Norwegian National Security Authority

Network Security Guidance

Last updated: 2014-08-22

N-01 Network Security Guidance

Guidance on Network Security to comply with the NSM Information Security directive

This document provides guidance on Network Security requirements according to the Security Act.

NSM reference: A03 – S:12/00310-4

Norwegian National Security Authority

The Norwegian National Security Authority is a cross-sectoral professional and supervisory authority within the protective security services in Norway and administers Act of 20 March 1998 relating to Protective Security Services. The purpose of protective security is to counter threats to the independence and security of the realm and other vital national security interests, primarily espionage, sabotage or acts of terrorism. Protective security measures shall not be more intrusive than strictly necessary, and shall serve to promote a robust and safe society.

Purpose of guides

NSM's guidance activities are intended to build expertise and increase the security level of organisations through increased motivation, ability and willingness to carry out security measures. NSM regularly issues guides to help implement the requirements of the Security Act. NNSA also publishes guides in other professional areas relating to protective security work.

Postal address
P.O. Box 14
1306 BÆRUM
POSTTERMINAL

Civilian phone/fax
+47 67 86 40 00/+47 67 86 40 09
E-mail address
post@nsm.stat.no

Military phone/fax
515 40 00/515 40 09

URL
www.nsm.stat.no

Content

1 Introduction

NSM is directed through the Norwegian Security Act § 9 e. to give guidance and advice on, securing information systems that are classified according to the Security Act § 11 and 12.

NSM guidance G-01 to G-06 provides high-level security requirements to the system platform. The N-requirements complement the G-requirements, by providing network security specific guidance on how to comply with the NSM Information Security Directive for those services. The N-01 guidance provides functional security requirements for network devices and infrastructure.

The requirements in this guidance are written according to RFC 2119. The keywords “must, “must not, “required”, “shall”, “shall not, “should”, “should not”, “recommended”, “may”, and “optional” in this document are to be interpreted as described in RFC 2119[1].

NSM encourages readers to send their comments and viewpoints on this document to “NSM Kontakt” on FISBASIS-B/U (BEGRENSET) or post@nsm.stat.no (unclassified).

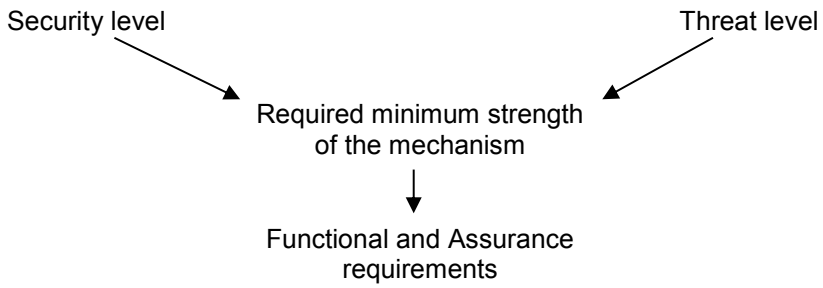
[1] In this guidance “shall” are requirements, while “should” are recommendations

2 Security Model

Classified information systems are traditionally categorized based on mode of operation, i.e. dedicated, system high, partitioned and multi-level. This categorization will however not be sufficient to give a generic description of minimum requirements for network security, because different parts of the network are exposed to different levels of threat, e.g. threats originating internally versus threats originating externally, e.g. untrusted networks.

As the different tasks and services provided by the network grows in numbers, the overall network design structure tends to be quite complex. To be able to effectively and efficiently handle the information security, the security requirements have to be adapted depending on the security level[2] of the system, and the threat the service is exposed to[3].

Generic minimum network security requirements across different security and threat levels create a complex structure of requirements which is not always easy to navigate through. To make this more manageable and user friendly, a security model is developed. The model categorizes requirements into more manageable entities. Different security mechanism requirements are expressed through functional and assurance requirements.



2.1 Security levels

Security levels are associated with confidentiality, integrity, authentication and availability. This document uses slightly modified definitions of the security level defined in “NSM Cryptographic Requirements v2.2”.

High Security

- Confidentiality level equal to classification level “HEMMELIG”
- Confidentiality level equal to classification level “KONFIDENSIELT” in large information systems.
- When a breach of the service results in loss of integrity, authentication or availability of systems or information causing damage equivalent to compromise of information classified “HEMMELIG”, or equivalent to compromise of information classified “KONFIDENSIELT” in large information systems.

