



APPENDIX.D2.6

System Sikkerhet IDS proposal



INTERIM AGREEMENT

BETWEEN

GNR

AND

SYSTEM SIKKERHET

Table of Contents

1 PURPOSE.....1

2 IDS-SERVICE - EXPERIENCE AND FOCUS1

3 ESTABLISHMENT2

4 PLAN OF ACCOMPLISHMENT2

5 PRICING3

Travel expenses.....3

Invoice, payment and advance payment4

ATTACHMENT 1: SPECIFICATION OF THE PILOT SERVICE5

ATTACHMENT 2: SPECIFICATION OF NORMAL OPERATION OF THE IDS SUPPORT
SERVICE6

ATTACHMENT 3: IRT – INCIDENT RESPONSE TEAM8

ATTACHMENT 4: SECURITY TESTING.....10

ATTACHMENT 5: SECURITY HARDENING12

ATTACHMENT 6: SECURITY INFORMATION13

ATTACHMENT 7: TELEPHONE SERVICE14

ATTACHMENT 8: 7/24 SERVICE15



1 PURPOSE

The purpose of this agreement is to:

1. assist GNR in planning and clarifying the commencement and the extent of the pilot IDS service. The details and the extent of the support service, which means the normal running of the IDS service, should be clarified during the pilot phase. From the time the IDS-equipment is installed, the daily¹ analyse of the traffic will be performed and notified to GNR as a part of the pilot phase in parallel with the final tuning of the service
2. transfer the pilot service to the normal running of the IDS service, i.e. the pilot service enters into the operative phase of the support service. The suggested service include daily² analyse of the traffic and reporting as detailed in the pilot phase
3. assist GNR to build up and detail an IRT (Incident Response Team), OPTIONAL
4. assist GNR to test the security of the network, services and applications, OPTIONAL
5. assist GNR with a consulting service related to the competence and experience with security in the technical architecture to security harden the network, OS and applications, OPTIONAL
6. assist GNR by mail or similar to a continuous updating of relevant security information (threats, trends, weaknesses etc.) related to the set-up and the configuration of the OS, applications, security patches etc., OPTIONAL
7. assist GNR with a telephone service outside of office hours, if desired including assistance by turn-out, OPTIONAL
8. 24/7 service, OPTIONAL.

Several of these areas of assistance may be started simultaneously, such as items 1, 3, 4, 5 and 6, while items 2 and 8 should typically wait until the IDS service is incorporated in GNR's organisation.

For further information and details of the various areas of assistance, see attachments numbered as per item numbers above.

2 IDS-SERVICE - EXPERIENCE AND FOCUS

In order to perform an IDS-service, it is essential to have knowledge about weaknesses in operating systems, applications and protocols, which can be used by external intruders/-hackers or disloyal employees. In addition, the use of tools and methods to perform these kind of unwanted and hostile actions change and evolve continuously. Considerable and continuous efforts have to be used in order to keep updated knowledge in these matters. The rapid technological development further makes this a challenge.

System Sikkerhet makes use of considerable resources in order to keep up to date the knowledge about IT and Internet security, and takes active part in this nationally.

1 ½ years experience with performing the IDS-service for several customers has given System Sikkerhet good knowledge about what is crucial for succeeding with this service. One major factor is the human resources and knowledge. All commercial IDS-tools suffer

¹ With daily means every normal working day.

² With daily means every normal working day.



from weaknesses in connection with false positives and negatives, which means that the tools give a great potential in false alarms. Traffic looking like unwanted and aggressive traffic shows up to be perfectly normal traffic, and traffic looking normal can hide malicious and evil traffic. Due to this it is crucial for succeeding that the IDS-tools are combined with human analysis and continually adapting the IDS service with knowledge to understanding of the network and the architecture and available services for each customer. Further, the IDS-service requires continuity in work, which include that the organisation is able to handle an operative service even with seek-leaves, holidays and the overall turn over in the IT-business.

In order to minimize this challenge, System Sikkerhet can offer GNR to perform the daily analyse of traffic and tuning of the IDS-system, leaving GNR to make the necessary decisions based on the information and analyse from the IDS-service.

Few IDS-tools has built in functions for anomaly based IDS, functions which makes it possible to filter normal traffic through reduction of data in a way that leaves only the remaining traffic for human analysis. Most IDS-tools are based on signatures (like virus-detection tools), which recognise typical traffic-patterns and reports alarms based on this. The disadvantage with this kind of approach, is that the IDS-tools never get better than the signatures, and the tools very often gives limitations with regards to how thorough and deep the traffic information can be analysed.

Due to this, System Sikkerhet has developed a method for anomaly based IDS-services, which is included in our IDS-services. This is based on use of databases. The method gives an important complement to signature based analysis and contributes to reduce the probability for false alarms. Further, this IDS-service contributes in discovering errors in network configurations as well as detects new and unknown attacks patterns.

Our experience is that an incident detected at one customer, often also is detected at others. An IDS-service performed by a professional vendor with a broad spectre of customer will give synergies for each customer like early detection and early actions.

3 ESTABLISHMENT

The project is suggested to be started by December 1st 2000.

4 PLAN OF ACCOMPLISHMENT

The plan of the accomplishment of the IDS project is as follows:

- The pilot phase begins December 1st 2000 and goes on until February 31st 2001.
- The operative phase begins March 1st 2001 and goes on until February 28st 2003, and may be further extended by variation order.
- The need for assistance outside the IDS support service will be clarified as the project goes along.

For details with regards to the pilot phase and the operative phase, see attachments 1 and 2.



It is recommended that the beginning of phase 1, the more technical part of the IDS, also phase 4 is started, which is forming the Incident Response Team, see attachments 4 for more details.

The pilot phase will clarify any need for and extent of other assistance, such as security hardening, security information, testing, IRT, preparedness, see items 3 to 8 in chapter 1, as well as the attachments.

5 PRICING

The costs for the IDS support service, see items 1 and 2 of chapter 1, based on the use of 3 sensors:

IDS service per month, 0800-1600, excluding the technical solution **EURO 30.700**

alternatively:

IDS service per quarter (3 months), 0800-1600, excluding the technical solution - by prepayment (amounting to Euro 29.000 per month) **EURO 87.000**

An increase in the number of sensors within the same use of console and data base will increase the extent of the agreement by 5 – 9% (excluding the technical solution) and will depend on the number of additional sensors.

Hourly assistance with regards to the handling of incidents will be carried out at an hourly rate of EURO 190.

Assistance with regards to the OPTIONAL requirements will be invoiced at an hourly rate of EURO 190, unless otherwise agreed.

The assistance is for the time being not subject to VAT. Changes will inflict on the prices.

Travel expenses

Travel expenses are additional to the rates stated above, and will be charged as follows:

- travel expenses according to the Norwegian standard travel regulation rates
- travels within normal working hours will be invoices at 50% of the hourly rate
- travels outside of normal working hours will not be invoiced.

Travels will not be made unless GNR accepts them on beforehand.



Invoice, payment and advance payment

The IDS service as per items 1 and 2 in chapter 1 may be invoiced in arrears if monthly, or in advance if quarterly.

Hourly assignments will be invoiced biweekly according to attached time sheets.

Payment terms are net pr. 30 days from invoice. The date of invoice shall be in accordance with the date when invoice is sent.

Monthly payments and hourly rates can be altered under the following conditions:

- Change in governmental regulations causing an increase/change of taxes in connection with the agreed services which are not covered in the agreement

Information of price increase must be submitted in writing at least 2 -two- months before they become effective.

On behalf of GNR

On behalf of System Sikkerhet AS

.....

Client

.....

Contractor



ATTACHMENT 1: SPECIFICATION OF THE PILOT SERVICE

The purpose with IDS is to discover and prevent attacks on GNR network. The service is based on detecting traffic on selective network segments.

