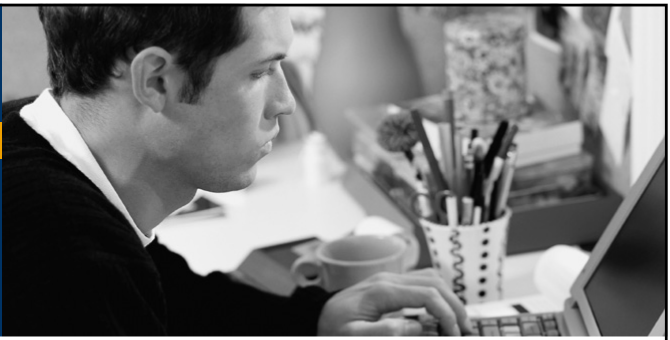


SCUR204 Strong Infrastructure and Network Security for Heterogeneous Applications

Patrick Hildenbrand
PM Security, SAP AG Germany

THE BEST-RUN BUSINESSES RUN SAP

Learning Objectives

As a result of this workshop, you will be able to:

- List security goals, threats and safeguards
- Categorize security measures
- List the necessary steps towards establishing a secure system environment

THE BEST-RUN BUSINESSES RUN SAP

Agenda

Security Threats

Technical Security Safeguards

- Firewalls
- Application Gateways
- Intrusion Detection Systems
- Cryptography

Applying Infrastructure Protection

- Example setup for SAP WebAS

Defense in Depth

Summary

Agenda

Security Threats

Technical Security Safeguards

- Firewalls
- Application Gateways
- Intrusion Detection Systems
- Cryptography

Applying Infrastructure Protection

- Example setup for SAP WebAS

Defense in Depth

Summary

Why Security?

Protection of Intellectual Property

Compliance

Legal Issues and Contracts

Trust Relationship to Business Partners

Continuous Business Operations

Protection of Image

Correctness of Data

Expenses Associated with Security Breaches

Hypothetical $1,000,000 theft from a small Online Bank

Expense	Cost
Return stolen money (1,000 accounts @ $1,000 each)	$1,000,000
48 hours network downtime @ 2mm/hour	$96,000,000
Emergency Audit	$1,000,000
PR damage control for 3 months	$6,000,000
Increased fraud premiums	$5,000,000
Loss of 10,000 accounts to other banks @ $250/account	$2,500,000
Total	**$111,500,000**

Source: Forrester Research

Computer Crime: a Security Survey (2002)

90% of those interviewed detected computer security breaches within the last twelve months

80% acknowledged financial losses due to computer breaches

223 respondents (44%) were willing and/or able to quantify their financial losses (altogether $455,848,000)