Medium Security

- Confidentiality level equal to classification level “KONFIDENSIELT”
- Confidentiality level equal to classification level “BEGRENSET” in large information systems.
- When a breach of the service results in loss of integrity, authentication or availability of systems or information causing damage equivalent to compromise of information classified “KONFIDENSIELT”, or equivalent to compromise of information classified “BEGRENSET” in large information systems.

---

[2] the damage incurred if the security service is disrupted or compromised

[3] threat level

Basic Security

- Confidentiality level equal to classification level “BEGRENSET”
- When a breach of the service results in loss of integrity, authentication or availability of systems or information causing damage equivalent to compromise of information classified “BEGRENSET”
- This security level might also apply to large UNCLASSIFIED system, as compromise of large amount of UNCLASSIFIED information might cause similar or larger damage than compromise of information classified “BEGRENSET”

Where a mechanism is identified at multiple security levels, the highest security levels shall apply.

2.2 Threat levels

As for security levels this document uses a modified version of the definitions for threat levels in “NSM Cryptographic Requirements”.

High Threat

- The mechanism is used to protect systems or information against threats from systems without sufficient accreditation level, or from individuals without sufficient clearance level for the system or information that is being protected. High threat includes the separation of special categories (SPECAT).

Medium Threat

- The mechanism is used to protect systems or information against threats from sufficiently accredited systems or individuals that are not authorized for the system or information that is being protected.

Standard Threat

- The mechanism is used to protect systems or information on a need to know basis.

Low Threat

- The mechanism is used to protect systems or information against threats from sufficiently accredited systems or from sufficiently cleared individuals that are authorized for the system or information being protected.

For the purpose of threat level definitions within this document, “BEGRENSET” is considered as a clearance level, i.e. threat level high applies to cases where mechanisms in a “BEGRENSET” system are protecting against threats from users who are not authorized for access to the system, or when a “BEGRENSET” system is connected to an UNCLASSIFIED system.

Where a mechanism is identified at multiple threat levels, the highest threat levels shall be applied.

2.3 Minimum requirements for security mechanisms

The minimum requirements for security mechanisms are given as four levels: Special, Enhanced, Standard and Moderate. The relationship between security level, threat level, and minimum requirements for network security is given in the following table.

	Threat level High	Threat level Medium	Threat level Standard	Threat level Low
Security level High	Special	Enhanced	Standard	Moderate
Security level Medium	Special	Enhanced	Standard	Moderate
Security level Basic	Enhanced	Standard	Moderate	Moderate

Mechanisms approved according to a higher set of requirements may be used in cases where a lower requirement set would be sufficient.

In some special cases a higher set of requirements than deduced from the table above may apply. In such cases the requirements are especially highlighted in the functional requirements in this document or in the different specialized network guidelines.

An example of a simplified system design implementing this model is shown in chapter 3.3.

2.3.1 Minimum assurance level of security mechanism

Based on the security requirements identified above, NSM require the following assurance levels of the security mechanisms according to Common Criteria (CC):

Special requirements	-	Assurance level according to risk assessment[4], minimum CC EAL 4
Enhanced requirements	-	Assurance level shall be according to CC EAL 4
Standard requirements	-	Assurance level should be according to CC EAL 4
Moderate requirements	-	Assurance level should be according to CC EAL 4

2.3.2 Functional requirements

Functional requirements describe minimum functionality to fulfill a given security requirement. In many cases, the required functionality will differ when the required strength of the mechanism changes. Hence there is no context-independent set of requirements for a given mechanism.

Technical requirements for network security in different contexts are described in Chapter 4. When not stated otherwise the requirements apply to all mechanism strength levels.

[4] Contact NSM for further information

3 Network Design

3.1 General Network Design

To achieve assurance of the quality of the security mechanisms and constant level of resistance in a secured system, there has to be established processes and routines that verify the effectiveness of the implemented mechanisms. To achieve this, the system design needs to be under strict control. Establishments of standard processes are more likely to achieve overall control than the ad-hoc approach.

Use of established and tested solutions for a given design or functionality will normally give a higher assurance level. Such reference solutions are often known as “Best practice” solutions.

