SAP NetWeaver 2004s SPS 4

Security Guide

Internet Transaction Server Security

Document Version 1.00 – October 24, 2005

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

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
	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

Internet Transaction Server Security

To link the SAP System applications to the Internet, we provide the middleware component Internet Transaction Server (ITS). The ITS allows for effective communication between the two systems, in spite of their technical differences.

In the topics that follow, we describe the system component architecture as well as the security measures and concepts necessary for providing security with SAP Internet applications. See:

1 Defining SAP Transactions as Internet Applications

SAP System transactions may be defined to run as any of the following Internet applications:

- Web transactions (IACs)
- Standard SAP transactions using the SAP GUI for HTML (or SAP GUI for JAVA)
- WebRFC or WebReporting

Transactions that are delivered with the SAP System are defined in one of the categories listed above. When developing your own transactions, develop them according to the needs of the transaction. For example, when defining Web transactions, you can change the screen layout to meet your own needs.

Defining Web Transactions (IACs)

SAP System transactions may be accessible as IACs (also known as Web transactions). In this case, the transaction finds all of the information it needs for the frontend presentation in its own service file and templates, to include the transaction code to start in the SAP System (defined with the parameter `~transaction` in the service file).

The transaction VW01 runs as an IAC that has its own service file, named `vw01.srvc`. In this example, the parameter `~transaction` in the file `vw01.srvc` contains the value `VW01`.

Defining GUI-Compatibility for Standard SAP Transactions

With the ITS Release 4.6B, standard SAP transactions are also Internet-enabled using the SAP GUI for HTML (ITS service `webgui`) or SAP GUI for JAVA (ITS service `jvgui`).

Using an ITS as of Release 4.6B, you can also access standard transactions in earlier releases using the SAP GUI for HTML or SAP GUI for JAVA.

Declaring Services that Use WebRFC

The ITS also supports RFC-based access to the SAP System using WebRFC or WebReporting. (WebReporting is based on WebRFC.)

Only those WebRFC or WebReporting modules can be accessed from the Internet that have been specifically written for the Internet scenario.

Additionally, as of Release 4.5, you must explicitly release all reports and function modules that are accessible over the Internet (use transaction SMW0).

To disable the use of WebRFC altogether, delete the file `SAPXGWFC.dll` on the AGate server.

For Release 3.1H, there is a patch that you should run to prevent the starting of reports that contain an empty authorization group (see SAP Note 92725).

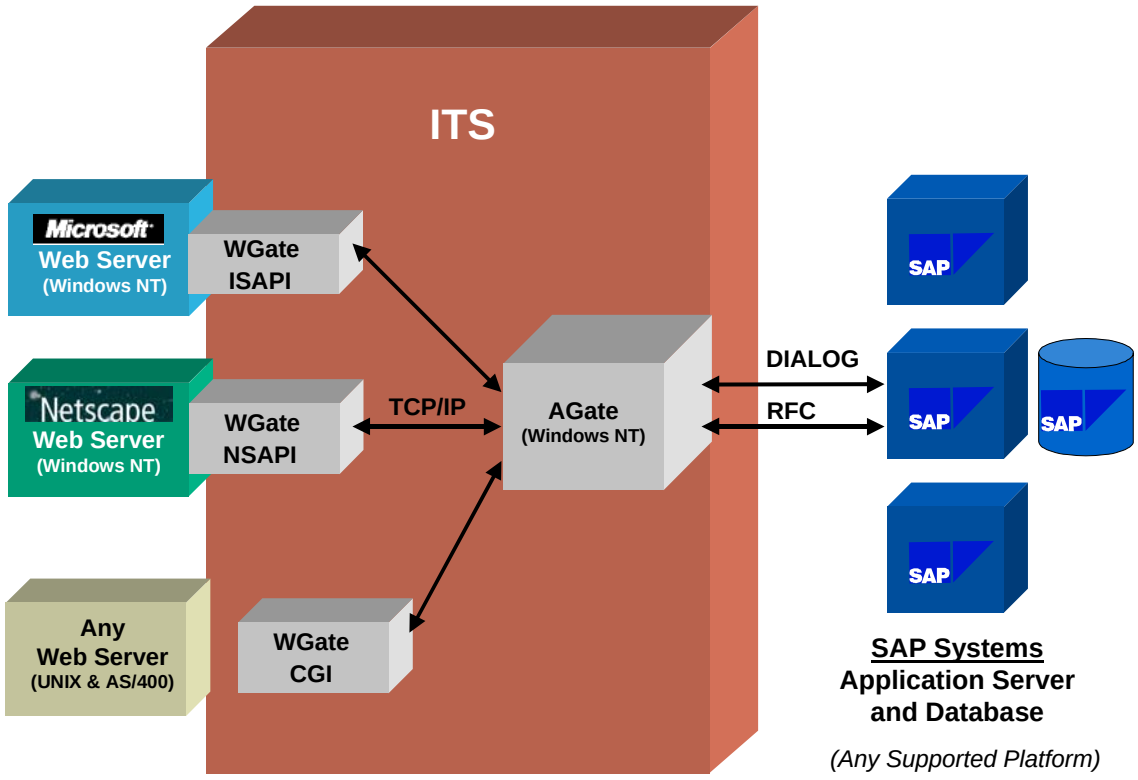
Additional Information

For more information, see the information on the SAP Service Marketplace at http://service.sap.com/sapgui.