55% reported denial of service

Source: Computer Security Institute http://www.gocsi.com/press/20020407.html

CSI
COMPUTER
SECURITY
INSTITUTE

Goals of a Secure Business Process

Goals

Authentication

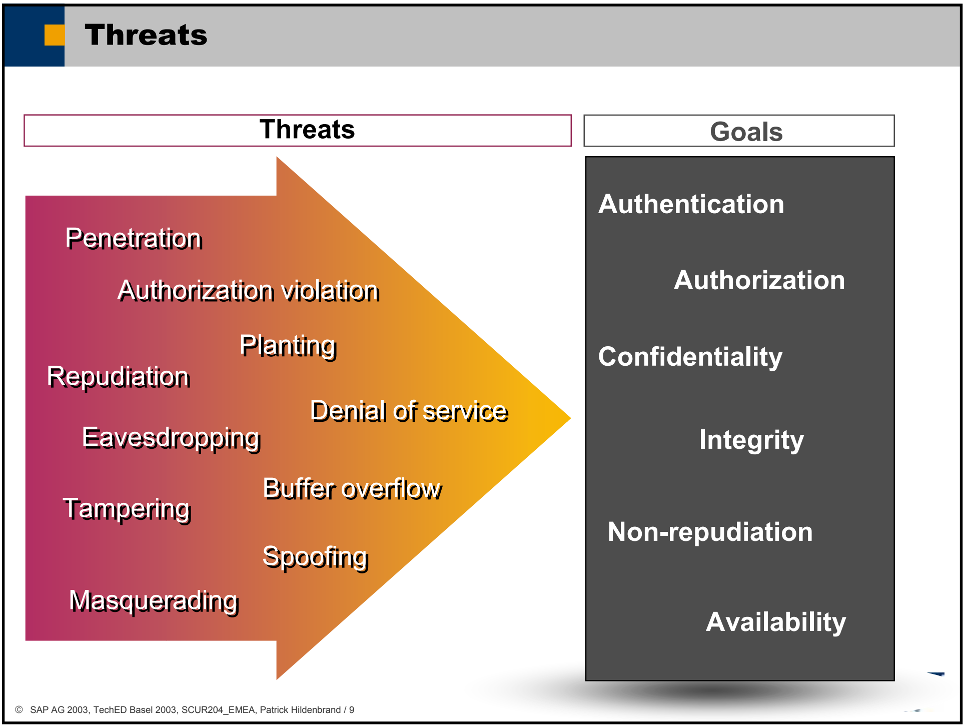
Authorization

Confidentiality

Integrity

Non-repudiation

Availability



Threats

Threats

Penetration

Authorization violation

Planting

Repudiation

Denial of service

Eavesdropping

Buffer overflow

Tampering

Spoofing

Masquerading

Goals

Authentication

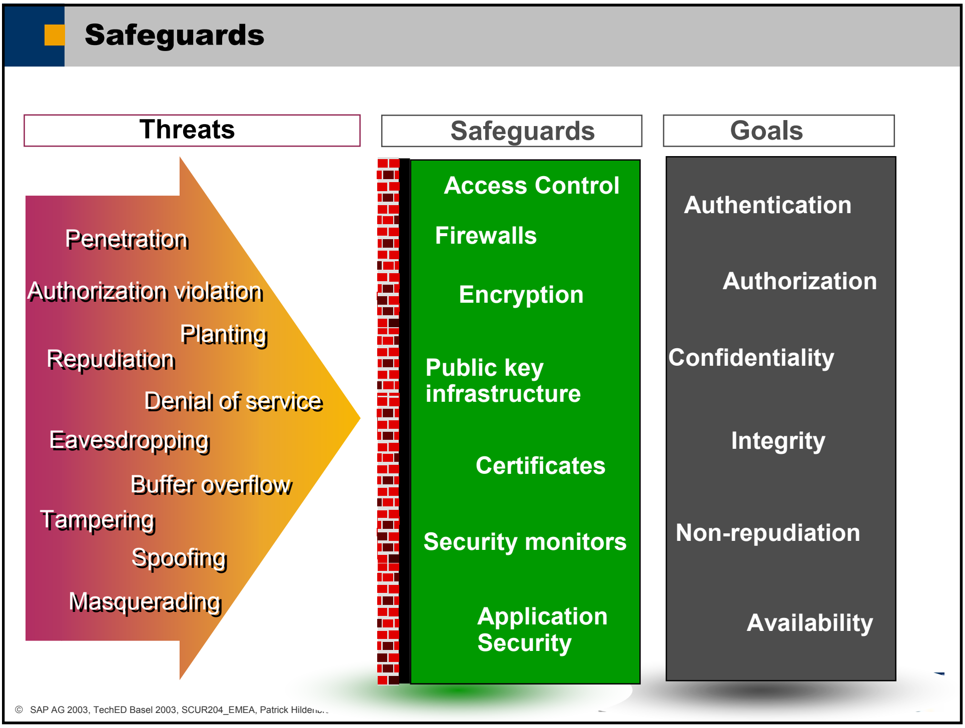
Authorization

Confidentiality

Integrity

Non-repudiation

Availability



Safeguards

Threats

Penetration

Authorization violation

Planting

Repudiation

Denial of service

Eavesdropping

Buffer overflow

Tampering

Spoofing

Masquerading

Safeguards

Access Control

Firewalls

Encryption

Public key infrastructure

Certificates

Security monitors

Application Security

Goals

Authentication

Authorization

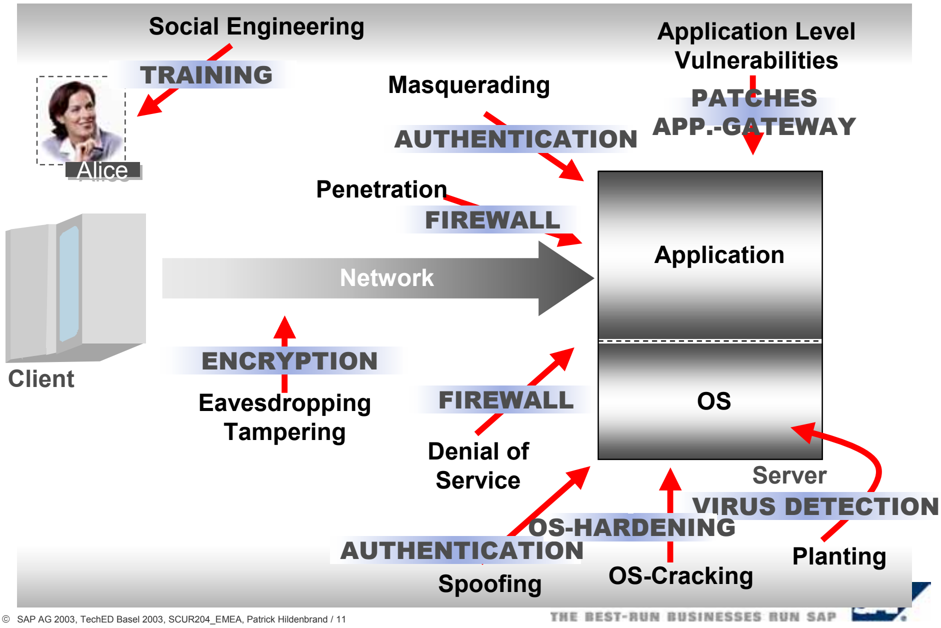
Confidentiality

Integrity

Non-repudiation

Availability

Safeguards Versus Threats



Social Engineering

TRAINING

Alice

Masquerading

AUTHENTICATION

Application Level Vulnerabilities

PATCHES

APP.-GATEWAY

Penetration

FIREWALL

Client

Network

Application

OS

ENCRYPTION

Eavesdropping

Tampering

FIREWALL

Denial of Service

Server

VIRUS DETECTION

OS-HARDENING

AUTHENTICATION

Spoofing

OS-Cracking

Planting

Types of Security Safeguards

- ❒ Organizational
  - ❒ Security policies
  - ❒ Continuous monitoring
  - ❒ Training
  - ❒ Disaster plans

- ❒ Physical
  - ❒ Server facilities
  - ❒ Computers
  - ❒ Rooms
  - ❒ Buildings
  - ❒ Smoke detection

- ❒ Technical
  - ❒ Encryption
