Options and Strategies to Secure Internet-Facing Portals

Nicholas Holshouser
SAP Labs
What We’ll Cover ...

Introduction
Internet Security Concepts and Scenarios
Security Architecture
Implementing the Right Security
Configuring the SAP Web Application Server
Configuring the Secure Client Access
Troubleshooting Security Configuration
Wrap-up
Introduction

Internet Security Concepts and Scenarios
Security Architecture
Implementing the Right Security
Configuring the SAP Web Application Server
Configuring the Secure Client Access
Troubleshooting Security Configuration
Wrap-up
Enterprise Security Requirements

Enterprise applications need protection for proprietary and confidential information and systems

These requirements are driven not only by the desire to protect against unwanted access, but also by regulatory constraints regarding personal privacy (Sarbanes-Oxley)
Data and Application Security

Data security is required to protect proprietary or personal information from unauthorized access. This includes:

- Restricting application users from accessing data they are not authorized to see
- It also includes encryption of data to prevent unauthorized access to the data by users outside the application

Application security is required to ensure that:

- Only authorized users are allowed to access the system
- Data security is maintained inside the application
Today we are concerned with end-to-end security concepts focused on data security, specifically with ways to ensure that application data is transmitted securely (encrypted) between the system and its users.

We are also concerned with application security, specifically with ways to ensure that the application does not expose itself to unauthorized access.

- Applications should be configured in such a way that they do not expose any sensitive information about themselves to unauthorized parties who might use that information to mount an attack.
What We’ll Cover ...

Internet Security Concepts and Scenarios

Security Architecture
Implementing the Right Security
Configuring the SAP Web Application Server
Configuring the Secure Client Access
Troubleshooting Security Configuration
Wrap-up
Safeguards vs. Threats

Masquerading  
Eavesdropping  
Tampering  
Denial of Service

Masquerading  
Eavesdropping  
Tampering  
Denial of Service

Social Engineering

TRAINING

Application-Level Vulnerabilities

Patches App.- Gateway

Application

Network

Client

Encryption

Eavesdropping Tampering

Penetration

Firewall

Application

OS

OS-Cracking

OS-Hardening

Virus Detection

Authentication

Patches App.- Gateway

Server

Planting

Alice

Social Engineering

TRAINING

Application-Level Vulnerabilities

Patches App.- Gateway

Application

Network

Client

ENCRYPTION

Eavesdropping Tampering

Penetration

Firewall

Application

OS

OS-Cracking

OS-Hardening

Virus Detection

Authentication

Patches App.- Gateway

Server

Planting

Alice
Common Use Cases

Supplier Portal/Customer Portal
- It is very common that mySAP Business Suite components such as mySAP ERP or mySAP Customer Relationship Management (mySAP CRM) are used in Internet-facing scenarios to facilitate direct access to enterprise data by suppliers, customers, or partners.

Business Process Integration
- The continued evolution of process integration between companies and business units further moves the requirement for access to back-end applications from direct person-to-application access to more complex interactions that often invoke transactional business processes between these entities.
- This area is outside the scope of today’s session; however, you can find information regarding Web Services security within the SAP NetWeaver Security Guide.
  - http://help.sap.com/saphelp_nw04s/helpdata/en/54/a5d13f83a14d21e1000000a1550b0/frameset.htm
Basic scenarios allow direct access from the Internet to back-end systems.

A more secure configuration is to place an application gateway between the user and the back-end system.

See this SAP TechED session
Internet-Facing Scenario – Complex

- Multiple entry points
- Multiple protocols
- Multiple applications
Internet Scenarios with mySAP Business Suite

- mySAP ERP
  - E-Recruiting
  - Employee Self-Service
  - Human Capital Management

- mySAP Supplier Relationship Management (mySAP SRM)
  - SAP Enterprise Buyer
  - Supplier Self-Service applications
  - Live Auction

- mySAP Customer Relationship Management (mySAP CRM)
  - Internet Pricing and Configurator
  - B2C integrations

- And many more
What We’ll Cover ...