2 The Architecture of the Internet Transaction Server (ITS)

The overall architecture of the ITS is shown in the graphic below:

The Internet Transaction Server Architecture



Components and Data Flow

WGate

The WGate component connects the ITS to the Web server. The WGate is always located on the same computer as the Web server. The following standard Web server interfaces are supported:

- **Microsoft's Information Server API (ISAPI)** on Windows NT.

  The Microsoft Information Server API loads the WGate into the Web server process as a dynamic link library (DLL).

- **Netscape Server API (NSAPI)** on Windows NT.

  The Netscape Server API also loads the WGate into the Web server process as a DLL.

- **Common Gateway Interface (CGI)** on UNIX and AS/400 (controlled availability as of Release 4.5A).

  On the UNIX and AS/400 platforms, the Common Gateway Interface starts the WGate as an external executable program.

AGate

The AGate program is implemented as a Windows NT service. Although the AGate can be located on the same machine as the WGate, we recommend that you keep the two components on two separate machines.

The AGate is responsible for managing the communication to and from the SAP System, including:

- Establishing the connection to the SAP System using DIAG (SAP GUI) or RFC protocols
- Generating the HTML documents for the SAP applications
- Managing user logon data
- Managing session context and time-outs
- Code page conversions and national language support

Data Flow

The WGate establishes the connection and forwards requests to the AGate. The components communicate using the SAP Network Interface (NI), which in turn uses a TCP connection.

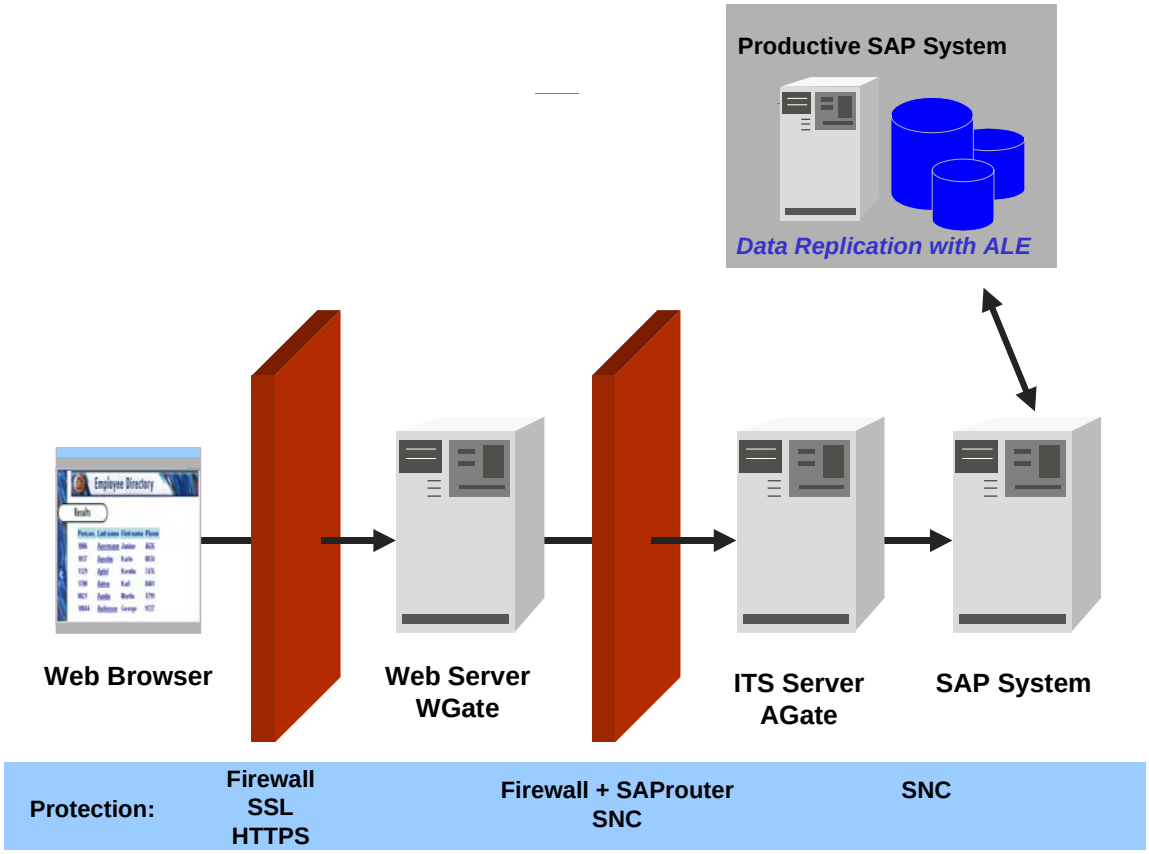
The AGate receives Web requests from the WGate and communicates with the SAP System application server (using DIAG or RFC). It processes the HTTP request, sends the appropriate data (including logon information) to the SAP System, retrieves information from the SAP System, processes it, and sends the response back to the WGate.