  - ❒ Security Monitors
  - ❒ Access control
  - ❒ Firewalls
  - ❒...

Agenda

Security Threats

Technical Security Safeguards

- Firewalls
- Application Gateways
- Intrusion Detection Systems
- Cryptography

Applying Infrastructure Protection

- Example setup for SAP WebAS

Defense in Depth

Summary

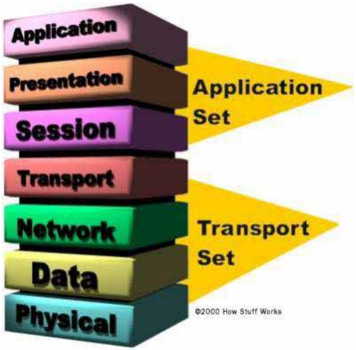
Protecting the Border Using Firewalls

Firewalls are mechanisms used to protect access between different systems

Firewalls can be used to connect and control internal/secure, intermediate and/or external/insecure networks

Firewalls can be realized as IP-filters, filtering proxy gateways or a combination thereof

Firewalls can be used to connect networks using private (RFC1918), conflicting and public adresses



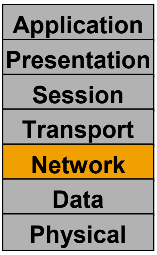
But No Firewall is able to provide Perfect Security

SUPER TOP SECRET
TOP SECRET
RET
LOS ALAMOS LABORATORY
THE CHRISTIAN SCIENCE MONITOR
Bennett

http://www.claybennett.com/pages/los_alamos_security.html

Types of Firewalls – Packet Filters

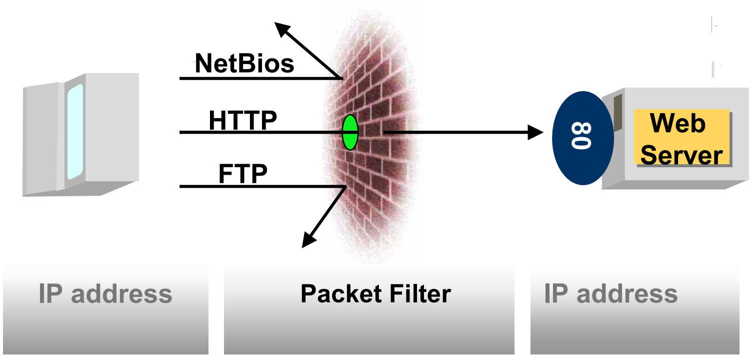
- ‘Classic router solution’
- Only checks for IP header information
- Pros
  - Cost-effective
  - Fast – data gets routed immediately
  - Simple setup
  - Transparent to the application
- Cons
  - Prone to IP spoofing attacks
  - Ruleset can be complex and hard to maintain
- Info required for setup
  - IP adresses
  - Ports used
  - Direction of traffic



Application
Presentation
Session
Transport
Network
Data
Physical

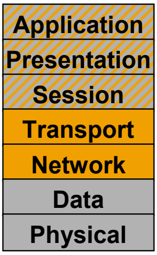
Packet Filtering

Policies within packet filters can be set that will restrict traffic based on IP addresses, ports, or even the protocols being used.