Introduction
Internet Security Concepts and Scenarios

**Security Architecture**
Implementing the Right Security
Configuring the SAP Web Application Server
Configuring the Secure Client Access
Troubleshooting Security Configuration
Wrap-up
Some common hardware infrastructure

- **Firewalls**
  - Security for access control, user authentication, and network and application-level attack protection

- **Web Appliances**
  - Scalable approach to accelerating application performance, increasing WAN capacity, and enabling application prioritization and visibility

- **Load Balancers**
  - Provide a means to scale your application infrastructure and facilitate HA and switchover solutions by distributing load to clusters of servers

- **Application Gateways**
  - Protect applications from direct access by clients; can also provide performance improvements when used in combination with caching
Identity management
- Commercial products used to manage users, roles, and provisioning
- Provides secure user administration and maintenance capabilities for enterprise applications and infrastructures

Access management
- Commercial products used to manage and control access to Web resources (URLs)
- Provides access control capabilities that are integrated with identity management and Single Sign-On (SSO) solutions
  - Typically, they protect URLs and restrict client access to unauthorized resources
Secure Network Topology and Layered Defense

Internet

Outer DMZ

Firewall

Application Gateways

SAP Web AS, Enterprise Portal, or other Web service

Inner DMZ

Firewall

Application server farm

Back-end Networks

ERP

ERP

DIR

Intranet

Firewall

Firewall

Firewall

© SAP AG 2006, 16
What Is an Application Gateway?

Application that acts as a “middleman” between your computer and the Internet resources you are accessing (e.g., Web sites, FTP archives)

No direct connection between client of the local network and server on the Internet (or vice versa)

Relays traffic between actual client and actual server while doing checks and access controls that typical client and server SW does not support
Possible Features of an Application Gateway

Pre-authentication and authentication

- Is the user permitted to access the server/service/URL?

Validity of a service request/URL

- Is access to the requested URL via the Internet permitted?
- Does the request contain no known exploits?
- Is the source of the request permitted (sender address)?

Integrity and correctness of the message (for example, SOAP)

- Is the destination for the SOAP message known, and is access to it via the Internet permitted?
- Is the sender permitted?

Auditing

Other (non-security-related)

- Combining different information sources under one external name (content unification)
What We’ll Cover ...

Introduction
Internet Security Concepts and Scenarios
Security Architecture
Implementing the Right Security
Configuring the SAP Web Application Server
Configuring the Secure Client Access
Troubleshooting Security Configuration
Wrap-up
Understanding Security Policies in Your Organization

Current policies drive requirements and may create constraints
- Know what the current policies are, and discuss your project in order to understand how those policies will impact your project.

New policies may be necessary to address new scenarios
- If this is the first time your organization has allowed Internet access to back-end systems, you may need to proactively address policy requirements and drive new policies that clearly define the rules your implementation must live by.

Be aware of lead times – security takes TIME!
- Security policies are developed after careful consideration of all requirements, costs, and desired outcomes. Security is a critical aspect of your IT practice – a good policy TAKES TIME to develop.
- Don’t rush security people – they can always say NO in a hurry.
Planning Appropriate Security

Securing the Application
- Ensure that access is properly restricted and authentication mechanisms meet your company’s security policies

Securing the Data
- Be aware of the data-security requirements and implement rule-based access control to ensure that application data is displayed only to users authorized to see it

Securing the Systems
- Keep critical systems out of Internet-facing security zones and preferably keep them in their own application zones where access is strictly controlled by firewalls and other security infrastructure
Security Awareness in the Implementation Project

Start Security Planning Early
- A review of current security practices and policies should be undertaken at the beginning of the implementation
- No development should occur until you understand how policies will drive your implementation

Test with Security in Place
- Security adds complexity to the implementation
- Test with security in place to validate that the processes and programs work under the most strict security requirements possible

Understand the Performance Impact of Security
- By testing with security configuration in place, you will be aware of any potential performance bottlenecks that might be created by the implementation of strict security
Why Audit Security?
- Do you know everything about the security policies and practices in your organization?
- Ask for an audit, and the security team becomes a partner and not an adversary!

