internet Assigned Numbers Authority (IANA) at http://www.iana.org/assignments/port-numbers.

3 Using Firewall Systems for Access Control

The firewall is a system of hardware and software components that define which connections are allowed to pass back and forth between communication partners. By using a firewall system, for example, between your intranet and the Internet, you can allow a defined set of services to pass through the different network zones while keeping other services out. For example, you can allow users in your company's intranet to use Internet services such as `mail` or `http`, but not other services such as `telnet`.

The graphic below shows an example firewall scenario. Note that the machines in the so-called "demilitarized zone" are not directly accessible from either the internal or the external networks. The routers and packet filters are configured to allow only connections for specified network services.

Firewall System



Firewall Types

There are two primary firewall types:

- Packet filters

  The functions used for packet filtering are typically available with routers. The router's primary function is to route network traffic based on the source or destination IP addresses, TCP ports, or protocols used. In this way, certain requests are routed to the server that can best handle the request. For example, mail requests are routed to the company's mail server; ftp (file transfer protocol) requests are routed to the company's ftp server.

  By using the router’s packet filtering functions, you can also restrict traffic based on this information, for example, to completely block requests using undesired protocols, for example telnet.

  However, the packet filter is not able to filter information sent at the application level.

- Application-level gateways

  Contrary to packet filters, application-level gateways or proxies work at the application level. They are capable of permitting or rejecting requests based on the content of the network traffic.

  Examples of access control functions that the application-level gateway can process:

  - Access control based on content: Does the request contain known exploits?
  - Access control based on user authentication: Is the user permitted to access the resource requested?
  - Access control based on source network zone: Is access to the resource from the source network allowed?
    For example, you can prohibit access to certain intranet resources from the Internet.
  - Access control based on source address: Is the sender address allowed access to the resource?

In addition, application-level gateways often provide auditing and logging functions so that the network traffic can be monitored or analyzed at a later time.

See also:

Application-Level Gateways Provided by SAP [Page 9]

3.1 Application-Level Gateways Provided by SAP

The SAProuter and the SAP Web dispatcher are examples of application-level gateways that you can use for filtering SAP network traffic.

Use the SAProuter for dialog and RFC connections. Use the SAP Web dispatcher for HTTP(S) connections.

SAProuter

Filtering Functions

You can use the SAProuter for routing and filtering traffic at the SAP NI layer. You can use it to:

- Filter requests based on the IP address or protocol. For example, you can reject any requests that do not use the SAP protocols.
- Require that a password is sent with the request.
- Require that secure authentication and data encryption occurs at the network layer using Secure Network Communications (SNC).

When using the SAProuter, you only have to open a single port on the firewall for the SAP protocols, which corresponds to the port on the machine running the SAProuter. All connections using the SAP protocols are then required to pass through this port (default=3299).

The SAProuter complements and does **not** replace the firewall. We recommend that you use the SAProuter and a firewall together. A SAProuter alone does not protect your SAP System network.

For an example of the network topology when using a SAProuter, see Example Network Topology Using a SAProuter [Page 10].

Configuration

To enforce access control, specify the IP addresses and address patterns that can access your SAP systems in the configuration file `saprouttab`.

When specifying the entries in the `saprouttab`:

- Use the S indicator in the `saprouttab` entries to specify that the entry applies to SAP protocols only.
- Only use the option P where necessary. This options specifies that the entry applies to non-SAP protocols as well.

If you use the SAP remote services (SAPNet–R/3-Frontend), you must use a SAProuter. See Example Network Topology When Using SAP Remote Services [Page 12].

For more information about the SAProuter, see SAProuter (BC-CST-NI) [SAP Library].

SAP Web Dispatcher

You can use the SAP Web dispatcher for load balancing and filtering HTTP(S) requests to the SAP Web Application Server. The rules to use for filtering the requests are contained in a file in the file system on the server where the SAP Web dispatcher runs. See SAP Web Dispatcher as a URL Filter [SAP Library].