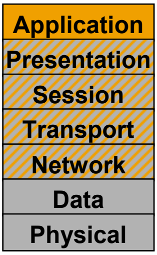
Types of Firewalls – Stateful Packet Filters

- ‘Typical firewall solution’
- Checks for IP address and ports
- Checks for TCP Sessions
- Can check for certain patterns in data
- Is able to detect protocol and add dynamic rules depending on protocol requirements (NFS, FTP)
- Pros
  - Good overall security
- Cons
  - May not be able to detect application based attacks
  - May introduce its own bugs
  - Does not understand application payload
- Info required for setup
  - IP addresses
  - Ports used
  - Direction of traffic
  - Protocol used



Types of Firewalls – Application Level Gateways

- Works on the application layer
- ‘Understands’ the traffic of the application
- Usually the packets are rebuilt by the gateway
- Pros
  - Highest protection
- Cons
  - Not transparent to the application
  - Proxies only available for standard applications
  - Slow, difficult to configure
  - May introduce its own bugs
- Info required for setup
  - IP addresses
  - Ports used
  - Direction of traffic
  - Protocol used
  - Protocol data permitted



Agenda

Security Threats

Technical Security Safeguards

- Firewalls
- Application Gateways
- Intrusion Detection Systems
- Cryptography

Applying Infrastructure Protection

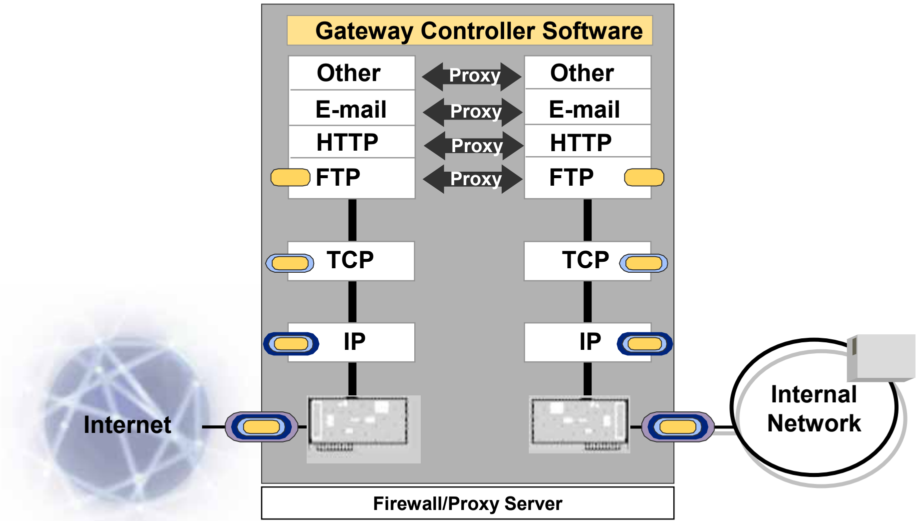
- Example setup for SAP WebAS

Defense in Depth

Summary

Application Level Firewall (Proxy)

Should be run on a dedicated host



Gateway Controller Software

Other — Proxy — Other

E-mail — Proxy — E-mail

HTTP — Proxy — HTTP

FTP — Proxy — FTP

TCP — TCP

IP — IP

Internet

Internal Network

Firewall/Proxy Server

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)

Agenda

Security Threats

Technical Security Safeguards

- Firewalls
- Application Gateways
- Intrusion Detection Systems
- Cryptography

Applying Infrastructure Protection

- Example setup for SAP WebAS

Defense in Depth

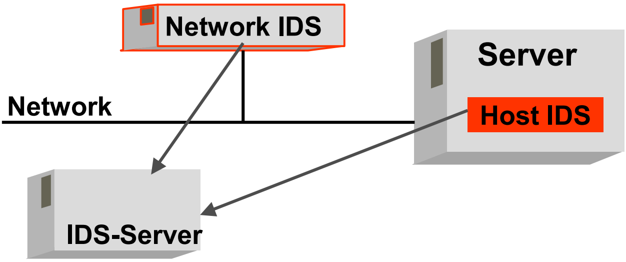
Summary

THE BEST-RUN BUSINESSES RUN SAP

IDS - Intrusion Detection System

An IDS is an extension to a secure environment, providing notification of attempted or successful security breaches.
An IDS consists of

- one or more network or host sensor(s)
- one or more monitoring and reporting systems (console)



THE BEST-RUN BUSINESSES RUN SAP

IDS – Host Sensor

Host-based IDS sensors monitor the local system for changes and unusual behavior by observing log files, system processes and resource consumption. They run as a background system on the monitored system and will send an alert to the console, for instance, in the case of unsuccessful login attempts.

Pros

- Can provide checks for system and/or data integrity
- Ability to monitor encrypted communications
- No limitations due to network layout (switched networks, ...)
- Platform dependent interpretation of data

Cons

- Can only partly monitor the network stack
- Can be compromised by attacking the OS or the IDS system itself

IDS – Network Sensor

Network-based IDS sensors monitor the network traffic between different systems searching for specific patterns in this traffic, identifying known attacks or searching for unusual usage patterns in this traffic. They run on separate hardware (network sniffer) or are integrated in certain routers or switches and will send an alert to the console, for instance, in the case of a port scan being detected.

