AMRES
Serbian Academic Network

BELGRADE SECURITY WORKSHOP 2015

ICT Security Architecture

Øivind Høiem

CISA, CRISC, ISO27001 Lead Implementer

Senior Advisor Information Security

UNINETT, the Norwegian NREN

GÉANT

About Øivind

About UNINETT

Corporate social responsibility
Transparency
Technology enthusiasm

The Norwegian HE Sector's Secretary for Information Security

What we do…

- Information Security Management Systems
- Policies, frameworks and methodologies
- Risk and vulnerability assessments
- Business impact assessments
- Continuity and disaster recovery plans
- Audits
- Templates and information material
- Information about the threat landscape
- Information security awareness
- Organize security conferences
- Security portal and blog
- International cooperation

Document goal

The goal of this Campus Best Practice-document is to serve as a guide for the implementation of ICT security architecture that will enable HE organizations to appropriately protect their information

Content in the document

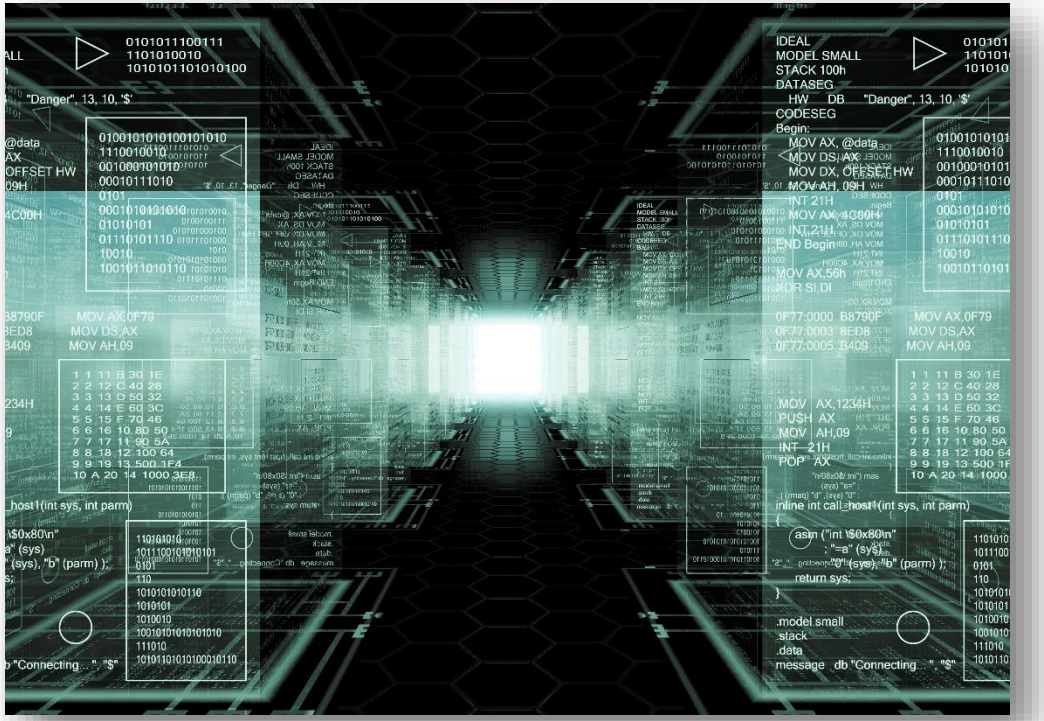
- Overall requirements
- The security architecture
- Authentication and access control
- The services and systems in the zoned network
- Definitions and references

Overall requirements

- Adequate protection of information assets
- Information security policy
- Regulatory requirements and directives
- The institution’s objectives
- Agreements with third parties
- Appropriate capacity
- Robustness in the event of failure
- Quality

Security architecture principles

- The network must be subdivided into zones and security classes
- Separation between servers and clients
- Servers and clients must be placed in relevant security classes based on risk assessments
- Access to services must be controlled by appropriate security barriers



Subdivision into zones and segments

- Risk assessments
- System owner is responsible
- Zones is an underlying principle for the security architecture
- A zone defines a minimum level of security
- Security barriers between zones
- Each zone contains one or more network segments