The pilot phase will include specifying and implementing the IDS-system, as well as traffic analysis from the time the system is installed.

This should include a planning of equipment to be used for the IDS. In addition, identification and definitions of type of incidents should be made based on the security policy at GNR.

The pilot phase will be necessary to clarify and take into consideration relevant approaches, such as:

- a discussion of the network and the network structure
- the rules and policy for fire walls
- the Internet policy, connections and legal/undesirable traffic
- the configuration of the services
- the security policy for the use of services
- the information from any previous risk analysis, vulnerability assessment and/or security test and revision
- the information from any previous breach of security
- the need for back up of the log data.
- Agree upon necessary technical contact person(s) in order to
 - discuss what kind of events to consider for reporting, i.e. criteria to be used in order to detect abnormal behaviour
 - inform us about changes in GNR normal services

From the time the IDS-equipment is installed, the traffic analysis will be performed in parallel with the tuning and defining of what is the relevant traffic/incident GNR will be informed and alarmed about.

Details in connection with warning procedures for the various incidents should be defined. The following is recommended:

- For Red incidents: representatives from management must be available, as incidents are business critical (TBD)
- For Orange incidents: representatives from service provision and management of technical services
- For Yellow incidents: system and network administrators, as well as security department

By the end of pilot phase, suggested for three months, the IDS-service could be turned over in a permanent IDS-service, ref attachment 2.



ATTACHMENT 2: SPECIFICATION OF NORMAL OPERATION OF THE IDS SUPPORT SERVICE

Intrusion detection systems description

The details for the normal operation of the IDS service will be specified during the pilot phase, ref attachment 1.

Changes in the need of sensors will affect the total expenses of the service with 4-9% of the given rates for each new sensor, depending on where the sensor is placed, type of sensor (host or network based), level of traffic, documentation, response. In addition to the direct cost of equipment and licences needed.

Intrusion detection is performed and with adequate number of sensor devices, as well as sampling of data from other sources, such as servers and network devices. The following issues will as a minimum be decided upon during the pilot phase:

- Notification time for incidents that are candidates for yellow severity class will be alerted within 48 hours
- Notification time for incidents that are candidates for orange severity class will be alerted within 12 hours
- Notification time for incidents that are candidates for red severity class will be alerted within 6 hours
- Notification of newly discovered vulnerabilities relevant for computer systems in use at GNR.
- Incident handling will depend on the causes for incidents:
- Internal incidents will be handled maximum 4 hours from notification
- External incidents will be handled maximum 2 hours from notification
- Normal traffic pattern model and intrusion detection monitoring profile will be updated on a weekly basis.
- Final classification of incidents are the responsibility of the GNR Incident Response Team Manager
- Alerts, Weekly and Monthly reports. Status reports 4 times a year.
- Monthly port scans to detect and verify changes to service provision, intrusion detection and monitoring profiles.

Changes in the need of sensors will affect the total expenses of the service with 4-9% of the given rates for each new sensor, depending on where the sensor is placed, type of sensor (host or network based), level of traffic, documentation, response. In addition to the direct cost of equipment and licences needed.

Incident response and Incident severity escalation procedures



It is important to include the correct level of management and decision makers for incidents:

- For Red incidents: representatives from management must be available, as incidents are business critical
- For Orange incidents: representatives from service provision and management of technical services
- For Yellow incidents: system and network administrators, as well as security department

As this is an escalation procedure, representation is additive as severity increases. For further handling of the incidents, see attachment 3.



ATTACHMENT 3: IRT – INCIDENT RESPONSE TEAM

Background

System Sikkerhet has based the development of an Incident Response Team on the all over accepted standards and templates available. The information on this topic is drawn from CERT, AUCERT and FIRST, among others.

There are several national and international sources describing the organising and the requirements to how an IRT should be constructed and function. This information has been used when System Sikkerhet has gathered the expertise now used for this kind of assignments.

Competence

System Sikkerhet has built up a team specifically in charge following up and assure the quality of all IRT projects. The team is also in charge of following up both national and international trends in this area. Furthermore, the team should continuously develop and improve the product. In addition, the team will provide the Client with essential information and instructions to ensure the best possible capability of the team to respond to the incidents.

Establishing an IRT

System Sikkerhet can offer the Client:

- to swiftly set up a framework of how an IRT should be organised, and describe and develop the master guidelines and processes.
- to exploit System Sikkerhet's broad experience and expertise actively in the process of developing an operative IRT.
- to prompt, and to act as a catalyst in the establishment of an IRT, so that the project's milestones will be met, as well as provide the required quality assurance of the work.
- to advise how to secure evidence/tracks while complying with legal requirements and requirements to the protection of privacy.
- to ensure that requirements to security and confidentiality are implemented in the IRT.
- to perform tests/alertness rehearsals to train the members of the team.
- to assist the IRT with help and guidance during the start-up phase.
- to supply the information and training to improve the understanding and the competence in the Client's organisation.
- to assist in establishing contact with similar organisations.

International networks - FIRST (Forum of Incident Response and Security Teams)

The organisation consists of IRTs from both public and private sectors. The participants are mainly from the USA, although several European countries are represented (Germany, Denmark, United Kingdom, Italy, Spain, Norway). It is at the discretion of each organisation to apply for membership in FIRST. A majority of 2/3 of FIRST's steering group is necessary to become a full member, as well as a sponsor who will vouch for that one follows the requirements and standards with regards to routines and requirements to security and confidentiality.

Establishing an IRT for GNR



A preliminary IRT for Nameplanet should be within the range of 150 hours. To carry out the project, some assistance by the Client will be required. This may be questions and reading of documents prepared by System Sikkerhet relating to knowledge to the organisation and existing routines.



ATTACHMENT 4: SECURITY TESTING

The following security testing may be carried out:

1. External security testing of Internet connections
2. External security testing of other connections
3. Testing of applications, typically testing of a web server
4. Internal security testing
5. Testing of alertness.

Items 1 to 4 will test whether unauthorised users (external and/or internal) manage to access through the security barriers in place, or whether the security barriers are configured satisfactorily. During the testing, an unauthorised user will try to acquire privileges or block services.

The first part of the attack will typically consist of a port scanning. To obtain this, tools such as Nmap, NSlookup and Netcap will be used. Furthermore, standard programs such as Telnet and FTP will be used to clarify which services and versions are available as a part of the port scanning.

Knowledge about weaknesses, exploits and security holes for operating systems, security barriers and applications is used during the testing. Ready-made programs that may perform Denial of Service attacks and give access to the root directory will be used for the attack itself. In addition, System Sikkerhet's database with exploits and tools will be used.

The purpose of alertness testing is to verify whether the organisation responsible for firewalls and networks has the necessary security to withstand penetration or attempted penetrations from the Internet. An alertness testing will begin with a cautious port scanning increasing in intensity over a few days, to enter into a direct attack where weaknesses or holes will be tried.

The costs of a security test will vary from EURO 12.000 to EURO 35.000, depending on what and how much should be tested. This must be agreed for each test.

The availability of the Client for any questions arising or clarifications needed is expected.

Security testing procedures

Performance of security testing of IP services exposed to the Internet 4 times a year to control the enforcement of the firewall/router management and access restriction as well as vulnerabilities in customer services. The reports will contain:

- IP number
- IP service(s)
- Port number(s)
- IP service description
- Vulnerability status
- Corrective measures



The report will also contain a management level summary, as well as recommendation regarding other measures required such as procedural or organisational actions.




ATTACHMENT 5: SECURITY HARDENING

Security hardening entails a discussion and an assessment of the actual implemented solution in order to recommend improvements to the security and changes to the configuration. This will be based on System Sikkerhet's experience and competence, as well as a continuous follow-up on security patches, weaknesses and threats.