Pros

- Can detect ‘network-based attacks’
- Can analyze raw network data
- Can’t be detected or attacked easily by an attacker

Cons

- Needs constant maintenance of signatures
- More ‘false positives’
- Can’t analyze encrypted traffic

Agenda

Security Threats

Technical Security Safeguards

- Firewalls
- Application Gateways
- Intrusion Detection Systems
- Cryptography

Applying Infrastructure Protection

- Example setup for SAP WebAS

Defense in Depth

Summary

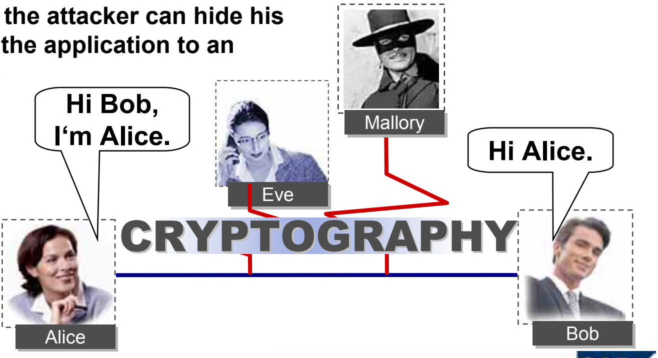
Cryptography

Cryptography can provide safeguards against different threads, depending on how it is used:

- **eavesdropping <-> encryption**
- **masquerading <-> authentication**
- **repudiation <-> digital signatures**

Protection provided by cryptography may also be abused !

- **Using SSL/SNC the attacker can hide his attacks against the application to an IDS or Firewalls**