Security barrier elements

The security barrier may consist of one ore more of the following elements:

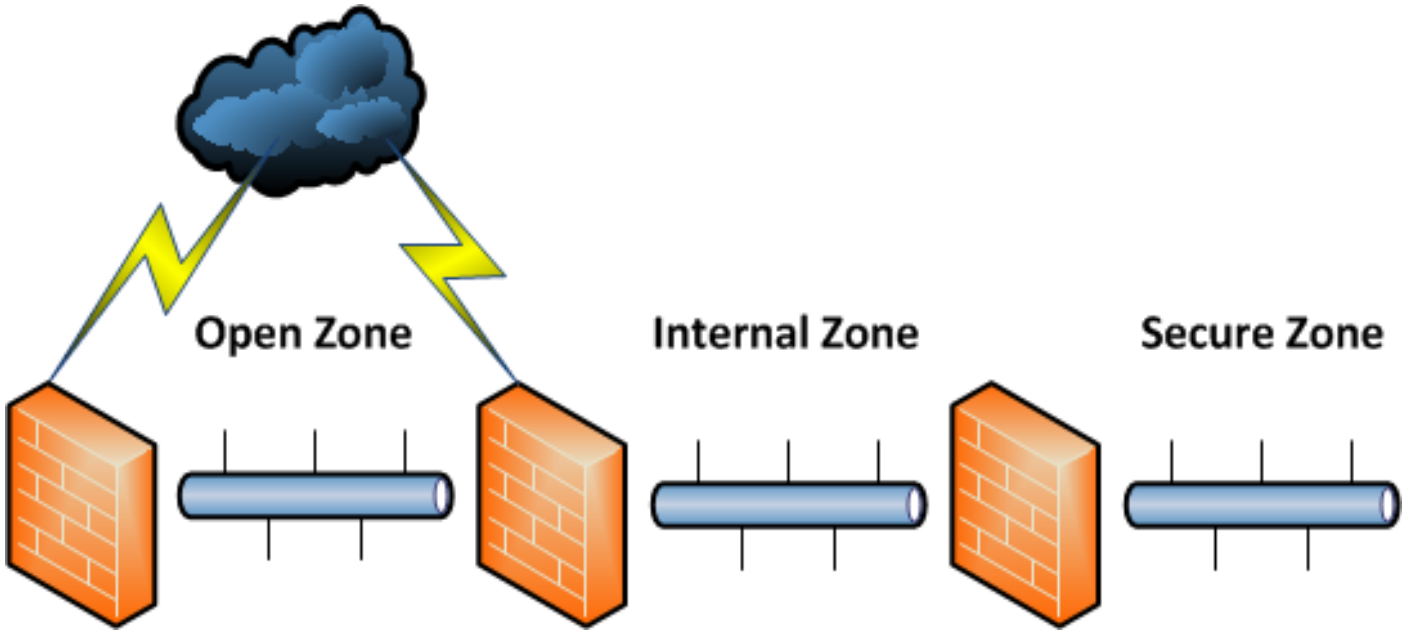
- Firewall/firewall functionality in a router
- Packet filter
- Application gateways, such as proxies and terminal servers
- Authentication and access control
- VPN systems/SSL Gateways
- Client requirements
- Server requirements

Zone assignment

It is recommended to organize the zones as follows:

- **Secure zone** for sensitive data and critical systems
- **Internal zone** - internal network segments
- **Open zone** for everything else

Implementation of zones and security barriers



Security barrier
Packet filters
Firewall
Antispam

Security barrier
Packet filters
Firewall
Antispam

Authentication
VPN
Terminal server

Security barrier
Packet filters
Firewall

Authentication
Terminal server

Requirements for dedicated servers

- **Open zone**
  Requirements related to good system administration, such as patching and the disabling of unnecessary services, security hardening and central logging
- **Internal zone**
  The same requirements as for the Open zone
- **Secure zone**
  The same requirements as for the Open zone

  Consider additional measures such as integrity checks, host-based intrusion detection, data encryption and security hardening

Requirements for clients

Clients should be separated from dedicated servers and located in different network segments

- **Open zone**
  No requirements or requirements determined by the institution
- **Internal zone**
  Clients must be administered centrally
  Clients must comply with the institution's standards for operating systems
  Antivirus software and other protection measures
  No private clients
- **Secure zone**
  No clients in the secure zone
  Access by clients from the internal zone
  Special care for remote access

Authentication and access control

The term access control describes a security barrier that a client must pass in order to gain access to resources hosted in a specific zone and security class.