Benefits of Early Assessment Efforts
- Know when and why your design might not meet security requirements
- Understand potential performance impacts and set proper expectations

Understanding the Audit Process
- An audit is an opportunity for you to improve your implementation
- Don’t try to hide anything – there’s no such thing as security by obscurity
Use encrypted communications (SNC/SSL)

Check/set good password rules and session timeouts

Protect OS and DB users of the SAP system

Tune authorizations for technical users to the minimum required

Enable auditing and logging (also HTTP logging)

Only enable required services and applications

Apply available patches regularly

Do not install/remove test/demo software from productive systems, where possible
Internet Communication Manager (ICM) and Internet Communication Framework (ICF)

To guarantee the security of your ICF connections, include the following points in your setup and take the appropriate measures:

- Activate only those services that you really need
- Define authentication methods and logon sequences for users of services
- Use SSL for ICF communication
- Be restrictive when assigning ICF authorizations
Security Recommendations

- Install the SAP Cryptographic Library for Java to enable encryption of system credentials
- Restrict authorizations to administrative tools
- Do not install/remove test/demo software from productive systems, where possible
- Protect network access to administrative interfaces
  - P4 (visual administrator)
  - telnet (J2EE console)
As SAP NetWeaver Enterprise Portal runs on SAP Web Application Server Java, make sure you have followed the suggestions there. In addition:

- Modify all access restrictions to allow required but minimal access only
- Apply all available and recommended patches regularly for all components used in the Enterprise Portal
- Modify the portal permissions for iViews and security zones to provide users with exactly the permissions they require and not more
- In an Enterprise Portal installation that will be used productively, remove all iViews that are not required
- Delegate administration tasks among several users
- Disable user self-registration if not required
- Remove unused iViews and portal components
What We’ll Cover ...

Introduction
Internet Security Concepts and Scenarios
Security Architecture
Implementing the Right Security
Configuring the SAP Web Application Server
Configuring the Secure Client Access
Troubleshooting Security Configuration
Wrap-up
1. Client makes request
2. Enterprise Portal computes the target URL and returns an HTTP-302 redirect to the client
3. Client makes request based on HTTP-302 response directly to SAP system
4. SAP system returns result
For IAC iViews

Target URL: http://ssphlrig607.phl.sap.corp:8000/
Enterprise Portal URL Computation – ITS with Proxy

For IAC iViews

Property Category: Internet Transaction Server (ITS)

- ITS Description: WAJ
- ITS Host Name: proxy.phl.sap.corp:8000
- ITS Path: sap/bc/gui/sap/its
- ITS Protocol: https

Target URL: http://ssphlrig607.phl.sap.corp:8000/
In this scenario, the <protocol>://<host>:<port> are for the proxy in all cases
A common issue with proxies is the matter of URL generation by the back-end (proxied) applications

- When applications generate URLs to other applications or to themselves, you must ensure that all hostnames can be resolved by the client browser.

Use of the HTTP Host header is the proper way to generate absolute URLs.

Proxies such as Apache provide the ProxyPreserveHost directive that ensures the hostname requested by the client is passed all the way through to the application.

SAP NetWeaver '04 and NetWeaver 2004s systems have configuration capabilities that provide a mechanism for controlling what hostname is returned to the client.
Sometimes it is important to create fully specified URLs. For some of these cases you could use the host header and determine the port from the list of active ports configured on the server.

This procedure often works well, but not always. First of all, some cases that need fully specified URLs are considered:

- When the protocol is switched. This is usually a switch from HTTP to HTTPS to ensure the data transfer is secure. This case arises often:
  - When a Java applet is loaded sometimes a fully specified URL is required in a complex frameset, because otherwise the applet is loaded from the server where the root document is located rather than from the frame owner where the applet is located
  - Return URLs in typical catalog applications. Here a URL is required that is used to return data to the server and for the specific application. In this case a fully specified URL is also necessary.
Using Proxies for Back-End Systems

Proxies are a common component of IT landscapes.

Application gateway is another name for proxy.

Proxies provide a useful layer of abstraction that hides the real host:port information from clients.

Proxies provide a useful intermediate layer that prevents direct access to the servers that host the applications.

Section 8.1.3 or RFC 2616 addresses rules for Internet proxies.