Time needed will typically be a couple of days per system/application and will be invoiced at an hourly rate unless otherwise agreed.

The availability of the Client for any questions arising or clarifications needed is expected.

	INTERIM AGREEMENT – Nameplanet and System Sikkerhet SS RAP/1126/AGREEMENT	Page 13 of 14 Date: 20-Sep-00
---	--	----------------------------------

ATTACHMENT 6: SECURITY INFORMATION

The Client may subscribe to this service, which will continuously offer an assessment of the at all times occurring incidents in the trade, as well as weaknesses and deficiencies in services and security patches, and what this will mean for the Client's specific solution. This provides the Client with an assessment of critical areas and a recommendation of critical alterations and updating with the latest security patches.


This service will have a monthly cost of about NOK 5.000 to 10.000, depending on the number of operative systems and applications subscribing to this information.



ATTACHMENT 7: TELEPHONE SERVICE

The Client may subscribe to the availability of competent personnel who may assist by turning out or by telephone support outside of office hours.

This is a new service, expected to be available at the end of August/beginning of September. Suggestions to a pricing structure will also be made by that time.

	INTERIM AGREEMENT – Nameplanet and System Sikkerhet SS RAP/1126/AGREEMENT	Page 15 of 14 Date: 20-Sep-00
---	--	----------------------------------

ATTACHMENT 8: 7/24 SERVICE

In the course of this autumn a round-the-clock service covering the examination and analysing of the log data with regards to the most critical incidents, will be offered. This will be in addition to the current log examination and analysis performed every morning working days.

This is a new service, expected to be available in the first quarter for 2001, subject to the market conditions, and it will be developed as a pilot project at on or several clients'.



APPENDIX.D.2.6.2

System-Sikkerhet IDS Presentation





**Offer to
The Global Name Registry
from System Sikkerhet
for an IDS system**



System Sikkerhet A/S

- **An Independent Consultancy**
- **Long experience – was founded 14 years ago**
- **Highly professional environment, in-depth knowledge – concentrates solely on information security**
 - Internet, protocols, OS, firewalls, Internet crime, security deficiencies related to the technology
 - Security w.r.t policy, IT, personnel, physical and document security
- **Consulting services**
- **Security testing**
- **Intrusion Detection Systems**
- **Good relations to the Norwegian Defence (ND), the Data Inspectorate and the Banking, Insurance and Securities Commission of Norway**
- **All personnel/Company has a military clearance SECRET (ND)**



System Sikkerhet A/S

- **Knowledgeable w.r.t rules and regulations**
 - Has assisted the Data Inspectorate in setting up rules and requirements
 - Has participated in preparing the new Data Security Guidelines
 - Assess the Data Security Guidelines w.r.t the Government, military infrastructure and tactical systems
- **Good relations to the Norwegian Defence and to the Data Inspectorate enable us to informally discuss solutions to security concepts.**
 - E.g. Possibility to define role function in tactical systems without logging on.
 - Finding solutions for the handling of sensitive personal information (approval by the Data Inspectorate)



Consulting

- **Vulnerability assessment**
- **Security revision**
- **Preparation of security architecture of networks and for e-business**
- **Security hardening of network/services**
- **Preparation of security policy and strategy**
- **Security evaluation of products**
- **Professional support w.r.t contractors/suppliers**
- **Consultancy w.r.t IDS and the forming of an Incident Response Team (IRT)**
- **Consultancy w.r.t certification, BS7799**
- **Consultancy w.r.t complying with the requirements of the Data Inspectorate**
- **Consultancy w.r.t challenges in complying with the requirements from the National Defence**
- **Assistance w.r.t the process of obtaining acceptance related to**
 - **Certification according to BS7799**
 - **The requirements of the Data Inspectorate**
 - **Classified information systems**
- **Security evaluation as a technical basis for acceptance/certification**

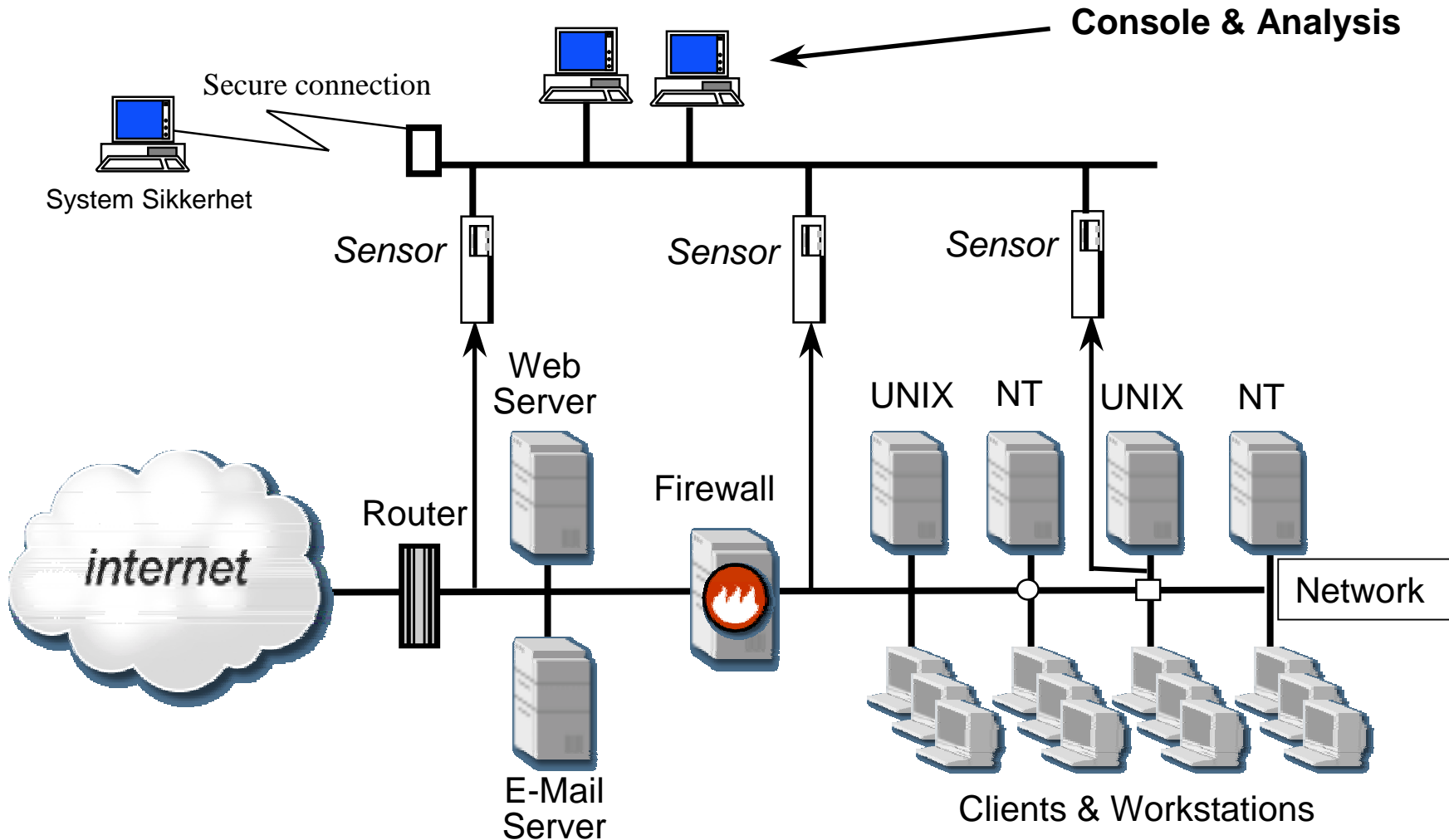


Categories of tests

- **External security test of the Internet connection**
- **External security test of other connections**
- **Internal security test**
- **Preparedness test**
- **Web and application test**