3 A Secure Network Infrastructure for the ITS

The ITS architecture has many built-in security features, such as the possibility to run the WGate and AGate on separate hosts. We strongly recommend that you set up a network infrastructure that makes use of these features to control access from the Internet to internal networks. We also recommend you use other security components, such as firewalls, packet filters and SAProuters to separate the individual parts of the network from another. It is important to use a multi-level security concept so that if an undesired event does occur in one area of your system, the consequences are limited to that part of the system and do not affect your system on the whole.

The graphic below shows some of the components that you can use to build a secure network architecture when using ITS.

Providing ITS Security



You may decide to implement some or all of these components depending on your security policy. You can find details about the components and a concrete example network setup in the topics that follow.

To protect critical data, you can use a separate system (for example, replicated using Application Link Enabling) for your "Internet" system, instead of your productive system.

4 Protecting the Server and Network Components

Our recommended network topology consists of three separate network segments that are connected by two firewall systems. Note that we use the term "firewall" in a very broad sense here. Some of the described firewall systems may only consist of a usual network router with packet filtering capabilities. Refer to Network Infrastructure [SAP Library] for details on our networking topology and an introduction to TCP ports. In the following topics, we explain only the specific aspects pertaining to Internet applications with SAP Systems.

See:

4.1 Protecting the Web Server

The WGate component of the ITS runs on the Web server.

You should protect your Web server against any kind of network packets that are not needed for the HTTP communication. Configure the router to pass packets to the corresponding TCP port only.

Usually a Web server requires one TCP service. Port number 80 is reserved for HTTP and used by default by all servers and browsers. Web servers that support HTTPS (HTTP plus the Secure Sockets Layer protocol), use port number 443 by default.

You should configure the Web server operating system as closed and restrictive as possible. You should disable all unnecessary network services. Also, keep your operating system up-to-date regarding security-related patches released by your operating system vendor. For more information, see Operating System Protection [SAP Library].

4.2 Protecting the AGate Server

We strongly recommend that you take additional measures to isolate the Web server from your internal corporate network and place the AGate in your internal network. Protect your internal network (that contains the AGate component) with a firewall and SAProuter. The WGate and AGate only need one TCP/IP connection between them for their communication purposes. Configure the firewall and SAProuter accordingly and monitor the connection carefully.

If you save user information in the service files on the AGate (see Authenticating Users [Page 16]), then take extra care to protect the AGate computer from unauthorized access. In particular, protect the service file and template directories. For more information, see the *SAP@Web Installation Guide* in the section titled *Setting Security for a virtual ITS*.

It is possible to install multiple "virtual" AGates on a single computer. Each virtual AGate then has a unique name and a separate Windows NT service. The AGates share the executable files. Each WGate is then configured to connect to exactly one virtual AGate on the AGate host.

4.3 Protecting the SAP System Application Servers

The SAP System servers (as well as the AGate) are located in your internal network that should be separated from the external network (Internet) with a firewall system as previously described.

If you want to completely isolate your SAP System servers, you can also use the network measures as described in Network Infrastructure [SAP Library] to separate your AGate(s) from your SAP System server(s). The AGate communicates with the SAP System in the same way as with SAP GUI and you can therefore use the same mechanisms to separate it from your SAP System server LAN as you use with your SAP GUI frontend clients.

4.4 TCP Ports Used by the ITS

The WGate and AGate communicate using one TCP socket connection. The WGate initiates the connection to the TCP port of the AGate service. The connection is opened for each new incoming request and closed once the connection is finished.

The AGate service's port is `sapavw00_<INST>`, where `<INST>` is the name of the virtual ITS instance. The file `\WINNT\System32\Drivers\etc\services` (`/etc/services` on UNIX) defines which port number corresponds to this port name; normally 3900 for the first virtual AGate installed. Multiple virtual AGates use separate ports.