The following general principles apply:

- Access shall be granted on a “need-to-have” basis only
- Adequate mechanisms must be in place to enable logging and traceability

Authentication and access control – Open zone

- Access control for wireless networks should be implemented using eduroam or equivalent implementations
- A separate arrangement must be put in place for guests who are not participants in eduroam
- Eduroam or equivalent authentication procedures must also be employed in a wired open zone, such as in auditoria and meeting rooms

Authentication and access control - Internal zone

- All equipment connected to the network must be authenticated
- All users should be authenticated against a central user database
- Systems that do not support central authentication must be given special protection

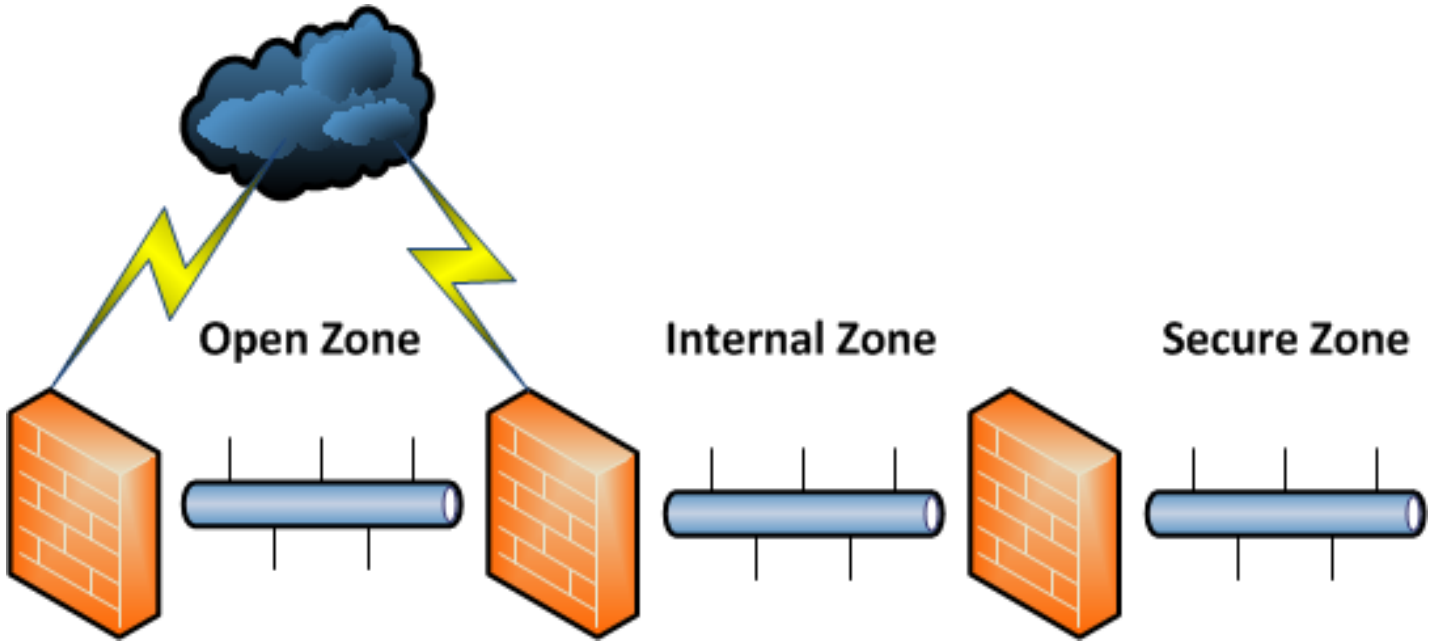
Authentication and access control - Secure zone

- Users wishing to gain access to the secure zone from the internal zone must be re-authenticated
- Special care must be taken if remote access is permitted to a secure zone

The services and systems in the zoned network

The system owner of a given service is responsible for determining the zone in which the service will be located and the type of protection it will be allocated