Therefore, absolute URL generation must take into account that a proxy or gateway is an intermediary between the client and the server.
Internet Transaction Server (ITS)

- Without any configuration, the ITS will generate URLs using the hostname of the SAP Web AS server (itself)
- This behavior can be modified using TX SE16, which maintains the HTTPURLLOC table

This should be the hostname of your proxy server!
HTTPURLLOC – Definitions

- **MANDT**
  - Client for which the configuration is to be performed. Different clients represent different identities, for which different configuration data is needed. For instance, the hostname could be server.abc.com for client 100, whereas it could be www.xyz.de for client 200.

- **SORT_KEY**
  - Sort sequence of entries. Entries in this sequence are compared from top to bottom, and the first matching entry is used.

- **APPLICATN**
  - This string can be used to filter the entry for special application types. If this is configured, this entry is used as the template to determine how the current application that would like to generate a fully specified URL is used. For BSP, the string /BSP/<namespace>/<name> is always used.
  - Leave this field empty if this configuration is used again and again
  - Examples of values:
    - /BSP/SAP/IT00 assigns access rights only to BSP application IT00
    - /BSP/XYZ/* assigns access rights to all BSP applications in the XYZ namespace (registered namespace of the organization)
    - /BSP/* assigns access rights to BSP applications
    - An empty string assigns access rights for all applications
HTTPURLLOC – Definitions (cont.)

- **PROTOCOL**
  - Protocol for which a fully specified URL must be generated. It can be HTTP or HTTPS.

- **HOST**
  - Mandatory field for generating the new URL
  - If the host is requested from an API, this field is used as a filter for the host header of the inbound request to decide which configuration line is to be used
  - It is a special case when the exception table is not to be used for an entry. If the field for the host is empty and the other parameters tally, this field is used as an indicator to specify that the local host data is used for generating the URL, and not the exception table.

- **PORT**
  - Port number used in the new, fully specified generated URL
The browser communicates always with the AS-ABAP through a reverse proxy server. For this reason all generated URLs must contain the name and port of the reverse proxy server.

**Example:**


Host: Webas.sap.corp (http:1080, https:1443)

HTTPURLLOC

<table>
<thead>
<tr>
<th>MANDT</th>
<th>SORT_KEY</th>
<th>PROTOCOL</th>
<th>APPL</th>
<th>HOST</th>
<th>PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>C10</td>
<td>HTTP</td>
<td>*</td>
<td><a href="http://WWW.SAP.COM">WWW.SAP.COM</a></td>
<td>80</td>
</tr>
<tr>
<td>100</td>
<td>C11</td>
<td>HTTPS</td>
<td>*</td>
<td><a href="http://WWW.SAP.COM">WWW.SAP.COM</a></td>
<td>443</td>
</tr>
</tbody>
</table>
Direct Communication and Through a Reverse Proxy

Some Web browsers always communicate with the AS-ABAP through a reverse proxy server (Internet scenario). Other browsers communicate directly with the AS-ABAP (for example, in an organization’s intranet).

Example:


Host: Webas.sap.corp (http:1080, https:1443)

<table>
<thead>
<tr>
<th>MANDT</th>
<th>SORT_KEY</th>
<th>PROTOCOL</th>
<th>APPL</th>
<th>HOST</th>
<th>PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>020</td>
<td>HTTP</td>
<td>*</td>
<td>WEBAS.SAP.CORP</td>
<td>1080</td>
</tr>
<tr>
<td>100</td>
<td>021</td>
<td>HTTPS</td>
<td>*</td>
<td>WEBAS.SAP.CORP</td>
<td>1443</td>
</tr>
<tr>
<td>100</td>
<td>030</td>
<td>HTTP</td>
<td>*</td>
<td><a href="http://WWW.SAP.COM">WWW.SAP.COM</a></td>
<td>80</td>
</tr>
<tr>
<td>100</td>
<td>031</td>
<td>HTTPS</td>
<td>*</td>
<td><a href="http://WWW.SAP.COM">WWW.SAP.COM</a></td>
<td>443</td>
</tr>
</tbody>
</table>
When HTTPS is used in the Internet, HTTP can be used from the reverse proxy to the server. In this special case, the generation of absolute URLs is very important, particularly for special resources such as return addresses that match the external protocol used in the Internet.