Modularization, standardization and reuse are common principles in system design to lower the complexity, and achieve more efficient operations. These principles will also ease the aspect of maintenance and verification of the security mechanisms.

a. The network shall be designed through a planned process
b. The design shall incorporate the security principles from the “Regulation on protection of classified information”[5] § 5-5; *Minimalism, Least privilege, Redundancy, Defense in depth, Self-protection, Controlled data-flow and Balanced strength*
c. The network design shall follow NSM or vendor best practice guidance when applicable
d. The design shall incorporate modularization, standardization, and reuse when applicable

3.2 Network Security Zones

In an information system, different users and devices will normally have different requirements and authorization. To maintain the principle of minimalism for all users and devices, it is good practice to group devices and users with similar needs into different security zones.

To achieve controlled data flow, flow control mechanisms shall be implemented in the interconnection point between security zones. Such mechanisms shall inspect and enforce data flow policies inbound as well as outbound.

a. End-user equipment, servers and other common equipment shall be placed in separate network security zones
b. Servers with different roles shall be placed in separate network security zones
c. Connections to other information systems shall be terminated in dedicated network security zones, solely used for such information exchange
d. System management shall use dedicated network security zones
e. Flow control devices shall be established at the interconnection point between security zones

Requirements for flow control mechanisms are described in 4.4.

3.3 Example Design

3.3.1 The network as an integrated part of an information system

To demonstrate how implementing different network security zones in an information system can be done, an example design has been developed. This example design also shows how the security model from chapter 3 can be used to identify minimum strength of the different security mechanisms in the system.

The example design in Figure 1 is a system high design for one of the partitions in a compartmented information system at security level high. The system also has connections to several other information systems and a solution for remote access.

[5] Forskrift om informasjonssikkerhet

The system operation and management zone require protection from the rest of the information system. This protection mechanism will normally require the strength level of “STANDARD”.

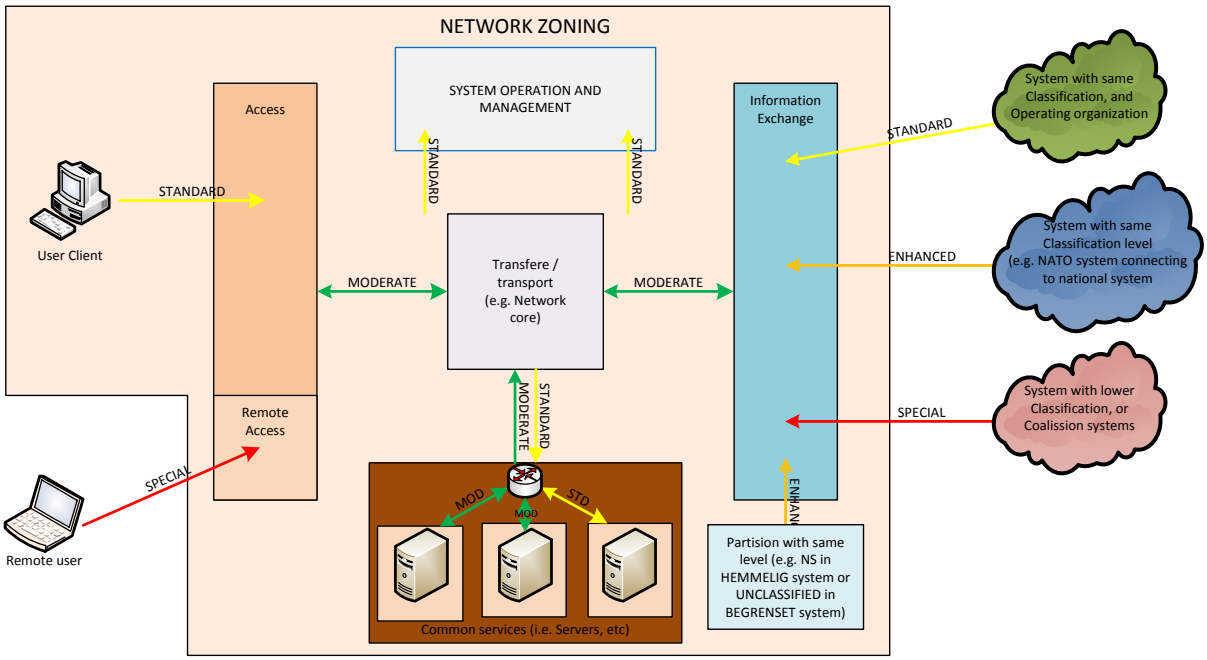


Figure 1 – Example of a high level security design of an information system with security level high, and how the security model is used to identify required minimum strength of the different security mechanisms in the system. In this example system the different servers are placed in a common server network security zone. The server zone is further divided into smaller security zones based on the functionality and protection requirements of each of the different servers, e.g. authentication services will normally require better protection than intranet services. This approach makes the different filtering rules more manageable as common filtering can be performed at the common zone, while more application specific, fine-grade filtering are performed at the smaller network security zones within the common server zone.