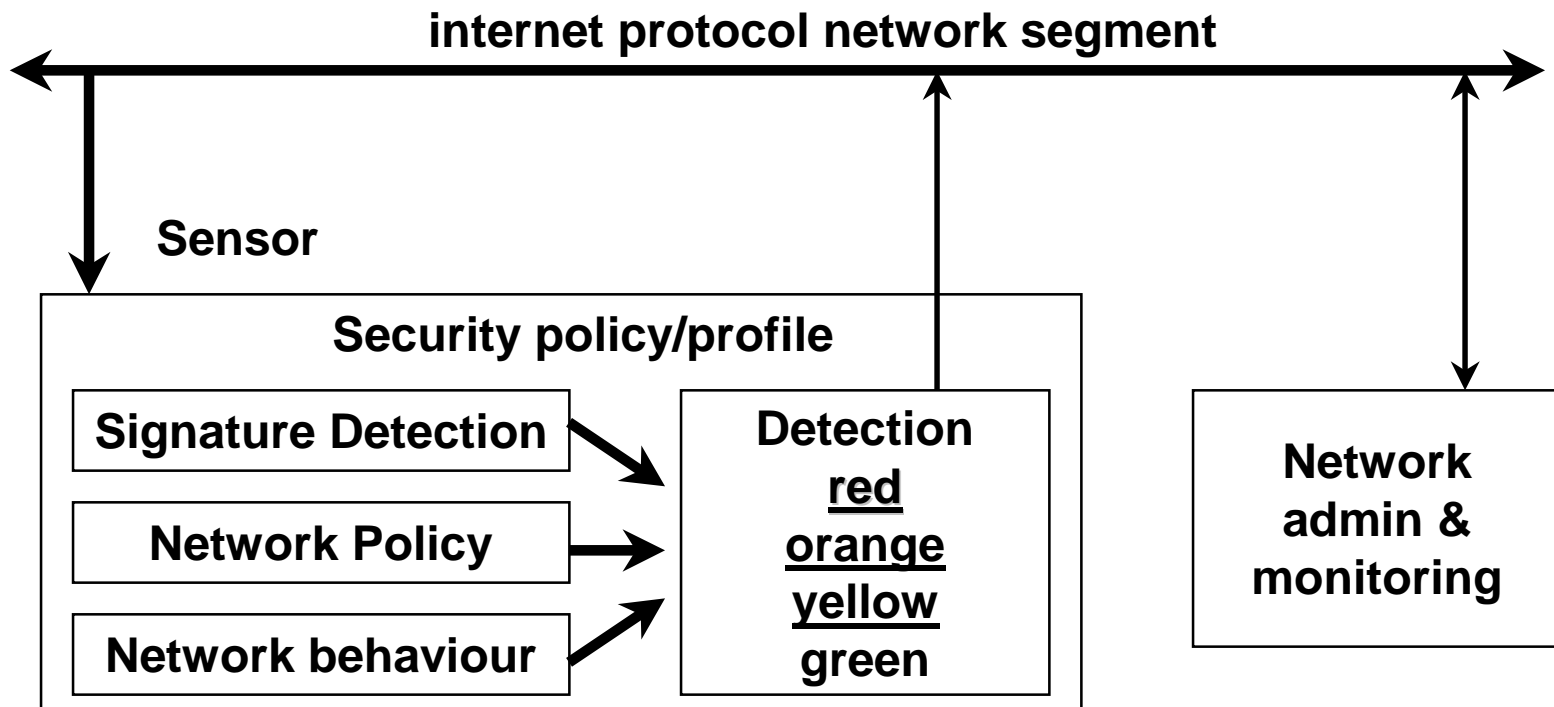
Intrusion Detection Systems (example)





Intrusion Detection System IDS

- “Intrusion detection and control”





Definitions

- **“False positive” is a false alarm**
- **“False negatives” are incidents which have not been discovered**
- **“Events of interest” – incidents/traffic we wish to evaluate/analyse**
- **Red, orange, yellow and green traffic/incidents**



WHAT DO WE DO?

We

- **monitor the traffic from known sources and keep these under surveillance**
- **co-ordinate the log results at the Client's with our own IDS review**
- **keep ourselves updated w.r.t new methods, vulnerabilities, exploits og "happenings"**
- **test new versions of IDS tools**

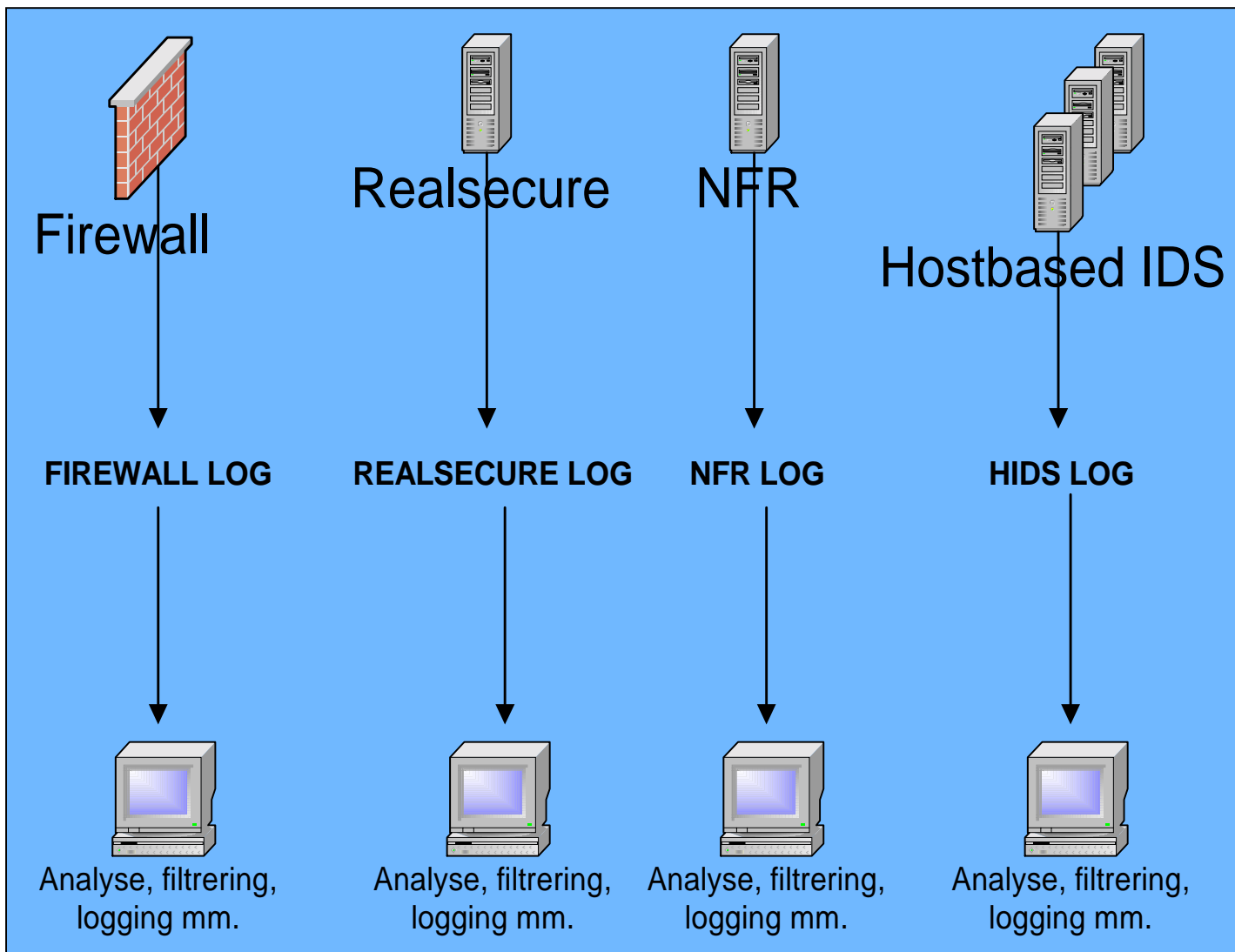


Actions during service

- **Logging of "Events Of Interest" (EOI)**
- **Categorising of EOI:**
Red, Orange, Yellow and Green traffic/incidents
- **Constant keeping-in-touch with Client IDS-Team**
- **Assistance with the handling of incidents**
- **Regular weekly, monthly and quarterly reports**
- **Contacting the ISP and CERT when undesired traffic is discovered**
- **monitor the traffic from known sources and keep these under surveillance**
- **keep ourselves updated w.r.t new methods, vulnerabilities, exploits og "happenings"**