When installing the ITS, ten TCP ports are automatically added to the file `etc\services`, for example:

```
sapavw00_<INST>     tcp/3900
sapavw01_<INST>     tcp/3901
...
sapavw08_<INST>     tcp/3908
sapavwmm_<INST>     tcp/3909
```

ITS versions prior to 2.0 allocate 100 ports in a similar fashion. However, because these versions do not support virtual ITS instances, the `<INST>` string is empty.

For normal ITS installations only the port `sapavw00_<INST>` is required. The other ITS ports are not used and may be deleted from `etc\services`.

During installation, the ITS setup program tries to find a sequence of 10 unused ports on the installation machine starting with port number 3900. As a result, the port number associated with the port name `sapavw00_<INST>` may vary for different installations. You need to check your installation to find out which port number is actually used. Each virtual ITS instance uses a separate port.

Make sure that the port numbers associated with port name `sapavw00_<INST>` are identical on the WGate and the AGate host. The ITS does not automatically guarantee consistency.

4.5 Using the SAProuter

We recommend using a SAProuter in your firewall system. Configure it to relay only one specific WGate ←→ AGate connection and deny all other connection attempts.

To configure the WGate to connect to the AGate via a SAProuter, enter the corresponding route string in the Windows NT registry on the WGate host in the following location:

`HKEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<INST>\Connects\Host`

where `<INST>` is the name of the virtual ITS installation.

Enter a route string of the type:

`/H/<SAProuterhost>/S/<routerservice>/H/<host>`

Do not specify the AGate port in the route string.

In addition, the SAProuter host must be able to map the port that is entered in the following key to a port number:

`HKEY_LOCAL_MACHINE\Software\SAP\ITS\2.0\<INST>\Connects\PortAGate`

The default entry is `sapavw00_<INST>`. If this port is not mapped in the SAProuter's `etc\services` file, enter the port number directly in this key.

For a detailed description on using and administering the SAProuter, see SAProuter (BC-CST-NI) [SAP Library].

4.6 Using Other Firewall Components

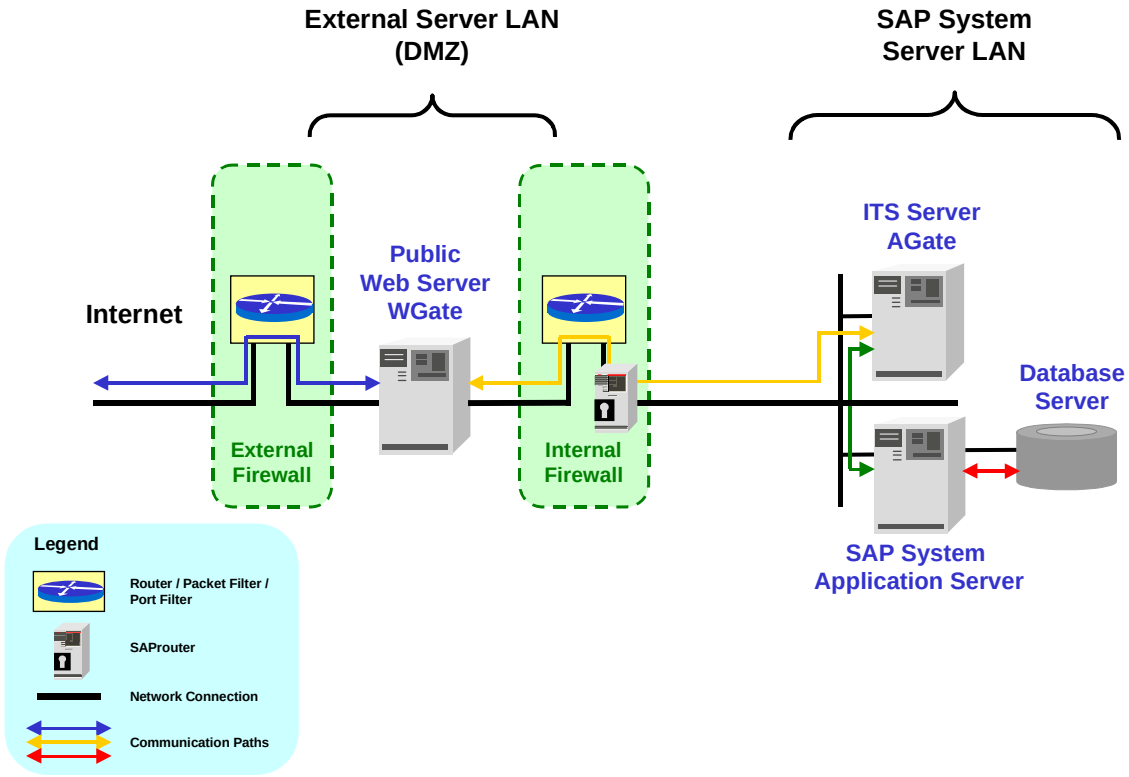
You can use other firewall products to relay the TCP connection from the WGate to the AGate.