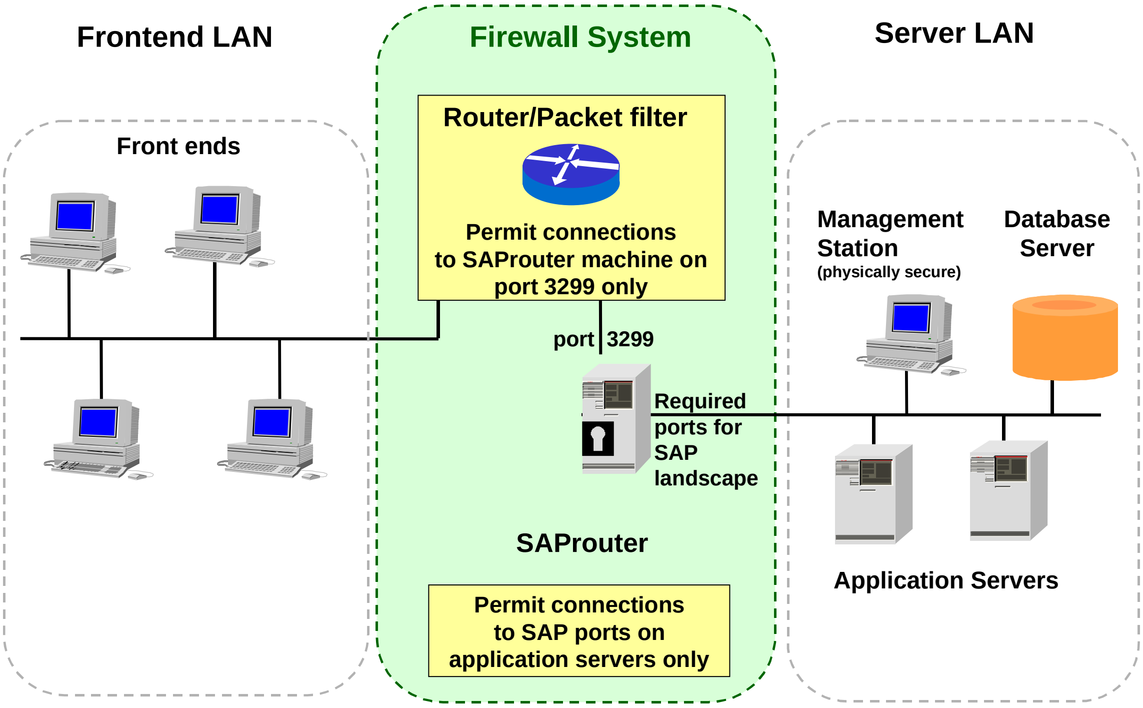
The SAP Web dispatcher also supports the use of the Secure Sockets Layer (SSL) protocol to secure the communications at the transport level.

For more information about the SAP Web dispatcher, see SAP Web Dispatcher [SAP Library].

Example Network Topology Using a SAProuter

The graphic below shows an example SAP system network topology that uses a router or packet filter in conjunction with an accordingly configured SAProuter to separate the SAP system server LAN from the front end LAN. We suggest using this or a similar setup for productive and other security-critical SAP systems.