Standard IDS



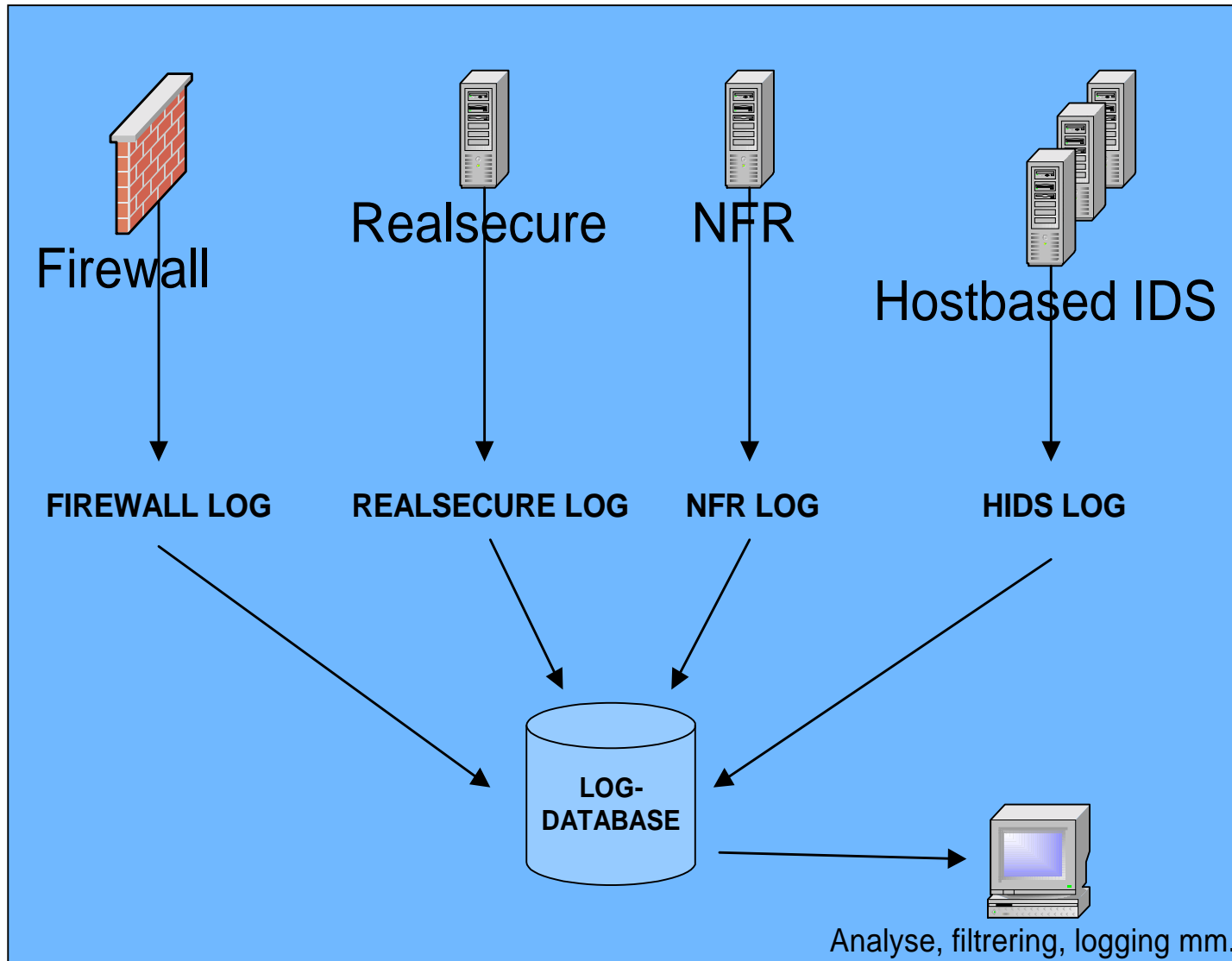


WHAT DO WE SEE?

- Innumerable scanning for accessible services
- Errors to the network configuration
- The use of standard tools. BO2K, NMAP, +++
- Slow scannings
- Attempts against simple services. Telnet, SSH, POP, +++
- Exploits
- WEB scannings and attempts against known vulnerabilities
- Activities by own employees and own operation and security personnel
- All traffic to and from the Client's network



System Sikkerhet - IDS





WHAT MORE DO WE SEE NOW?

- **Connection between our own and Client's data/attack/scannings**
- **More efficient log examination**
- **The entirety of the picture is understod much sooner**
- **More thorough analyses are made**
- **More noise is filtered**
- **Tests w.r.t new exploits i a laboratory environment**
- **Tests w.r.t new filter for the IDS**



Pilot phase

- **Security policy and strategy**
 - **Actions (firewalls, www, email, servers...)**
-
- **Mapping of the placing of sensitive information in the network and systems**
 - **Network topology and security measures**
 - **Assembling of basic data for the classification of traffic**
 - **Establishing an adaptive security strategy**
 - **Definition of the various incidents (Red, Orange, Yellow, Green)**



Operative phase

- **Periodical port scanning and mapping of network services**
 - Verifying that no *uncontrolled* changes to the network have taken place, also whether any changes have deteriorated the security
- **Daily log examination**
 - Searching for undesired activity and exploitation of vulnerabilities by means of logs from firewalls and IDS tools
- **Reporting of incidents**
 - Classification of incident (Red, Orange, Yellow)
 - Preventive measures
 - Warding off attacks and compromising conscious/unconscious)
 - Securing of evidence for further investigation and handling of incidents



Operative phase

- **Assistance to the Incident Response Team**
 - By compromising or attacks
- **Weekly and monthly reports**
 - A summing-up of the most significant incidents in the network, as well as a description of trends and potential threats.
- **Updating of security measures and policy**
 - Organisational measures
 - Technical measures