For more information, see the documentation for your firewall product.

5 An Example Network Setup

The graphic below shows an example network security infrastructure suitable for Internet access to SAP Systems using the SAP Internet Transaction Server:

An Example ITS Network Topology



The "security" of the network zones increases from left to right. The external firewall allows direct access from the Internet to the Web server's TCP ports only in the demilitarized zone (DMZ). The internal firewall is then configured to deny any direct access from the DMZ to any host in the corporate LAN except for the SAProuter's TCP port on the SAProuter host. Therefore, the connection from the WGate to the AGate can only be transmitted via the SAProuter. In the example, the AGate exists in the SAP System server LAN, which is also protected from the client LAN with a firewall and SAProuter.

If desired, as mentioned in the previous section, you can also place a router or packet filter between the AGate and the SAP System application server (see also SAP Note 104576).

For an example network infrastructure that also includes the client LAN, see An Example Network Setup (with Client LAN) [Page 14].

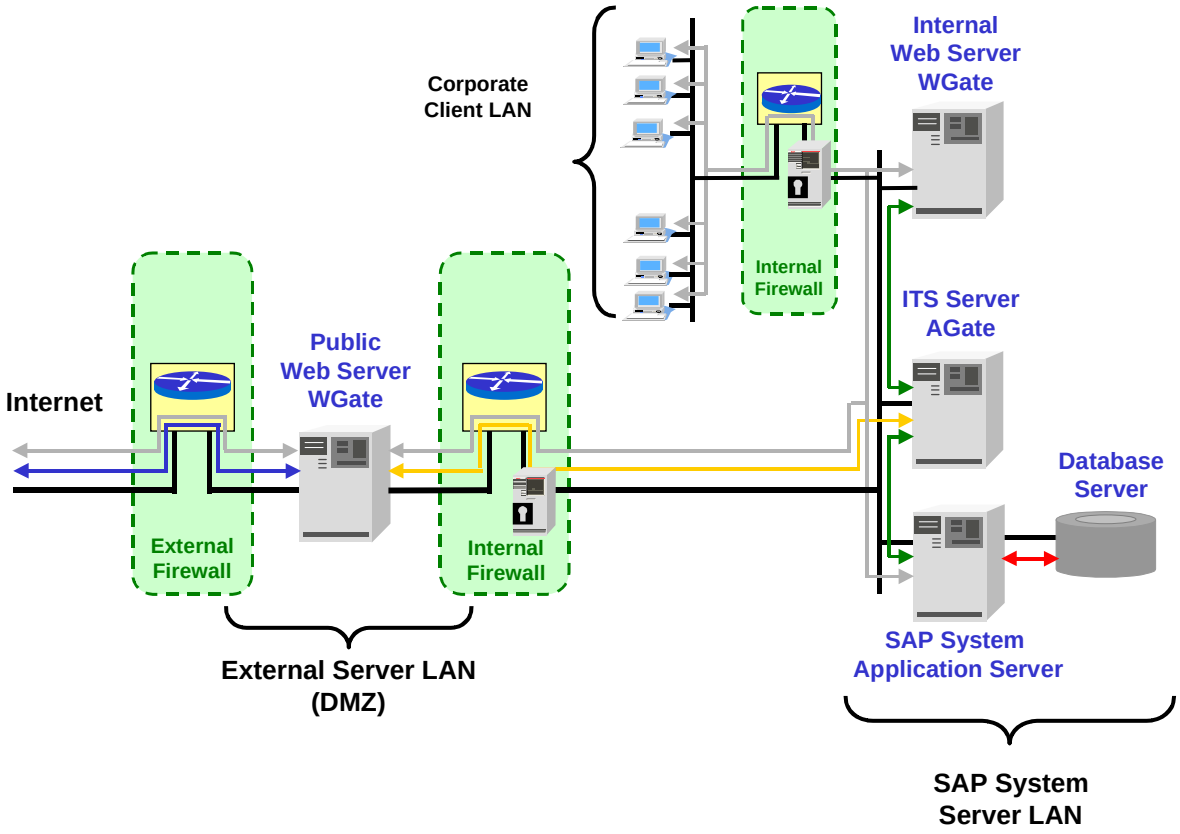
For more information about the configuration of the routers and SAProuters, see Network Infrastructure [SAP Library].

In the above example, we have chosen to show a setup using standard network and computer components. Many vendors offer specialized firewall products for these tasks. You may use such products; however, we do not describe them in more detail here in this guide.

5.1 An Example Network Setup (with Client LAN)

The following graphic shows how the client LAN also fits into the network infrastructure. In this example, the clients are able to communicate with the SAP System application server as well as the Internet (via the SAProuter and firewalls used for the DMZ). For intranet Web services, the clients communicate with the internal Web server and WGate, which then sets up the communication to the AGate and the SAP System application server.