3.3.2 The network as a system of its own

The network can also form a system of its own, e.g. a service provider network. The figure below illustrates how the security model can be used to identify different security requirements in this scenario.

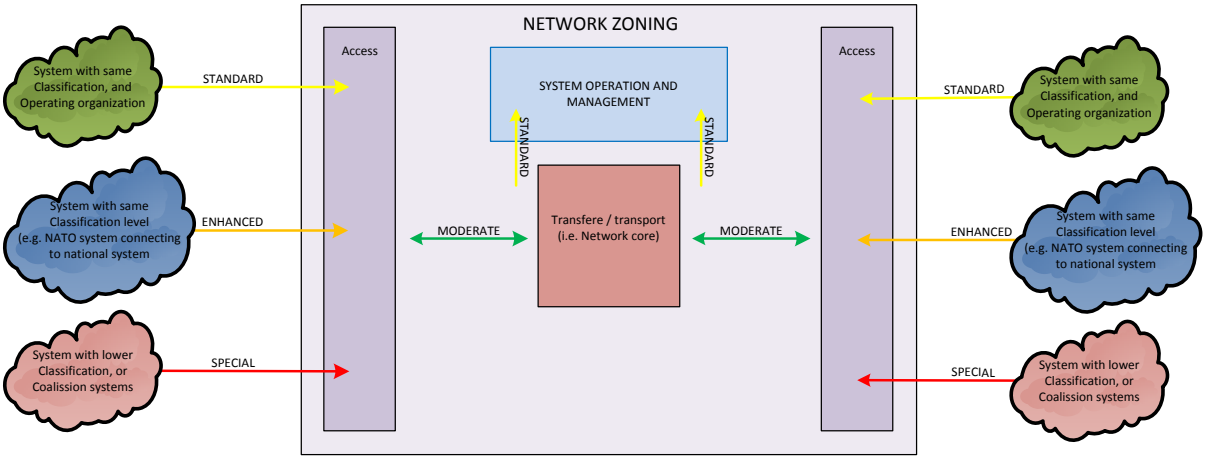


Figure 2 - Example where the system consists of the network only. The network creates connectivity between different systems or between different locations within a system. All devices connecting to the network are considered to belong to external systems.

4 Functional Requirements

4.1 General Network Functionality Requirements

4.1.1 Network Security Zones

Users and devices with different requirements and authorization shall be grouped into different security zones to make enforcement of the principle of minimalism more manageable.

Mechanisms to control information flow between zones shall be implemented to enforce controlled data flow between devices and users in different security zones. If the communication between zones is not controlled, the connection between the zones will short-circuit the segmentation and create one large security zone.

a. Network security zones shall be defined and established
b. The network shall have mechanisms to prevent information leakage between zones
c. The network shall have mechanisms to control information flow between security zones

4.1.2 Availability

Lack of availability of important services often impose a similar threat to modern information infrastructures as broken confidentiality. Lack of availability can arise from several conditions, such as equipment failure, network saturation etc. Traditionally, the concept of availability has focused on limiting the impact of equipment failure. This is still important, but this approach does not cover denied access to services resulting from network saturation.

Quality of Service (QoS) has traditionally not been seen as part of network Infosec, but primarily a mechanism to enable time sensitive applications in packet based networks, e.g. voice over IP. In network Infosec, QoS can be used to reduce the impact of network saturation; QoS enables better control of bandwidth usage and makes it possible to prioritize services according to importance and technological requirements.

To make QoS effective, the QoS has to be implemented end-to-end throughout the entire network with common policy settings. To minimize impact of priority misuse, the traffic should be prioritized and policed as close to the end-point as possible. In addition, policing should be performed on all interfaces where saturation may occur. The entire network needs to be protected against network saturation. Traffic flows which violate the priority policy should either be stopped or remarked with a lower priority given by the overall QoS policy.

a. The network should have redundancy to prevent and minimize impact of equipment failure
b. The network should implement QoS to prevent network flooding and provide service availability
c. QoS should be implemented as an end-to-end functionality across the whole network
d. Network traffic flows shall be classified based on technological requirements and the importance of the service generating the flow.
e. QoS marking shall be done as close to the network edge as possible.
f. QoS policing should be implemented to prevent priority violations and saturation
g. QoS policy violations shall be logged

QoS is not required, but still recommended, for systems with security level “Basic” according to the definitions in chapter 3.