When the programming interface is called without a specified protocol, instead only a server object is specified, and the protocol currently in use determines which name and port to use. In such a case, one entry only is usually sufficient. The protocol to be used is returned from the API call.

**HTTPURLLOC**

<table>
<thead>
<tr>
<th>MANDT</th>
<th>SORT_KEY</th>
<th>PROTOCOL</th>
<th>APPL</th>
<th>HOST</th>
<th>PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>010</td>
<td>HTTPS</td>
<td>*</td>
<td><a href="http://WWW.SAP.COM">WWW.SAP.COM</a></td>
<td>443</td>
</tr>
</tbody>
</table>

It is important that for the inbound request the reverse proxy uses the active protocol used in the Internet section of the request. The Web dispatcher transfers this information into a header field named ClientProtocol, when option wdisp/add_clientprotocol_header = 1 is set. With an Apache reverse proxy, this can be done using the request header with client protocol HTTPS.
A URL configuration table often has to be used during the logon procedure. This is particularly important if a Web dispatcher is used that has configured various ports, and when the logon application must switch to HTTPS to guarantee the secure transfer of passwords.

The logon application runs in two different clients; one runs in client 000 as user SAPSYS until the logon has been successfully completed, and the other runs in the designated client with the logged on user. During the first part of the logon, the logon application finds Table HTTPURLLOC in client 000. Therefore, it is essential that all entries are duplicated in client 000 when the logon application is in use.

Starting from the second scenario table, HTTPURLLOC looks like:

<table>
<thead>
<tr>
<th>MANDT</th>
<th>SORT_KEY</th>
<th>PROTOCOL</th>
<th>APPL</th>
<th>HOST</th>
<th>PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>010</td>
<td>HTTP</td>
<td>*</td>
<td><a href="http://www.sap.com">www.sap.com</a></td>
<td>80</td>
</tr>
<tr>
<td>000</td>
<td>011</td>
<td>HTTPS</td>
<td>*</td>
<td><a href="http://www.sap.com">www.sap.com</a></td>
<td>443</td>
</tr>
<tr>
<td>100</td>
<td>010</td>
<td>HTTP</td>
<td>*</td>
<td><a href="http://www.sap.com">www.sap.com</a></td>
<td>80</td>
</tr>
<tr>
<td>100</td>
<td>011</td>
<td>HTTPS</td>
<td>*</td>
<td><a href="http://www.sap.com">www.sap.com</a></td>
<td>443</td>
</tr>
</tbody>
</table>
Java Dispatcher

- The HTTP Provider Service running under the Dispatcher Node of the Java engine provides a parameter ProxyMappings that facilitates use of front-end proxies serving SAP Web AS Java content.

- This parameter works in much the same way the HTTPURLLOC table does for ABAP.

- Client requests from a proxy will use the hostname configured in the ProxyMappings parameter when URLs are generated and returned to the client in HTTP responses.

- The Dispatcher is also where you enable SSL communication for the Java stack.
Java Server

- There isn’t any specific configuration of the server node required for proxies.
- You do need to enable the SSL service of the server and dispatcher, as well as complete the SSL configuration, in order to use SSL for client/server communication.
- It is recommended that SSL be used in every case where SSO and/or X.509 certificates are used for authentication.
- It is further recommended to use SSL to prevent unauthorized persons from reading traffic intercepted during transmission between the client and server.
Digital Certificates

- Digital certificates provide a means to authenticate users; they are the most secure method of authentication available.
- SSL must be used when digital certificates are used to prevent user credentials from being stolen while in transit.

Keystores

- Certificates are stored in the keystores of the various components. ABAP uses the external cryptographic libraries while the Java engine uses Java libraries.
ICM and ICF Configuration – Logon Methods

In TX SICF you can change the logon behavior of services. This allows you to restrict logon to only certificate or SSO (saplogonticket), for instance, or only allow SSL.
What We’ll Cover ...