Agenda

Security Threats

Technical Security Safeguards

- Firewalls
- Application Gateways
- Intrusion Detection Systems
- Cryptography

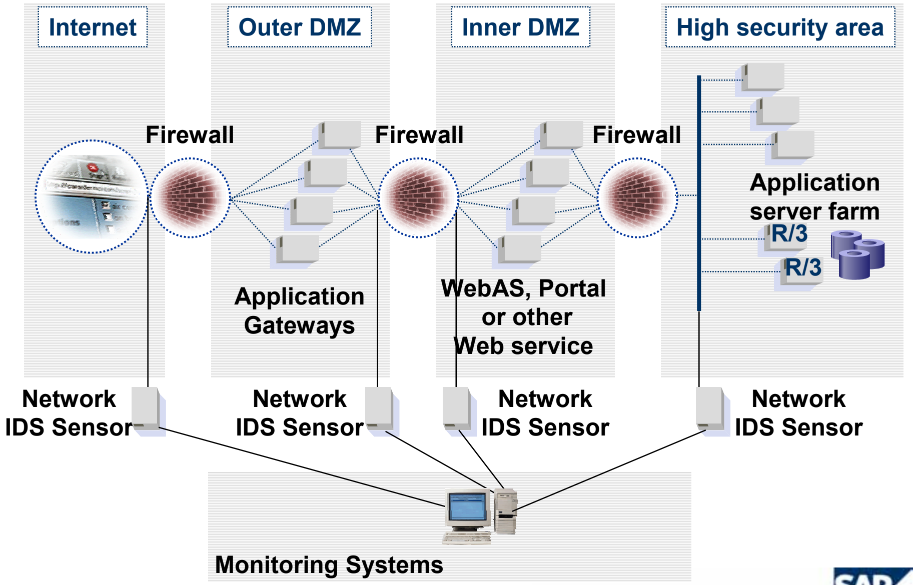
Applying Infrastructure Protection

- Example setup for SAP WebAS

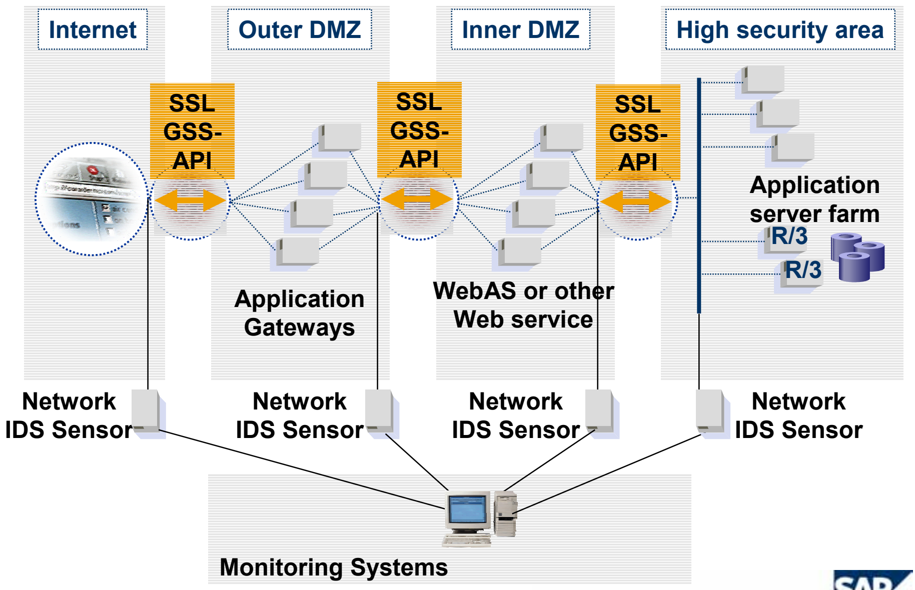
Defense in Depth

Summary

Secure Network Topology



Secure Network Topology with Encryption



Internet

Outer DMZ

Inner DMZ

High security area

SSL GSS-API

SSL GSS-API

SSL GSS-API

Application Gateways

WebAS or other Web service

Application server farm

R/3

R/3

Network IDS Sensor

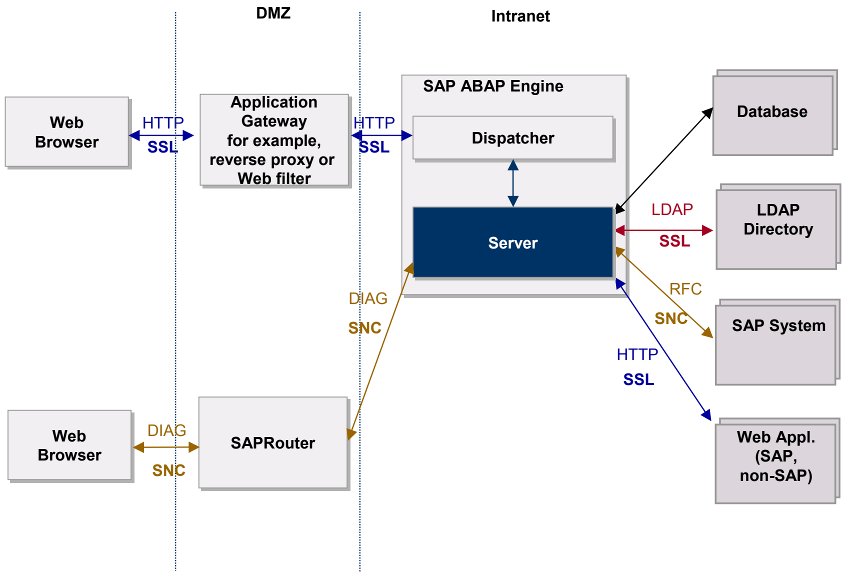
Network IDS Sensor

Network IDS Sensor

Network IDS Sensor

Monitoring Systems

ABAP Engine Protocols Overview



DMZ

Intranet

Web Browser

HTTP SSL

Application Gateway for example, reverse proxy or Web filter

HTTP SSL

SAP ABAP Engine

Dispatcher

Server

Database

LDAP SSL

LDAP Directory

RFC SNC

SAP System

HTTP SSL

Web Appl. (SAP, non-SAP)