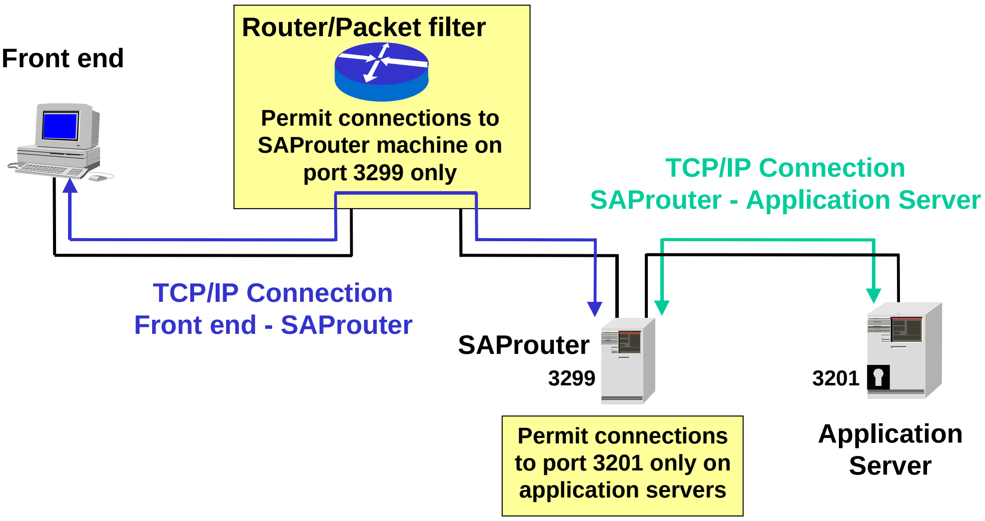
Recommended SAP System Network Topology


Frontend LAN
Firewall System
Server LAN
Front ends
Router/Packet filter
Permit connections to SAProuter machine on port 3299 only
port 3299
Required ports for SAP landscape
SAProuter
Permit connections to SAP ports on application servers only
Management Station (physically secure)
Database Server
Application Servers

The main security elements of this configuration are the router or packet filter and the machine running the SAProuter proxy. The router or packet filter is configured to allow only TCP connections from machines in the frontend LAN to the port 3299 (the default SAProuter port) on the SAProuter machine. The SAProuter is configured to explicitly allow or deny connections from a defined subset of client machines.

Using this setup, machines in the "open" frontend LAN cannot directly access the application or database servers. All front ends connect to a single port on the machine running the SAProuter software. The SAProuter machine opens a separate connection to one of the application servers. The graphic below illustrates this two-way connection.

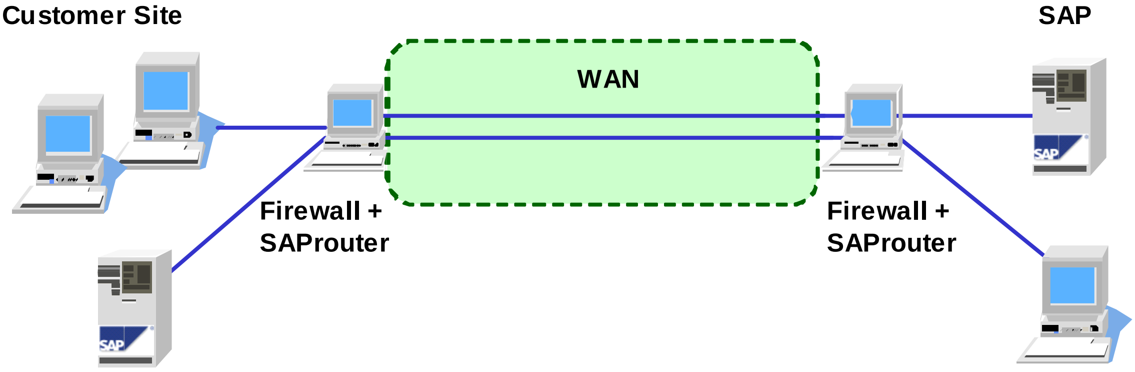
Two-Way Connection Using the SAProuter and a Router/Packet Filter


Front end
Router/Packet filter
Permit connections to SAProuter machine on port 3299 only
TCP/IP Connection SAProuter - Application Server
TCP/IP Connection Front end - SAProuter
SAProuter
3299
3201
Permit connections to port 3201 only on application servers
Application Server