Introduction
Internet Security Concepts and Scenarios
Security Architecture
Implementing the Right Security
Configuring the SAP Web Application Server
Configuring the Secure Client Access
Troubleshooting Security Configuration
Wrap-up
Putting It All Together ...

SSL enablement merits a whole discussion by itself, but for our purposes today we assume it is configured and implemented ...

We’ve covered the back-end ABAP configuration and the front-end proxy (Apache or SAP Web Dispatcher) configuration. Now we need to address the portal configuration and its integration through an application gateway.
You can integrate the following SAP applications in SAP Enterprise Portal as an iView:

- R/3 transactions
- Business Server Page (BSP) applications
- BW reports (BEx Web Application starting with Release 3.x)
- Crystal Enterprise reports
- Internet application components (IACs)
- MiniApps
- Appropriate iView templates are available in the Portal Content Studio for integrating the individual SAP applications
Creating SAP Systems in the Landscape Editor

The template for an SAP system defines the specific parameters needed to connect to an SAP application, and it contains a reference to the SAP connector.

The SAP system inherits these properties – some with default values, and others that require the setting of values. You edit the system by inserting needed property values and by modifying default values, if necessary.

SAP systems can be based on one of two templates:

- One template defines properties that support load balancing, making it more useful for large enterprises.
- The other template defines properties that support a dedicated system.
Building R/3 Systems in the Landscape Manager

- We typically build R/3 connections using the REAL HOST information!
- When we use proxies to access these back-end systems, we use the hostname of the proxy instead of the SAP Web AS when we define the system connection

Using Proxies Instead of Direct Connection

- The Enterprise Portal (EP) does not expect to find a Web AS behind a proxy
- When properly configured, the EP will never know that the proxy isn’t the real back-end host
Creating an R/3 System

System Wizard

Step 1: Template Selection

This wizard guides you through the steps required to create a portal system based on an existing template. The template list reflects the contents of the cache, and may need refreshing.

Choose Template *
- EP 5.0 System
- HTTP System
- JDBC System
- KM Lotus System
- KM WebDAV System
- KM Windows System
- SAP system using connection string
- SAP system using dedicated application server
- SAP system with load balancing
- Yahoo! System

© SAP AG 2006, 52
Maintain the parameters for ITS (IAC applications) and/or for the Web Application Server (BSP applications, BW reports)

It helps to note whether the system is the actual host or a proxy!
SAPLOGONTICKET is the preferred method of logon. If you choose UIDPW, you should make sure you allow users to map their accounts.
Creating IAC iViews

iView Wizard

Step 1: Template Selection

- RM Upload View
- RM EISL Form Builder Check View
- RM EISL Form Builder View
- Portal Activity Report View
- Portal to Remote View
- Quota View
- SAP BTP View
- SAP BW Report View
- SAP iView (JSON)
- SAP Web Dynpro View
- URL View
- Web Target View
- WIS Map View
- XML View

General Properties

- iView Name: WEBGUI
- iView ID: WEBGUI
- iView ID Prefix (Example: com.compannena): com.nitshouse
- Master Language: English
- Description: Start a WEBGUI

Application Parameter

Enter the parameter(s) of the application for which you want to create the View

- System:
- Internet Application Component (IAC):
- Application Parameters:
  - sap-client=80C
The SAP Web Dispatcher provides full proxy capability but is not able to proxy for multiple content sources.

The SAP Web Dispatcher is able to proxy and load-balance for a cluster of Web Application Servers as it communicates directly with the message server of the Web AS central instance.
You can find the SAP Web Dispatcher executable in the /sapmnt/<SID>/exe directory of any SAP Web AS. Use the
**bootstrap argument** for initial configuration.

- Remember to note the password generated for the admin user when you first configure the software.