Example Network Setup Including the Client LAN



6 Using Additional Security Mechanisms / Providing Privacy

You can use our additional security services to increase the security of the following connections:

- Between the Web browser and Web server
- Between the WGate and AGate
- Between the AGate and SAP System

Between Web Browser and Web Server

All data (including passwords) is usually transmitted through the Internet in plain text. To maintain confidentiality for this data, you can apply encryption to the connection between the Web server and Web browser. We especially recommend using encryption when you transmit passwords, orders, company-specific information or any other data that you consider sensitive.

P-supported Web servers and all modern browsers support the encryption of the HTTP data stream by means of the Secure Sockets Layer protocol (SSL), also known as HTTPS. HTTPS data streams are completely transparent to the ITS. For more details regarding encryption techniques, see the documentation supplied by the Web server manufacturer.

In order to use SSL encryption, the Web server must obtain an X.509 certificate that has been issued by a Certification Authority (CA). We refer to this certificate in this section as the **server certificate**. The server certificate is used to authenticate the server. If the Web browser receives a server certificate issued by a trusted CA, then the browser can verify that it is connected to the intended server.

If you want to offer a service for all Internet users, this server certificate should have been issued by an official CA that is trusted by most browsers used in the Internet. For internal users, you can set up a corporate CA and configure the browsers to trust this CA.

The Web server relies on **client certificates** to authenticate the user. To restrict access to SAP Systems, configure the Web server to accept only connection requests that present valid client certificates. The client certificates are again issued by a CA.

Between WGate and AGate

- ITS 1.0 and ITS 1.1

  Data sent between the WGate and the AGate is encrypted using a static key. This key is easily accessible; therefore, the protection that this encryption provides is minimal.

- As of ITS 2.0

  For better protection, as of ITS Release 2.0, you can use SNC (Secure Network Communications) to protect the link between the WGate and AGate. SNC uses an external security product to apply encryption to communication links between components of a SAP System. For more information, see [SAP Library]e section titled [SAP Library]r to the documentation provided with the security product itself for instructions on the necessary configuration.

Between AGate and SAP System

Prior to Release 4.5, we do not offer any security services for the connection between the AGate and the SAP System application server. However, as of Release 4.5, you can also use SNC to protect this communication path.

7 Authenticating Users

There are three different scenarios for authenticating users in SAP System Internet applications. See:

7.1 Authenticating Internet Users (Service Users)

In the **Internet** scenario, you do not necessarily know which users want to access the application data within SAP Systems. In addition, for the large number of Internet users, you normally cannot set up a separate account for each user. Therefore, if you want to make certain Web transactions available to anonymous Internet users:

- Define these services as Web transactions.
- Set up the corresponding service users with pre-defined passwords in the SAP System.
- Assign these service users only those authorizations they need to access the application (for example, a product catalog).

The user ID and password must be saved in the application's ITS service file. The password does not appear as clear text in the service file, but is encrypted using a static key. However, if you have service users with authorizations that are worth protecting, you should still take special care to protect the AGate from unauthorized access.

The ITS does not store any security-relevant information on the WGate.

If additional authentication is necessary (for example, when the user places an order), the application itself must perform the additional authentication.

7.2 Authenticating Named Users With User ID and Password

For applications that are to be accessed by named users (users with an account in the SAP System), do not save the user ID and password in the application's ITS service file. In this case, user authentication takes place entirely within the SAP System.

For example, the `webgui` service that allows access to standard SAP transactions should require the user's ID and password.

Do not store a user ID and password in the `webgui` service file!

As an alternative to using user ID and password authentication, as of Release 4.5B, named users can also log on using X.509 client certificates [Page 17].

7.3 Authenticating Named Users Using X.509 Client Certificates

Instead of using a user ID and password to authenticate themselves on the SAP System, users can present an X.509 client certificate. In this case, user authentication takes place using the SSL protocol and no transfer of passwords is necessary. User authorizations apply according to the authorization concept in the SAP System.