Example Network Topology When Using SAP Remote Services

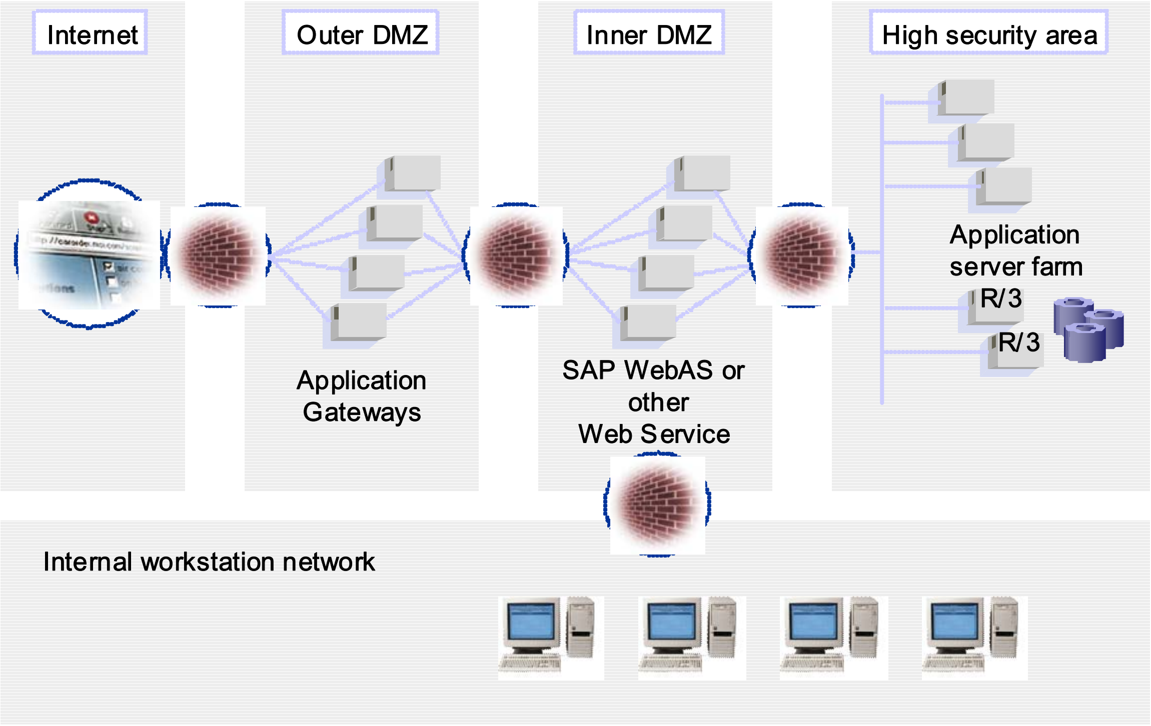
When using SAP remote services, you must use a SAProuter. Set up the network topology as shown in the graphic below.

Network Topology for SAP Remote Services



4 Using Multiple Network Zones

To ensure that the security protection provided by the protocols and functions mentioned (SSL, SNC, authentication and authorization) cannot be misused, additional security mechanisms are also necessary. Therefore, for additional access protection and optimal security, we recommend using security zones to establish a secure network infrastructure for your complete landscape.



The firewalls protect the network from undesired access from persons or resources outside of the designated area. The application gateway or proxy server in the DMZ makes sure that requests are not directly passed through to the desired resource, but are handled by the gateway or proxy server's own cache. Not only does this buffer zone reduce network load, but it also allows you to filter requests increasingly from the external to internal networks through the multiple firewalls. Application servers, database servers, and the user management systems have increased protection and are only accessible by authorized users or resources. In this way, you can provide for optimal protection.

The example above is an example of how a system landscape can be set up using network zones. Depending on the complexity of your own landscape, you may choose to use additional or fewer zones.

5 Transport Layer Security

SSL and SNC

Transport layer security for communication with or between SAP systems using either the Internet standard protocol Secure Sockets Layer (SSL) or the SAP interface for Secure Network Communications (SNC), depending on the underlying protocols used. See the table below.