An example configuration is shown in the next few slides. After initial configuration, you can modify the start profile to change parameters and properties.
Example interactive configuration of sapWebdispatcher:

us5003> ./sapWebdispatcher -bootstrap
us5003:root# ./sapWebdisp -bootstrap

SAP Web Dispatcher Bootstrap

This bootstrap will perform the following steps:
1. create profile file "sapWebdisp.pfl" for SAP Web Dispatcher (if not already existing)
2. create user for Web based administration in file "icmauth.txt" (if not already existing)
3. start SAP Web Dispatcher with the created profile

After the bootstrap you can use the Web based administration
Generating Profile "sapWebdisp.pfl"
Hostname of Message Server (rdisp/ms_host): ls4091.wdf.sap.corp
HTTP Port of Message Server (ms_host/http_port): 8891
Unique Instance Number for SAP Web Dispatcher (SAPSYSTEM): 91
HTTP port number for SAP Web Dispatcher: 8891
Profile "sapWebdisp.pfl" generated
Authentication file "icmauth.txt" generated
Web Administration user is "icmadm" with password "5574"
Restart sapWebdisp with profile: sapWebdisp.pfl
sapWebdisp started with new pid 10005
Please extract archive "icmadmin.SAR" to directory ./admin
Web administration accessible with "http://us5003:8891/sap/wdisp/admin/default.html"
SAP Web Dispatcher bootstrap ended (rc=0)
us5003:root# *** SAP Web Dispatcher up and operational (pid: 10005) ***
Results

If the internal ITS is configured properly in TX SCIF, you can start a Web GUI directly using:


Without any proxy configuration, you will be redirected to this URL on login:


It is the default behavior of the internal ITS

To understand where this URL comes from, you should look at the Web GUI configuration in SICF

The ICF configuration shows:
Apache Configuration

Apache requires two modules to enable full reverse proxy of Enterprise Portal and SAP Web AS ABAP integration:

- mod_proxy
- mod_rewrite

In httpd.conf Apache configuration file:

LoadModule proxy_module modules/mod_proxy.so
LoadModule rewrite_module modules/mod_rewrite.so

ProxyPass /sap http://ls4089.wdf.sap.corp:50089/sap
ProxyPassReverse /sap http://ls4089.wdf.sap.corp:50089/sap
Apache Proxy and Rewrite Tip

But there’s a twist ...

- Proxy rules fall over when the ICM puts session information into the URLs; then you need to add a rewrite rule

```
RewriteRule ^/(sap\.(.*) http://ls4089.wdf.sap.corp:50089/$1 [P,L]
```

Check the Apache documentation for all the details of proxy and rewriting

http://httpd.apache.org/docs/2.2/
Configuration Summary

What have we done?

1. Configured the ABAP system
2. Configured EP systems
3. Created the iViews
4. Configured the proxy or gateway
Introduction
Internet Security Concepts and Scenarios
Security Architecture
Implementing the Right Security
Configuring the SAP Web Application Server
Configuring the Secure Client Access

Troubleshooting Security Configuration

Wrap-up
Hostname and Domains
- Don’t blame SAP for issues with cookies and certificates if you do not maintain your servers with real hostnames and in the same domain. The rules for cookie and certificate handling are defined in RFC 2616 for HTTP/1.1.

The Configuration Isn’t Trivial
- Setup is the most common source of connectivity issues

Users and Authorizations
- Double-check all users and ensure that they can log on interactively prior to testing the same action through SSO

Protocols
- Validate your SSL separately!
Tracing the Security Communication

Several SAP Notes address the topic of tracing and logging for security communication:

Note 457222 – Gathering Security Trace Information

Note 495911 – Trace Analysis for Logon Problems

Note 320991 – Error Codes for Logon (list)

Note 791205 – Single Sign-On Using SAP Logon Tickets

You need to trace the communication through all components:

Client – browser-based, such as HTTP watch

Proxy – native tools/capabilities of the proxy

Portal – enable HTTP tracing in the HTTP provider service of the dispatcher

ABAP – sm50 and related methods described in the above SAP Notes
Logging Messages with SAP

Messages opened regarding security communication should have traces and logs uploaded at the time of message creation
- This will significantly improve response outcomes

Providing a landscape diagram will help the support staff understand your configuration better

Providing a detailed overview of the systems (hosts/OS/applications) allows for better reading/understanding of the traces
Keep-alive settings are used to optimize the network traffic and conserve resources.

In a gateway scenario, various components act as both client and server and thus maintain keep-alive connections with two different systems.

![Diagram showing keep-alive connections between Application Gateway, Enterprise Portal, and mySAP ERP.]