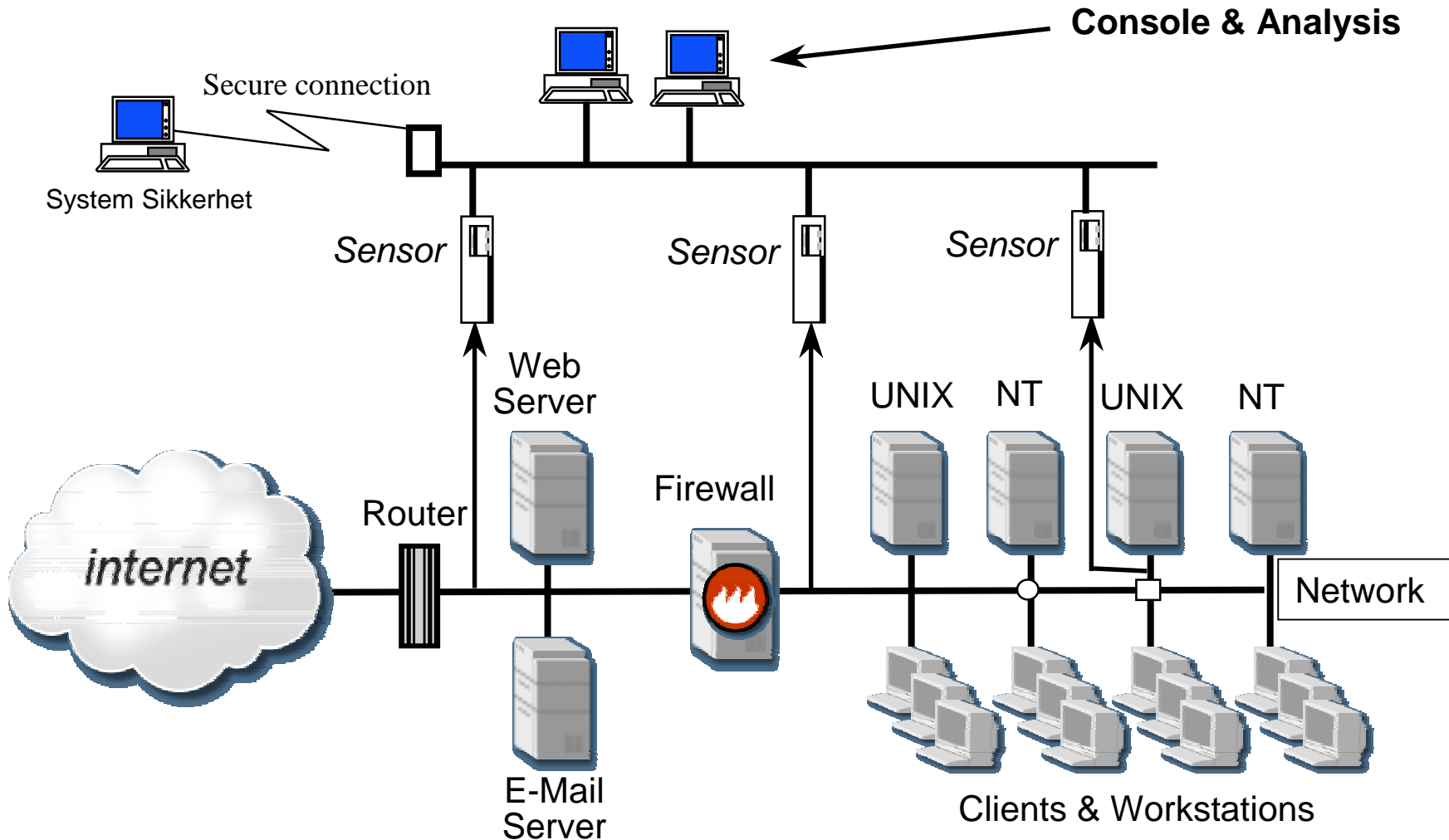


Operative phase

- **Preventive motive**
 - Knowledge about normal traffic
 - Knowledge about hackers and their motivation
 - To reveal attempts of port scanning
 - To use friendly attacks in order to reveal hostile attacks
 - » Eg. The mapping of a service may be the first phase in the exploitation of a vulnerability of the service
- **Active motive**
 - Discover well-meaning changes to the configuration which may compromise the security
 - Detect intrusions to and compromising of critical resources, as well as securing evidence for any legal actions



Intrusion Detection Systems (example)





Traditional Data Security

Vulnerability assessment

+ Security policy

+ Direct actions



**= Traditional communication
security**

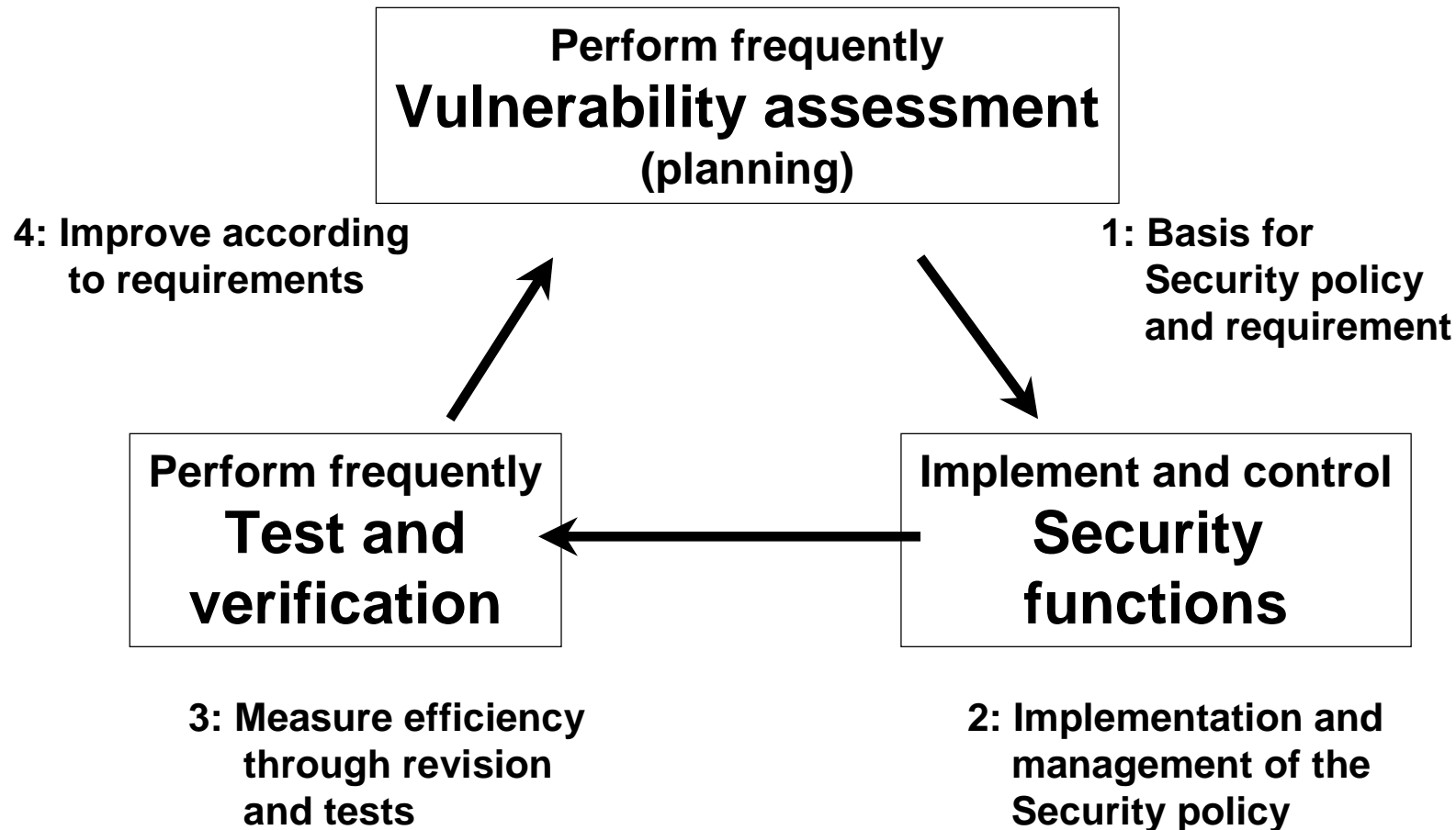
**Identification and authentication
Encryption
Access control (firewalls/usage)**