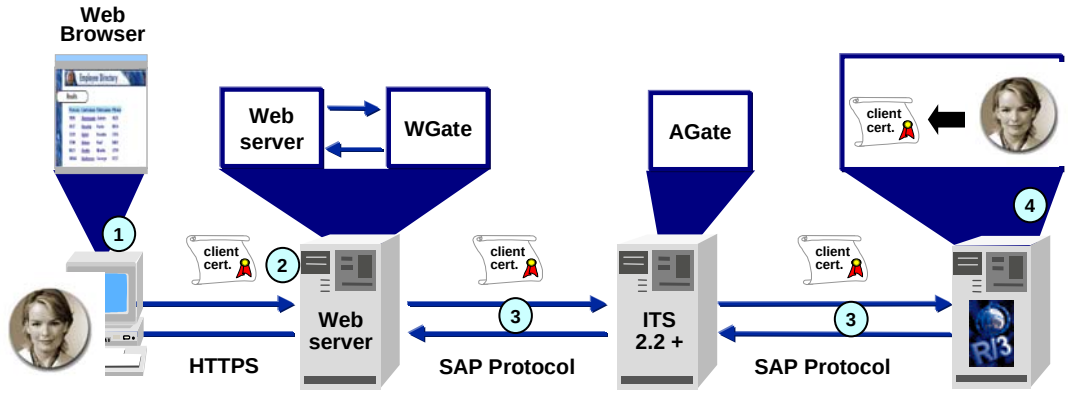
Prerequisites

- The SAP System needs to be Release 4.5B or higher.
- Your users need to possess valid X.509 client certificates that have been signed by a trusted Certification Authority (CA).
- You need to activate SSL for mutual authentication on the Web server.
- You need to use the ITS version 2.2 or higher.
- You need to use Secure Network Communications to guarantee secure communications between the WGate and the SAP System.
- You need to configure the SAP System and the ITS for using client certificates. (For more information, see the document *X.509 Certificate Logon via the ITS* (see http://service.sap.com/security).

Authentication Process

When a user logs on using a client certificate, the following occurs (see the graphic below):

Logon via the ITS Using Client Certificates



1. The user accesses an SAP Internet application.
2. The user's Web browser passes the client certificate to the Web server where the user is authenticated using the SSL protocol.
3. If the user's authentication on the Web server was successful, the ITS WGate passes the user's certificate to the SAP System via the AGate.

4. If the system can uniquely identify the owner of the client certificate as a user in the SAP System, then it logs the user on under the corresponding SAP System user ID and continues processing the Web transaction.
    - If the logon is a dialog connection, and certain information cannot be resolved (for example, if the SAP System client is not available, or if the certificate belongs to more than one user in the SAP System), then the user is prompted for the missing information.
    - If the logon occurs using RFC, and the client or user cannot be determined, then the connection terminates with an error.

7.3.1 Security Measures When Using Client Certificates

When using X.509 client certificates and SSL for user authentication, you should note the following:

- Choose a trusted CA.

  Your users need to possess valid certificates signed by a trusted CA. You can either establish your own CA and distribute certificates to your users yourself, or you can rely on a Trust Center service. The CA you choose to use must be designated as a trusted CA on the Web server.

- When using SSL with the ITS, then use SNC for the WGate / AGate / SAP system connections.

  Because user authentication takes place on the Web server and not in the SAP System, you need to use SNC to guarantee data privacy and integrity for the communication path between the WGate and the SAP System. For more information, see Network Infrastructure in the topic Secure Network Communications (SNC) [SAP Library].

- Inform your users about how to protect their private key.

  In this scenario, user authentication takes place using the SSL protocol, which uses public-key technology. Each user needs to possess a public-key pair. The public-key is contained in the X.509 client certificate and can be made public. However, the user's private key needs to be kept safe. The possibilities available for securing the private key depend on the Web browser you use. (For example, you may be able to protect it with a password or you may be able to use smart cards.) If the private key is stored on the front end client, your users should use screen savers protected with a password.

  If users share front ends, then note the following:
  - As long as the operating system separates and protects user data at the operating system level (for example, Windows NT), then the private key stored on the front end is protected by the operating system.
  - However, when using an operating system that does not separate user data (for example, Windows 95), then you should not store the private key on the front end.

  For more information on public-key technology, see Public-Key Technology [SAP Library].

8 Protecting Session Integrity

To maintain the integrity of the multi-step transactions when using SAP Internet applications, the ITS issues a unique session identification number when the user makes his or her first request. This session ID is sent to the browser with the first HTML page. It must be passed back to the ITS with every successive request. The session ID protects the session from being taken over by another user. (When using HTTPS, a session cannot be taken over by another user.)

ITS 1.0 and 1.1 use HTTP cookies to store the session ID. As of ITS version 1.11, you can disable cookies and then the session ID is stored directly inside the HTML pages.

As an additional security feature, the ITS stores the client IP address along with the session ID. A possible eavesdropper, who listens on the network connection and thus acquires the current session ID, cannot easily issue a fake reply. (His or her IP address does not match that of the original user.)

It is possible to configure the number of significant bytes used for the network address comparison. On the AGate, the following registry key specifies a mask of the significant network address bits:

```
HKEY_LOCAL_MACHINE\SOFTWARE\SAP\ITS\2.0\<INST>\Connects\IPChecking
```

The default value is 255.255.255.255, which specifies that the entire address should be compared. For an **Intranet** solution, you should enable this value. For **Internet** applications, you can adjust this value, for example, **`255.255.255.0`**. In this case, only the leading figures of a network address are compared. This allows clients who use Web proxy servers with load balancing to access the ITS.