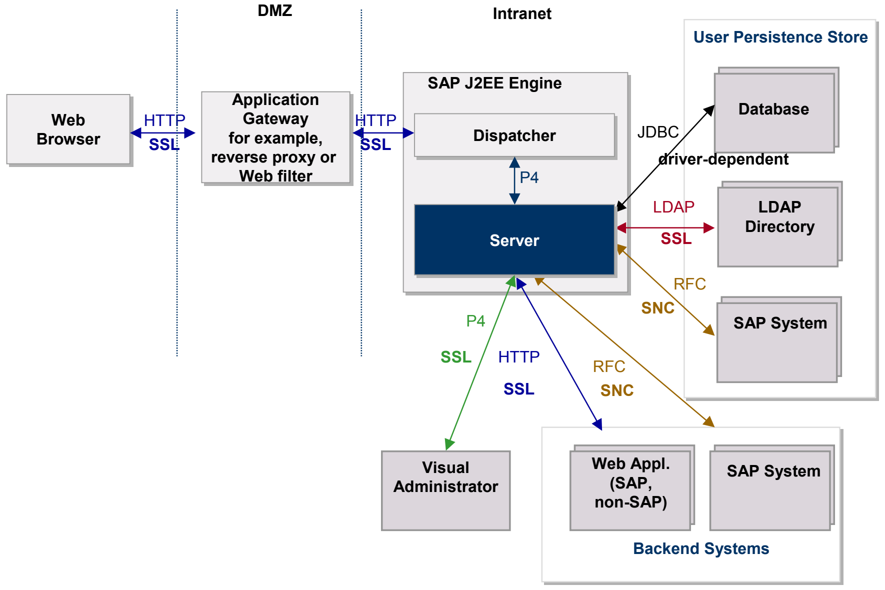
DIAG SNC

Web Browser

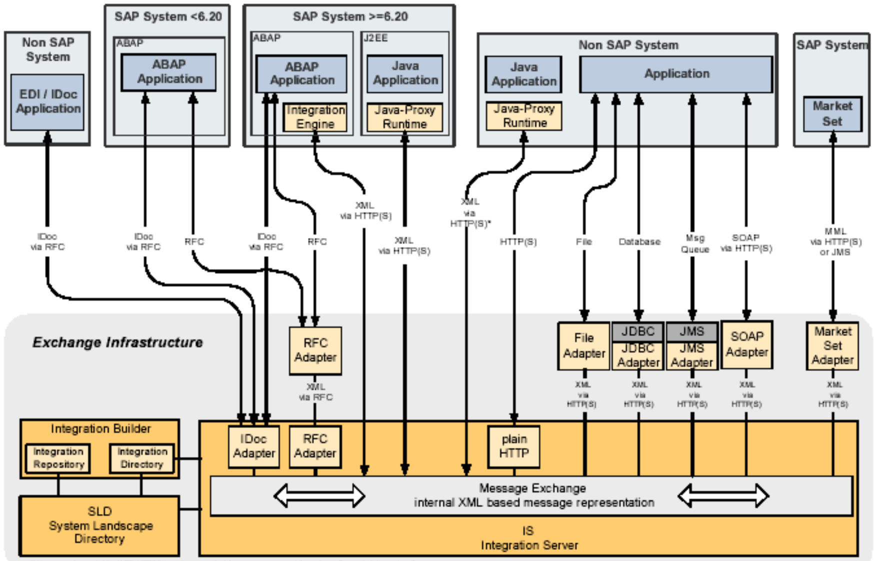
DIAG SNC

SAPRouter

J2EE Engine Protocols Overview

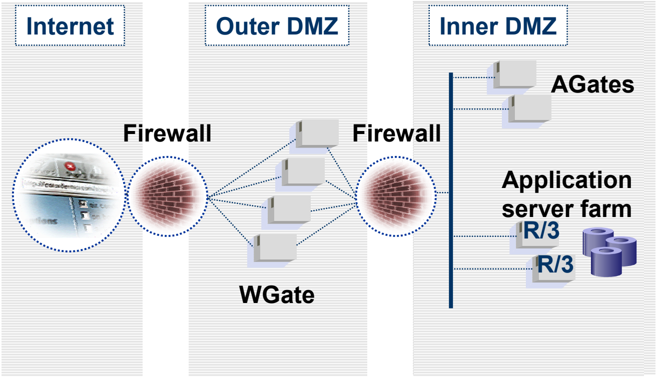


XI Infrastructure



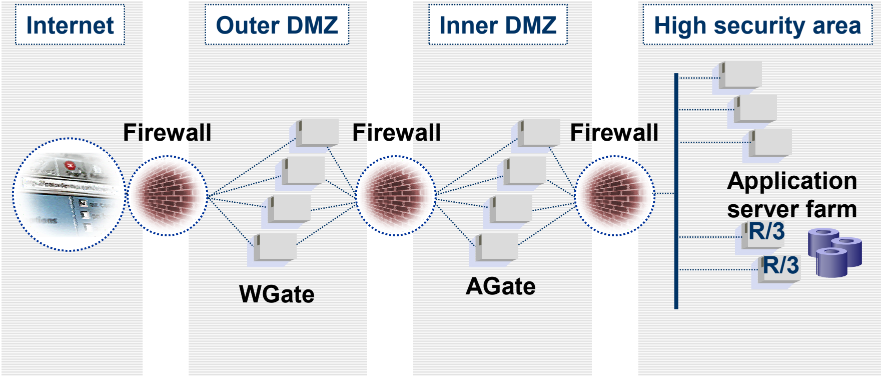
*When running outside J2EE, HTTPS is only supported for messages sent from Java-Proxy to Integration Server.

Other Setups – ITS 2-level



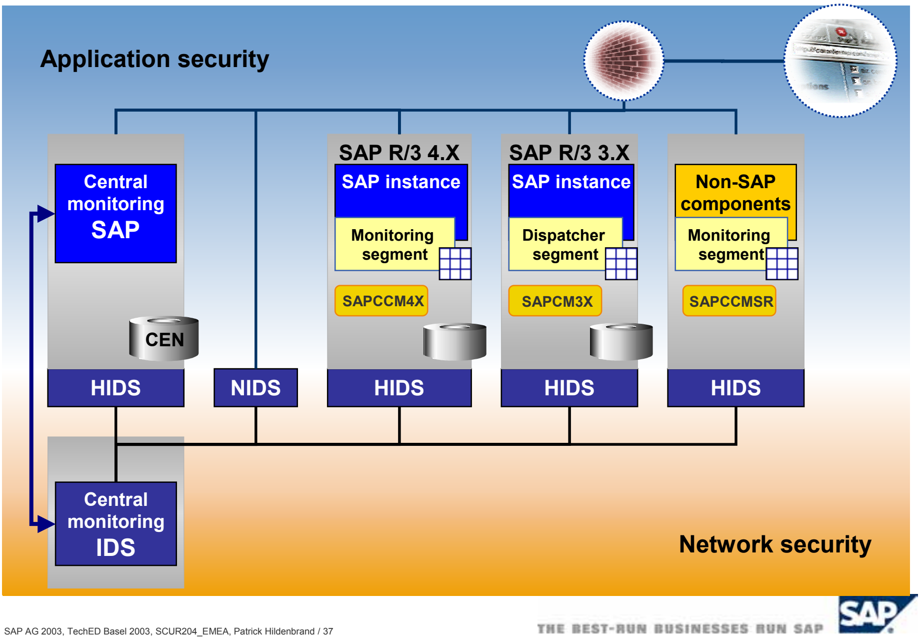
© SAP AG 2003, TechED Basel 2003, SCUR204_EMEA, Patrick Hildenbrand / 35