Transport Layer Security

Protocol	Security Method Used	Comment
Internet protocols (For example, HTTP, P4, LDAP)	SSL	SSL is a quasi-standard protocol developed by Netscape. It is used with an application protocol, for example, HTTP.
SAP protocols: dialog and RFC	SNC	SNC is an SAP interface that you can use to secure connections between SAP system components. For an overview of the connections that support SNC, see SNC-Protected Communication Paths in SAP Systems [Page 16].

There are laws in various countries that regulate the use of cryptography. If you use SSL or SNC, you need to be aware of the impact these laws may have on your applications.

Protection Provided

Both SSL and SNC provide for the following protection:

- Authentication

  The communication partners can be authenticated. With SSL, you can set up the connections so that only the server component for the connection is authenticated or that both partners are authenticated. With SNC, both partners are always authenticated

- Data integrity

  The data being transferred between the client and the server is protected so that any manipulation of the data is detected.

- Data privacy

  The data being transferred between the client and the server is also encrypted, which provides for privacy protection. An eavesdropper cannot access the data.

External Security Products for SNC

SNC is a software layer in the SAP System architecture that provides an interface to an external security product. The interface used for the integration is the GSS-API V2 (Generic Security Services Application Programming Interface Version 2).

We do have a default security product available, the SAP Cryptographic Library. However, due to export regulations, we do not deliver this library with the SAP system. It is available for download for authorized customers on the SAP Service Marketplace at http://service.sap.com/download.

This library is also only available for use between server components. To use SNC with client components, for example, SAP GUI for Windows, you must purchase a security product that has been certified by the SAP Software Partner Program. For more information, see http://www.sap.com/softwarepartner (SNC interface).

Additional Information

Using SSL

For more information about using SSL with the SAP Web AS, see

- SAP Web AS, ABAP Engine: Using the Secure Sockets Layer Protocol [SAP Library]
- SAP Web AS, J2EE Engine: Configuring the Use of SSL on the SAP J2EE Engine [SAP Library]
- SAP Web dispatcher: Configuring the SAP Web Dispatcher to Support SSL [SAP Library]

Using SNC

For more information about using SNC, see:

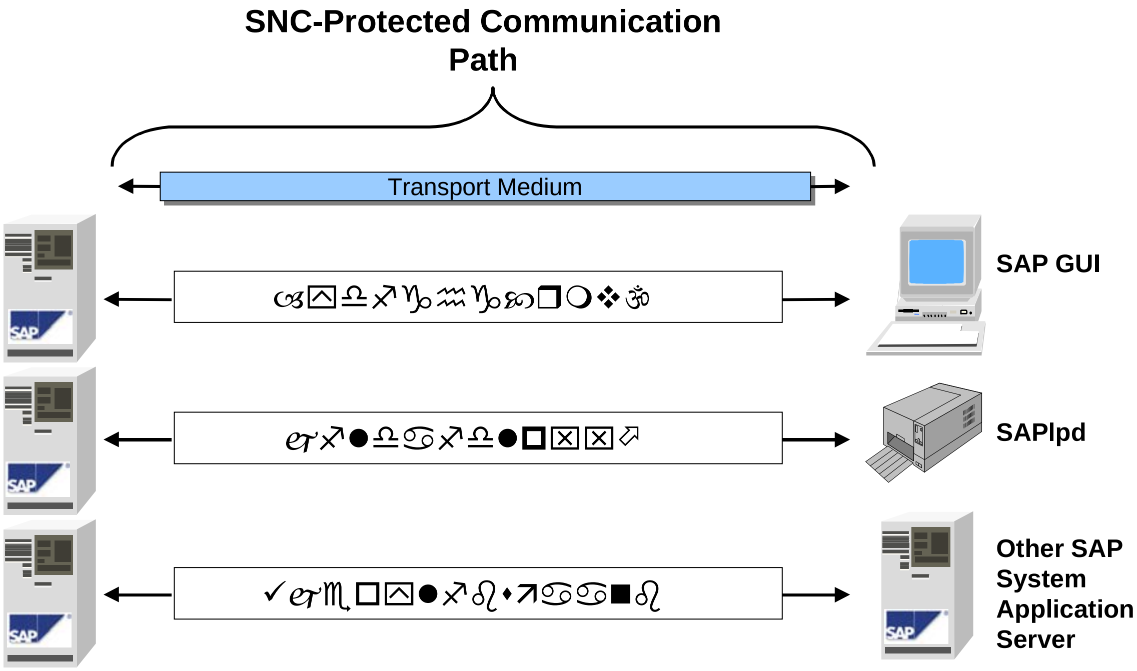
- Secure Network Communications (SNC) [Page 15]
- SNC-Protected Communication Paths in SAP Systems [Page 16]
- *SNC User's Guide* (available on the SAP Service Marketplace at http://service.sap.com/security)
- Using the SAP Cryptographic Library for SNC [SAP Library]
- SAP Web AS, J2EE Engine: Configuring SNC (SAP J2EE Engine --> ABAP Engine) [SAP Library]
- ITS: Configuring the AGate to Use the SAP Cryptographic Library for SNC [SAP Library]