Services and systems in zones

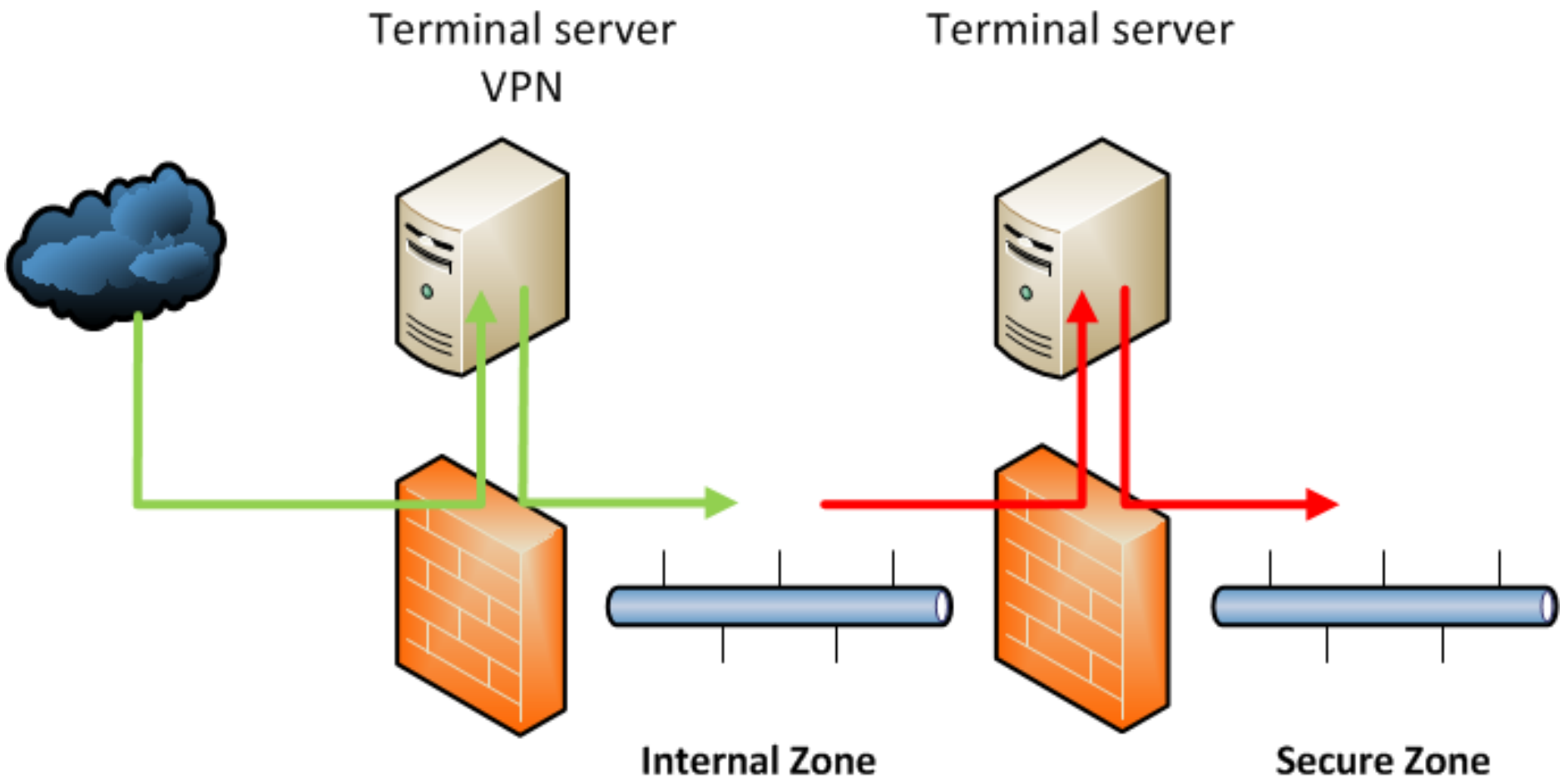


Open information
Guest networks
Student services
External websites
DMZ

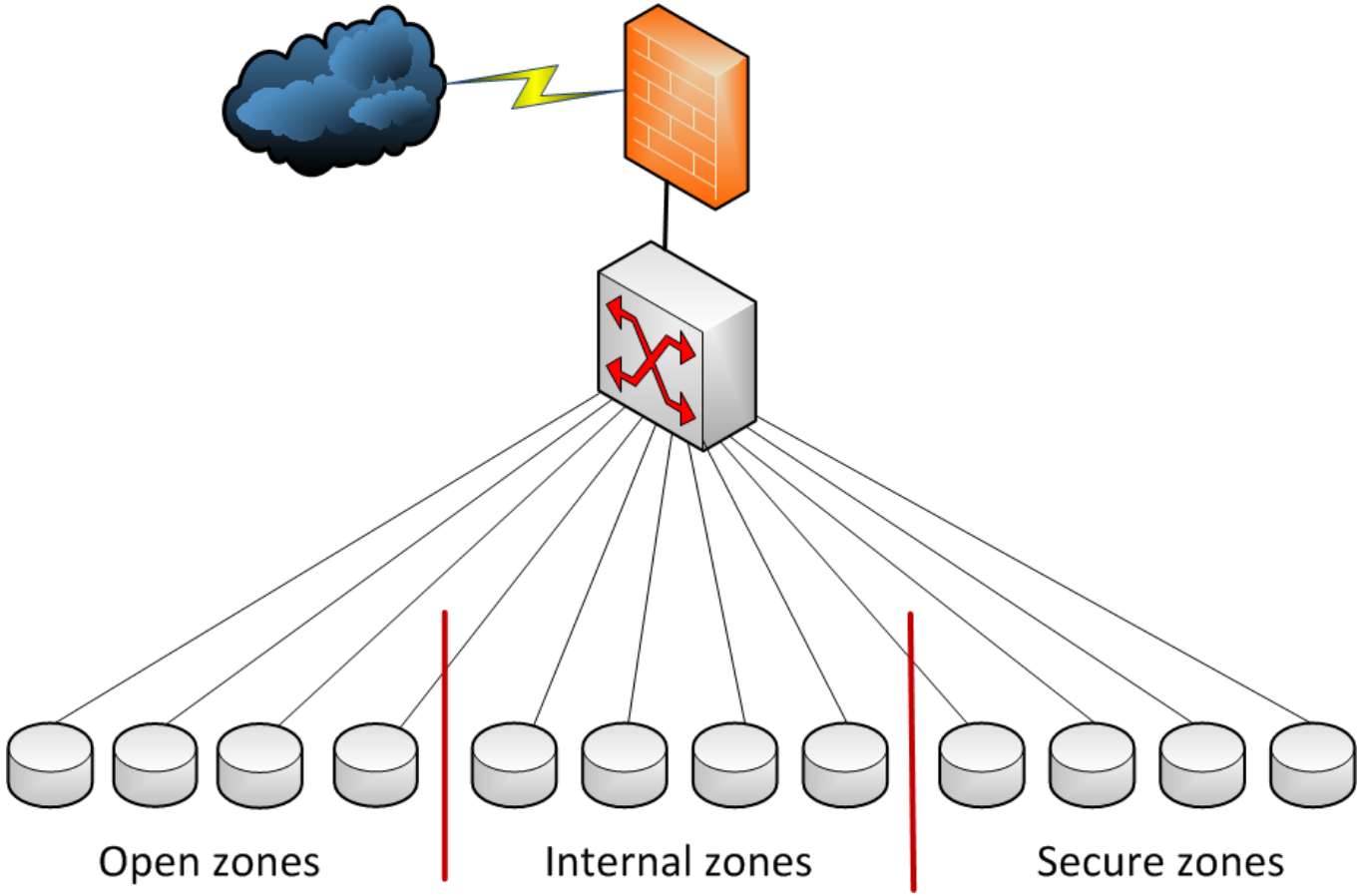
Internal information
Nonsensitive personal data
Administrative systems
Data storage
System services (AD, DHCP, DNS…)
Client administration systems
Monitoring services

Confidential information
Sensitive personal data
Mission-critical systems

Access to zones via terminal servers and/or VPN



Multiple zones



BELGRADE SECURITY WORKSHOP 2015