The value you specify depends on your own network topology.

9 Setting Security Levels

You should set the access permissions for ITS specific files on the WGate and AGate servers according to your security needs. For example, you probably want to set a high level of security (Level 3) for your productive system, and level 2 for your development system (see below).

ITS supports three levels of security (by default):

1. **Full Access for everyone**

   At this level, everyone can access all files.

2. **ITS Administrator and ITS Users**

   At this level, a single administrator account has access to all ITS-related files and members of a given ITS users group have restricted access to certain files. You can use this level, for example, for a development scenario. You can allow a group of users to make changes in certain files (for example, HTML templates and service files). Only the ITS administrator can access the rest of the files. Other users cannot access any files.

3. **ITS Administrator**

   At this level, only the ITS administrator has access to ITS-related files. Apply this level to your productive site.

   Users who access the ITS from the Internet have **no** access to ITS-specific files located on the AGate server.

You set the security level during the installation process; however, you can change the level at any time with the command-line utility `itsvprotect`.

10 Security-Relevant Settings for IACs

IACs are screen-based applications and like these, are subject to the security concept. No authorization checks take place within ITS. Authorization checks are only carried out in SAP Web AS in the backend. Due to this, it is important to restrict authorizations of the SAP Web AS user with which the IAC is executed to the precise duties or work to be carried out. In principle, requests (URLs) to the ITS could always be intentionally manipulated.

In addition, it is not permitted to set the ITS parameter `~generateDynpro` to 1 with IACs which are executed over the Internet. Using the parameter `~generateDynpro`, the system controls whether a screen should be automatically generated by ITS using SAPGUI for screens for HTML without an HTML template. If this parameter is set to 0, then ITS ends a session as soon as a screen for which no HTML template exits is sent from the SAP Web AS server. This can prevent an intruder from activating OK codes through targeted manipulation of the URL, which leads to a screen being displayed which the developer did not intend. All in all however, this parameter only offers the additional security in that no unrequested screens are displayed in the Web browser that contain information that could be used during further attacks.

11 SAP Web AS with Integrated ITS

As of SAP NetWeaver 04, the ITS is now integrated into the SAP NetWeaver component SAP Web Application Server as an Internet Communication Framework (ICF) service, which can, like other services, be accessed through the Internet Communication Manager (ICM). For more information, see Internet Communication Framework [SAP Library] and Internet Communication Manager [SAP Library].

The security considerations are the same as for any other SAP Web AS service.

With the integrated ITS in the SAP Web Application Server, the Web browser can now communicate directly with the SAP System. Furthermore, all ITS-related sources, such as service files, HTML templates or MIME files, are now stored in the system's database, similar to ABAP sources.

The following changes are made by default so that the existing SAP Web AS infrastructure can be reused Web AS:

- The integrated ITS uses the common HTTP mechanism as in SAP Web AS, no additional Web server is required as, in the case of the standalone ITS.
- HTML templates and services files are stored in the SAP database, not in the file system.
- You can reuse ABAP software logistics for template and service distribution.
- The ITS registry is replaced by SAP profile parameters.
- The Work process roll area is used to handle ITS session information
- The integrated ITS is completely hidden behind SAP Web AS infrastructure

The security considerations are same as for to any other ICF service (for example, use transaction SICF). For more information see Security Aspects for Connectivity and Interoperability [SAP Library] in the *SAP NetWeaver Security Guide*.

In the SAP Web AS environment, it is recommended to place an application gateway or SAP Web Dispatcher in the DMZ. This setup provides the same level of architectural security as the standalone ITS. Securing the integrated ITS amounts to securing SAP Web AS.

For more detail overview, refer to Using Multiple Network Zones [SAP Library] and the security mechanisms used for the protocols listed in Network Security for SAP Web AS ABAP [SAP Library].

See also:

- Security Aspects for Connectivity and Interoperability [SAP Library]
- Network and Transport Layer Security [SAP Library]
- Using the Secure Sockets Layer Protocol with the SAP Web AS ABAP [SAP Library]

12 Additional Information on SAP Internet Applications and the ITS

Type / Number	Title
SAP Library	ITS Administration Guide [SAP Library] SAProuter (BC-CST-NI) [SAP Library] Public-Key Technology [SAP Library]
SAP Note 60058	Security for R/3 Release 3.1 on the Internet
SAP Note 92725	WebReporting and Authorisation group
SAP Note 104576	Package filter (firewall) between ITS and R/3
Installation Guide (see http://service.sap.com/instguides)	*SAP@Web Installation Guide*
SAP Service Marketplace	Presentation Clients http://service.sap.com/sapgui