5.1 Secure Network Communications (SNC)

SNC is a software layer in the SAP system architecture that provides an interface to an external security product. With SNC, you can strengthen the security of your SAP system by implementing additional security functions that SAP systems do not directly provide (for example, the use of smart cards for user authentication).

SNC provides security at the application level. This means that a secure connection between the components of the SAP system (for example, between the SAP GUI and the SAP application server) is guaranteed, regardless of the communication link or transport medium (see the graphic below). You therefore have a secure network connection between two SNC-enabled communication partners.

Application-Level SNC Protection


SNC-Protected Communication Path
Transport Medium
SAP GUI
SAPlpd
Other SAP System Application Server

For a list of the connections in SAP systems that support the use of SNC, see SNC-Protected Communication Paths in SAP Systems [Page 16].

5.2 SNC-Protected Communication Paths in SAP Systems

The following components support the use of SNC for connections.

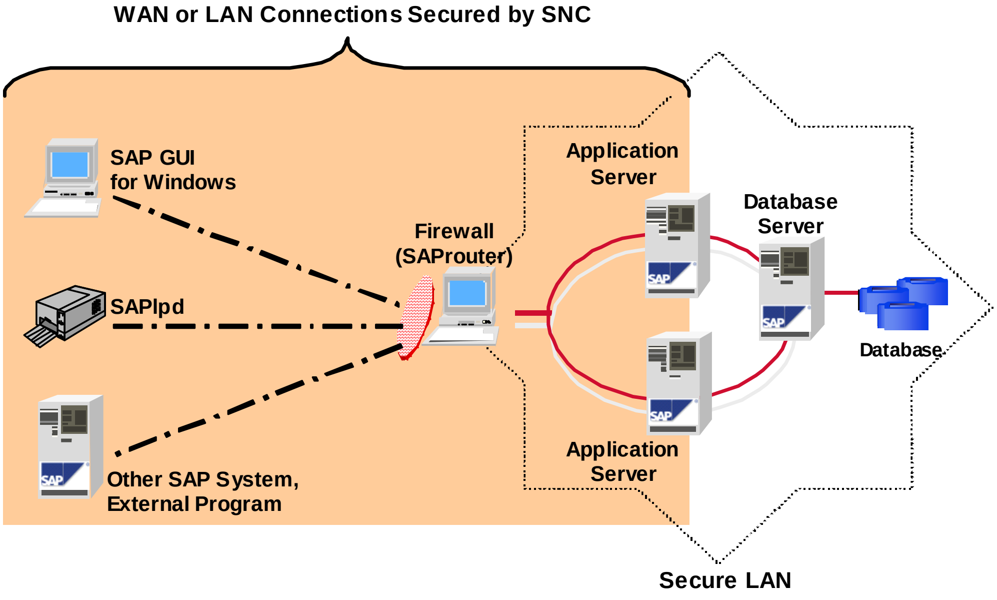
SNC protection only applies to connections that use SAP protocols (dialog, RFC or CPIC) protocols. For Internet protocols, use SSL for protection.