Other Setups – ITS 3-level



© SAP AG 2003, TechED Basel 2003, SCUR204_EMEA, Patrick Hildenbrand / 36

Connecting SAP Software to Intrusion Detection Systems



Agenda

Security Threats

Technical Security Safeguards

- Firewalls
- Application Gateways
- Intrusion Detection Systems
- Cryptography

Applying Infrastructure Protection

- Example setup for SAP WebAS

Defense in Depth

Summary

Defense in Depth

No system can be made 100% secure due to

- Human errors
  - In development
  - During configuration
  - During operations
- Make a system as secure as possible will cost to much

➡ "Defense in Multiple Places" or

Defence in Depth

Reasons for Defense in Depth

Example: Application of patches in the wrong order result in unprotected Web server

- Using an application gateway to protect the Web server you can shield it against most HTTP-based attacks

Example: New bug found in the Web server software and the system can't be upgraded due to dependent installations

- Using an application gateway may be able to block access to the resource showing the bug, thus giving you the time required to fix the system

Example: Due to an oversight, the administration port of an application is open and the password is still the default

- As the port has not been requested to be opened on the firewall, the port can't be accessed from the Internet

Agenda

Security Threats

Technical Security Safeguards

- Firewalls
- Application Gateways
- Intrusion Detection Systems
- Cryptography

Applying Infrastructure Protection

- Example setup for SAP WebAS

Defense in Depth

Summary

Summary

You are now able to

- List security goals, threats, and safeguards
- Categorize security measures
- List the necessary steps towards establishing a secure system environment
- Select appropriate security measures depending on your application requirements

Further Information

➔ Public Web:

www.sap.com/netweaver ➔ Key Capabilities ➔ Security SAP

SAP Customer Services Network: www.sap.com/services/

➔ Consulting Contact

Frank Rambo, SAP Security Consulting (frank.rambo@sap.com)

➔ Related SAP Education Training Opportunities

http://www.sap.com/education/

ADM960, Security in SAP System Environment

ADM950, Secure SAP System Management

➔ Related Workshops/Lectures at SAP TechEd 2003

SCUR251 Eliminating Authentication Pop-Ups in SAP Landscapes,
October 2nd 14:00 – 16:00, Room H10, Hands-On Session

SCUR351 Simplifying User Administration in Heterogeneous Landscapes,
October 2nd 9:00 – 13:00, Room H10, Hands-On Session

Questions?

Q&A

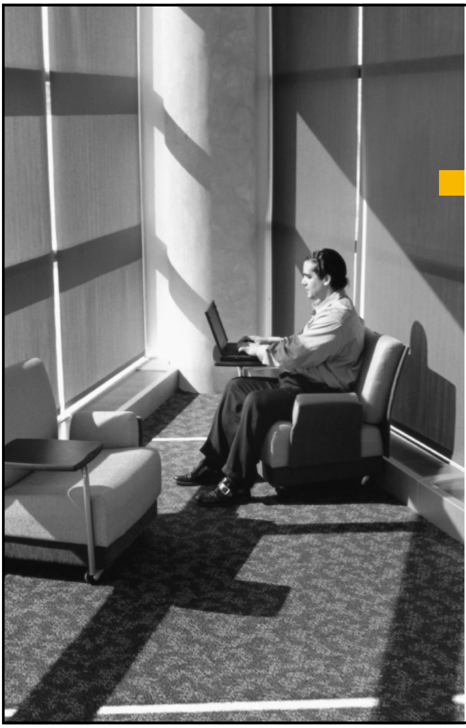
Feedback

Please complete your session evaluation and drop it in the box on your way out.

Thank You !

The SAP TechEd ’03 Basel Team

Copyright 2003 SAP AG. All Rights Reserved



SAP TechEd `03 EMEA Online

WATCH THE REPLAYS, DOWNLOAD THE SLIDES, AND READ THE TRANSCRIPTS.

www.sap.com/community