**Standardising and configuration control
Procedures and routines
System/Network revisions and
security testing**

**Properly implemented this should vouch for about 40-60% of the total
risk handling/security solution**



Efficient traditional Data Security





Adaptive Data Security

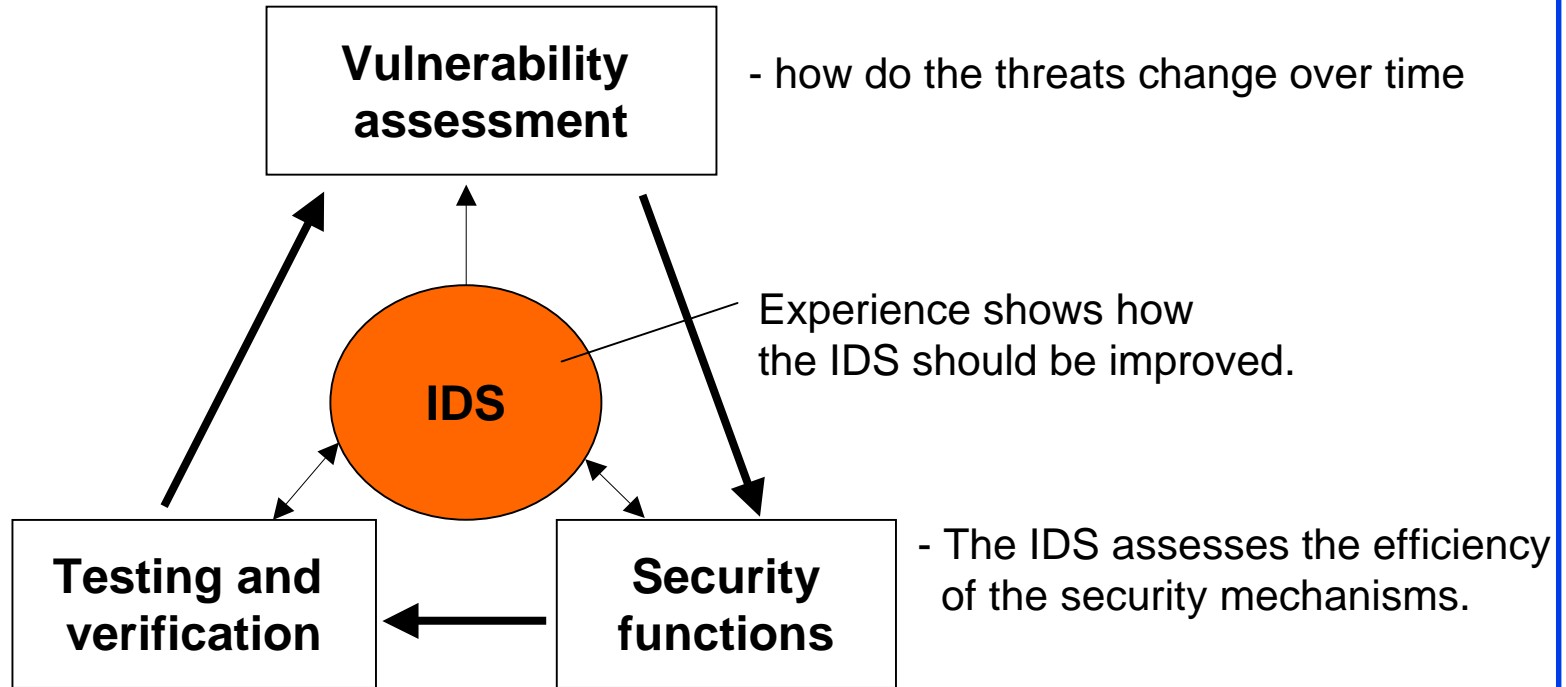
Traditional security

- + Threat/vulnerability surveillance → Threats, risks and prevention
 - + Threat/vulnerability detection → 'True time' surveillance
 - + Threat/vulnerability response → Prevention and/or tracing and evidence
(and investigation, police, as applicable)
-