SNC-Protected Communication Paths

From	To	Comment
SAP GUI for Windows or SAP GUI for Java	SAP system application server	
SAP system application server	SAP lpd	
External RFC or CPIC program	SAP system application server	Example: SAP Java Connector
SAP system application server	External RFC or CPIC program	Example: SAP Java Connector
SAProuter	SAP system application server	
SAProuter	SAProuter	
Internet Transaction Server	SAP system application server	

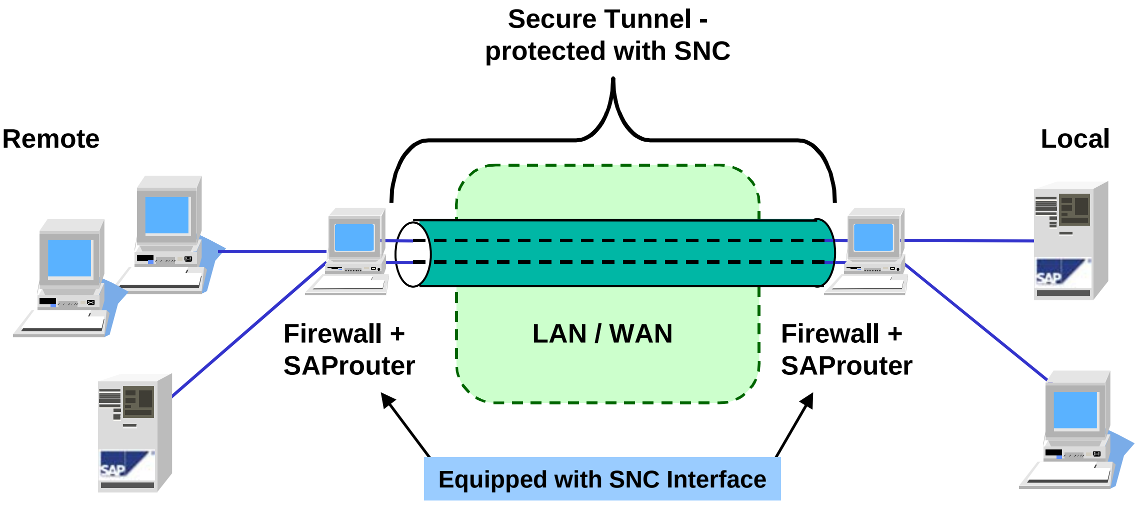
You cannot apply SNC protection to the communication path between your application servers and your database. Therefore, we recommend you keep your application and database servers in a secured LAN that is protected with a firewall and SAProuter (see the graphic below).

Network Area Protected with SNC



You can also use SNC between two SAProuters to build a secure tunnel between networks (see the graphic below).

SNC Protection between SAProuters



6 Additional Information on Network Security

Type / Number	Title / Link
SAP Library	Network and Transport Layer Security SAProuter (BC-CST-NI) SAP Web Dispatcher
SAP Note 66687	Use of network security products
SAP documentation	*Network Integration of SAP Servers* and *TCP/IP Ports Used By SAP Server Software* (see http://service.sap.com/network) *SNC User's Guide* (see http://service.sap.com/security)
SAP Internet: SAP Software Partner Program (SNC interface)	http://www.sap.com/softwarepartner
Internet: Internet Assigned Numbers Authority Reserved port numbers	http://www.iana.org/assignments/port-numbers