Keep-Alive = 60 seconds

Keep-Alive = 900 seconds

Connections to the back-end are pooled; many clients use the same back-end connection.

To prevent proxy errors related to closed TCP/IP sockets, it is necessary to configure back-end applications with higher timeouts than the gateway.

Otherwise, a back-end server may close a pooled connection without the gateway knowing the socket is closed.
Introduction
Internet Security Concepts and Scenarios
Security Architecture
Implementing the Right Security
Configuring the SAP Web Application Server
Configuring the Secure Client Access
Troubleshooting Security Configuration
Wrap-up
Guides and Documentation

Security at SAP – http://service.sap.com/security*

SAP NetWeaver Security Guide –
http://help.sap.com/saphelp_nw04/helpdata/en/8c/2ec59131d7f84ea514a67d628925a9/frameset.htm

Enable SAPGUI for HTML with integrated ITS –
https://Websmp204.sapag.de/~sapdownload/011000358700003584472004E/WebGUI_NW04.pdf*

* Requires login credentials to the SAP Service Marketplace
Resources

Public Web:
- www.sap.com
- SAP Developer Network: www.sdn.sap.com*
- SAP Customer Services Network: www.sap.com/services/

Related SAP Education Training Opportunities
- www.sap.com/education/

* Requires login credentials to the SAP Service Marketplace
Related Content From SMP

http://service.sap.com/NW04 alias Documentation link*
http://service.sap.com/NW2004S alias Documentation link*

* Requires login credentials to the SAP Service Marketplace
SAP Service Marketplace – Notes

- 833960 – Supported Application Gateway Configurations
- 750292 – BSP: URL Generation in a config of Web AS with Web Dispatcher
- 855574 – 640SP<=12, 620SP<=53: HTTPS and Web dispatcher
- 847636 – Attachments are not displayed: BBP_ROOT_URL
- 561885 – Generation of URLs (SAP Web Dispatcher/Reverse Proxy)
- 815658 – SSL-based communications without SAP Cryptographic Libraries
- 812903 – NW’04 Problems with absolute URLs/Reverse Proxy
- 812901 – EP 6.0 Problems with absolute URLs/Apache 2/Reverse Proxy
- 693220 – Recommendations for the security of ITS services
- 725931 – Security: ITS, security-relevant settings for IACs
- 457222 – Gathering Security Trace Information
- 495911 – Trace Analysis for Logon Problems
- 320991 – Error Codes for Logon (list)
- 791205 – Single Sign-On Using SAP Logon Tickets
7 Key Points to Take Home

- Implement appropriate technology to ensure regulatory Sarbanes-Oxley (SOX) compliance
- Understand the relationship between a threat and the corresponding safeguard
- Use infrastructure wisely
- Document the configuration necessary to complete each integration
- Manage the security configurations centrally for all applications
- Use encryption for all network communications if you want the best possible security
- Always look to the latest guides, SAP Notes, and documentation
How to contact me:
nicholas.holshouser@sap.com
Appendix

Useful help links:

SAP NetWeaver Security Guide:
http://help.sap.com/saphelp_nw04s/helpdata/en/8c/2ec59131d7f84ea514a67d628925a9/content.htm

URL Generation:
http://help.sap.com/saphelp_nw04s/helpdata/en/59/31ae42e0fac911e10000000a1550b0/content.htm

SAP Web Dispatcher:
http://help.sap.com/saphelp_nw2004s/helpdata/en/42/5cfd3b0e59774ee10000000a114084/content.htm

Apache Web Server:
http://httpd.apache.org
The central hub for the SAP technology community

- Everyone can connect, contribute, and collaborate—consultants, administrators, and developers
- Focus around SAP NetWeaver and SAP xApps

High quality of technical resources

- Articles, how-to guides, Weblogs, collaborative areas, discussion forums and downloads, toolkits, and code samples

A collaboration platform, not a one-way street

- SAP experts from customers, partners, and SAP

SDN is powered by SAP NetWeaver™

- Built on the SAP Enterprise Portal
- Featuring collaboration capabilities of SAP Knowledge Management

http://sdn.sap.com