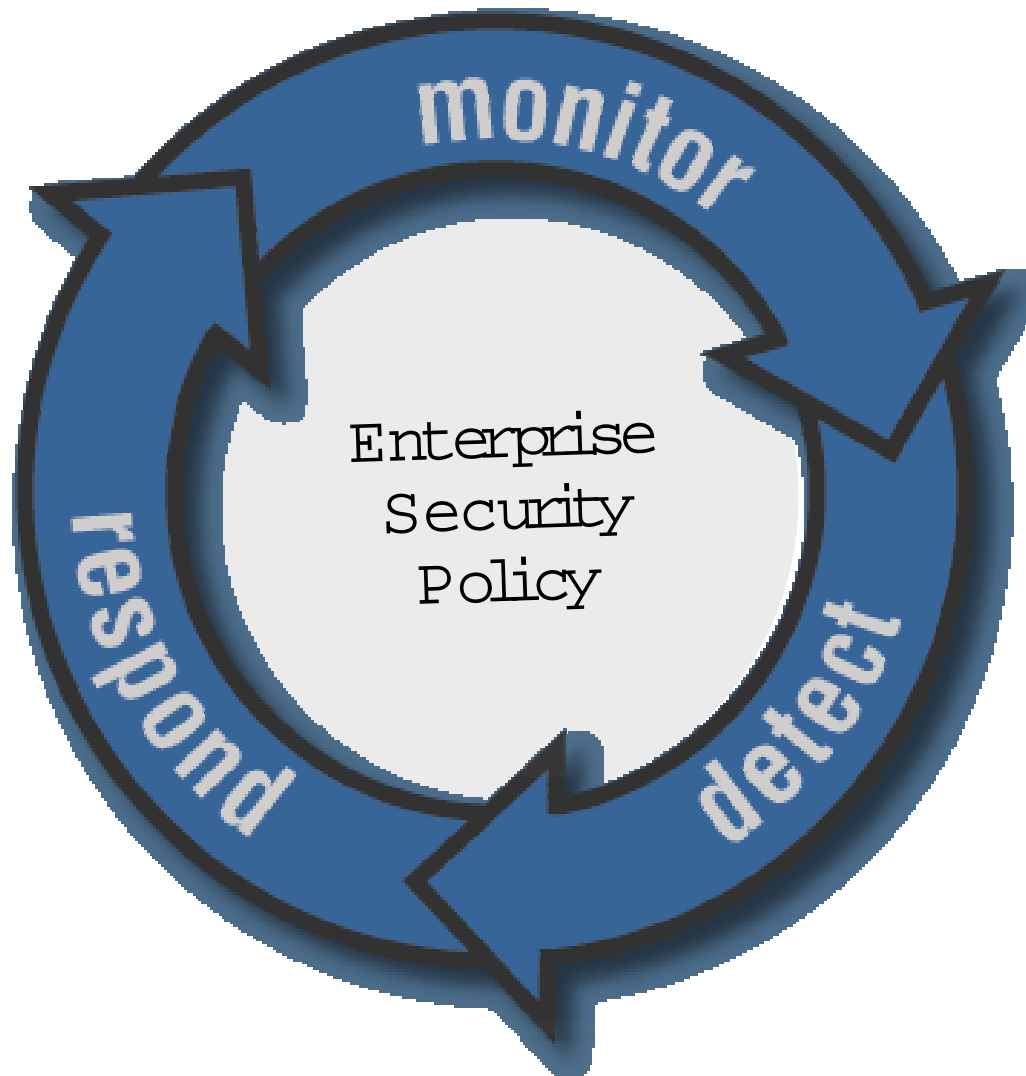
= *ADAPTIVE*
communication security



Adaptive security measures

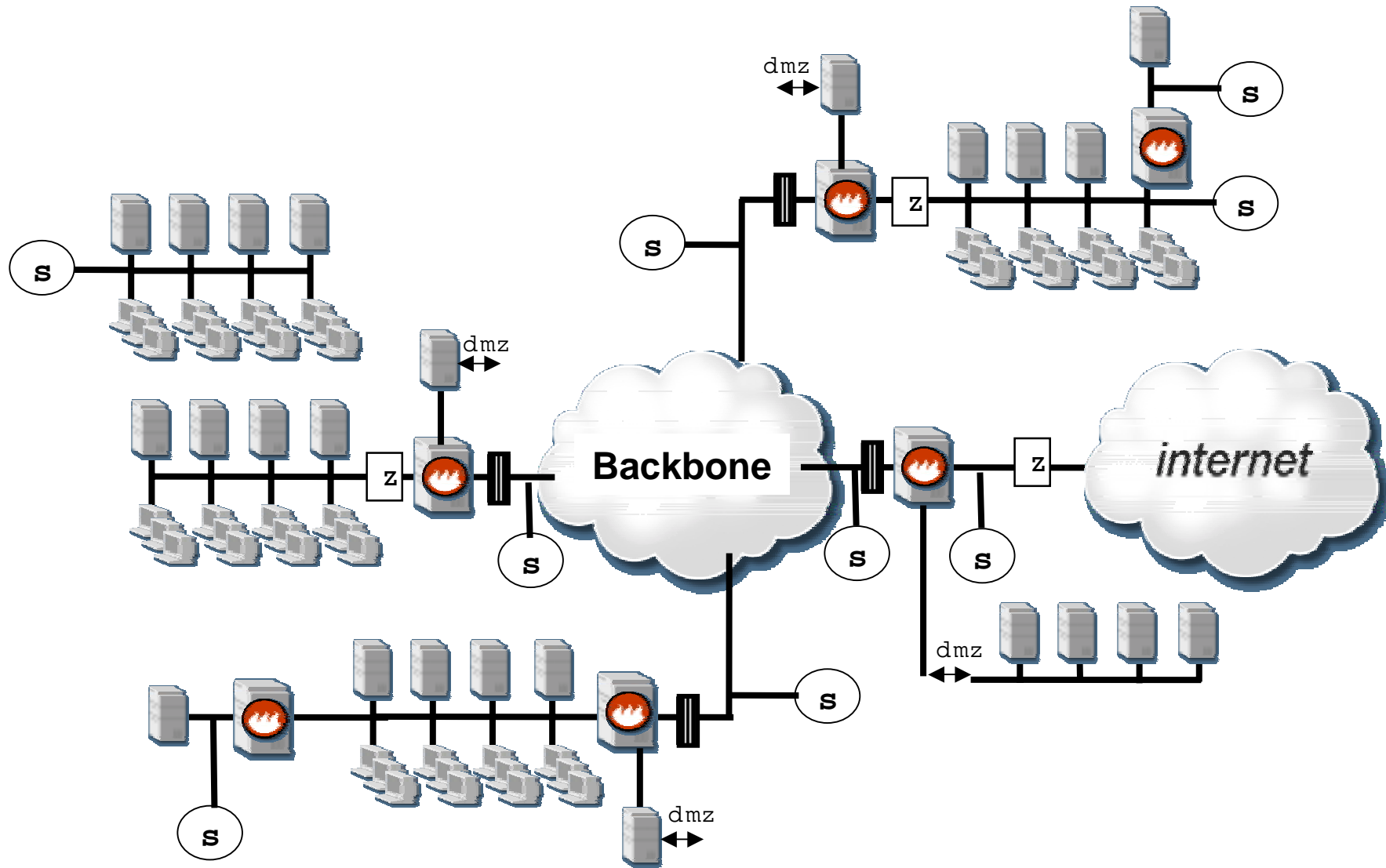


- The IDS makes the security **measurable**. Weaknesses in the implementation may be revealed sooner.





Internal Internet...





Host based IDS

- **What exactly is host based IDS?**
 - It is a **System Agent** installed on the host to be surveyed
 - It monitors system files and logs for any signs of undesired activity
- **Why is host based IDS useful**
 - Surveys what actually happens at the host
 - Provides an integration of system logs in the rest of the IDS
 - Simplifies the overall view of the extent of any damage



Host based IDS

- Why are host based IDS and network based IDS complementary?

NIDS	HIDS
Network perspective Transit traffic, clients, router access, switch access, ports/services, system independent	Server perspective System logs/activity, System configuration, System specific, console access
Anomaly/Signature	Signature
Early warning – 1st line	Successful intrusion and consequences – 2nd line
Passively listening - (Stealth mode) Unreachable to hackers	On host - more vulnerable to compromising (deletion, down time, alteration etc.)
Discovers attacks based on packet information	Discovers attacks based on log files and changes to these as well as to files, handles encrypted connections



Host based IDS

- Why are host based IDS and network based IDS complementary?

NIDS	HIDS
Cost effective – one sensor, traffic to/from several computers	More costly (in licence per server)
Important network segments	Business critical servers
Challenges related to band width and switched networks	Independent of band width and network technology
	Simplifies securing of evidence
No impact on performance (network, host, service)	May affect performance of service / host



Host based IDS

- **Sources**
 - Windows NT log
 - Unix system log
 - Can make user defined signatures based on text strings
 - » TCPwrapper, application logs
 - Can also log connection attempts against unused services
- **Incidents**
 - Unsuccessful events (files, change of password etc.)
 - Successful events (change of password, alterations of files, registry, registry, account policy shutdown, restart, root login, etc.)



Host based IDS

- **Challenges related to host based IDS**
 - **Server load**
 - » depends on the extent of the logging
 - » will be of maximum 1-2% with a little care and experience
 - **Active connection**
 - » two-way connection between IDS LAN and host
 - » requires consideration/security barriers so that:
 - the IDS service/traffic/user activities will not disturb the server
 - an incorrectly configured host may reduce the availability to the IDS LAN
 - **Requires synchronisation between**
 - new software versions on OS and sensor software
 - new signatures/upgrading with Client's operations personnel



Host based IDS

- **Status of the implementation**
 - Has been tested at our test laboratory during the summer
 - Will be implemented in a dedicated Web-server this week
 - Currently being tested at a pilot client, test net started in week 34
 - Stability tests at a pilot client's in a production copy net during weeks 38/39
 - Will be put into operation at Client's during weeks 39/40



Securing of the IT systems

- **Target : efficient reduction of risks**
- **Through : high resistibility**
- **The preferred method : The onion**
 - focuses on the crown jewels, i.e. the business critical servers, applications and clients
 - multiple security barriers - some soft and some hard
 - a combination of various security measures and products from different suppliers
 - one essential component/security measure: **HARDENING**
 - means that hardening should take place well within the net, not only in:
 - » the firewall and dmz servers



Securing of the IT systems

- **The traditional method : The egg:**
 - one hard shell - a firewall with a virus check against the Internet
 - "we trust our employees, at least the operations personnel" :-)
 - "we trust our partners"
 - a stressful weekday where the resources and the interest are enough to cover the latest software versions and availability
- **When the shell cracks, anything is possible**
 - the amount of existing weaknesses combined with the complexity of the systems will cause a crack



Hardening of data systems

- **Hardening, i.e. to increase the resistibility of the network equipment, servers and applications, examples**
 - Security concept/architecture
 - Filters (i routers and firewalls)
 - Configuration options in the OS or applications (e.g in NT registry or MIIS)
 - Correct services
 - Correct privileges (root privileges on applications)
 - Correct passwords (default password and password policies)
 - Correct patches
 - Correct versions



Hardening of the data systems

- **System Sikkerhet and hardening :**
 - Can contribute with competence into the organisation
 - » classification of information
 - » updated information
 - » adapted to the client's systems/architecture
 - » efficient measures which will not reduce performance /user-friendliness to any essential degree
 - Is consistently recommended as part of the implementation of the IDS
 - Can contribute by:
 - » advice, i.e. recommendations through discussions with technicians
 - » implementation
 - » verification by means of testing



The process of security work

- **Involve the management and key personnel**
- **Vulnerability analysis**
 - make use of interviews and discussions
 - Reveal the current status of the information security
 - Suggest measures based on risk - measures will be relevant to the importance and existing requirements
- **The analysis will be used as a process tool for the continuing work:**
 - E-business, BS7799