4.1.3 Preventing forged services

Several network services are essential for operation of information systems. DHCP, ARP and DNS are all examples of such services. If any of these services are compromised, the security of the system

can be severely damaged through e.g. man-in-the-middle attacks and Denial-of-Service (DoS) attacks.

a. The network shall have mechanisms to prevent forged network services
b. The network shall have mechanisms to protect internal essential functionality

4.2 Access to the network

The perimeter in a “defence in depth” security design is controlling access to the system as a whole; if you can’t access it you can’t attack it. In a computer network this is typically done by access switches at the network edge, gateways to other systems, or VPN concentrators which give access to the network from a remote location outside the systems control.

4.2.1 Authentication

To control access to the network, devices and users shall be authenticated before they are given access to any services to prevent unauthorized usage and access to the system. Maintaining a large number of locally configured databases for authorizations will become unmanageable as the size of the network increase. To maintain a manageable authorization database, the network shall use a centralized directory service.

The authentication process can also be used to place devices and users into different security zones based on their profile and authorization. In some situations there are however not possible to authenticate all devices or users. In such situation, those types of devices and users shall be placed in separate zone(s) which only gives them access to a strict minimum of services.

All connection and disconnection of devices should be logged to assist intrusion detection and support incident handling activities.

a. The access control mechanism shall authenticate users and devices connecting to the network
b. The authentication process shall use a centralized directory service
c. Authenticated devices and users shall be placed in network security zones based on their profile and privileges
d. Devices and users that are not authenticated shall be denied access, or be placed in dedicated zone(s) which only gives access to a strict minimum of services
e. All connection and disconnection of devices should be logged

4.2.2 Remote access

Remote access solutions give users access to internal features of the system from external locations, and therefor need to implement at least the same level of security as mechanisms used to control local access to the system. Remote access can however not rely on physical barriers like controlling physical access to an office, and hence need to take this into account in the technological mechanisms.

Remote access security relies on a combination of client security (i.e. the client operating system, client firewall, remote access client software, etc.), network security (i.e. the remote access termination point, network security zoning, etc.), and cryptographic requirements. This network security guidance only covers high level requirements for the remote access termination point of the solution.

The remote access termination point is a critical component to control access to the network, and hence need to be protected. When connecting from an external location, users can pose a greater risk to the system than connecting from an internal location. A risk assessment shall therefor be conducted to evaluate user privileges when connecting through the remote access solution.

To protect the information between the remote client and the system, the connection shall be encrypted. Both successful and unsuccessful remote connections shall be logged to assist detection of security breaches and support incident handling activities.

a. The remote access termination point shall be protected

b. The remote access mechanism shall authenticate users and devise connecting to the network
c. The authentication process shall use a centralized directory service
d. Users who connect to the system through remote access shall be terminated in a dedicated network security zone solely used for this purpose
e. A risk assessment shall be used to evaluate user privileges when connection are made through remote access
f. Devices and users that are not authenticated shall be denied access
g. The communication between the client and the remote access point shall be encrypted
h. Both successful and unsuccessful connections shall be logged

4.3 Routing

Routing information is used to decide how the information shall be transported through the network. If an attacker is able to control or manipulate this information, he or she can perform a range of different attacks, e.g. man-in-the-middle or DoS.

a. The network shall have mechanisms to prevent unauthorized manipulation of routing information
b. Routing information shall be isolated from user traffic

4.4 Flow Control

Flow control mechanisms are used to control the information flow between different network security zones. The flow control mechanisms protect the system by;

1. protecting against network-based attacks
2. breaking up, inspecting, and controlling communication between different security zones
3. hiding or masking sensitive protocol information that passes between the different security zones

Network security zone boundaries include both internal boundaries, and interconnections between systems.

Flow control can be achieved at several levels in the protocol stack; ranging from simple packet filtering mechanisms to complex proxy services and information exchange gateways. The different flow control mechanisms all have their place in the network to achieve a good system security design with a defense-in-deep approach. The different flow control mechanisms can be divided into filtering devices, proxy services, one-way flow devices (data diodes), and information exchange solutions.

4.4.1 Filtering devices

Filtering devices are most commonly implemented in firewalls, but can also be implemented in other network devices capable of filtering traffic based on access-lists.

Filtering devices which only inspect and control information flows based on network protocol layers up to and including OSI layer 4, can be used to reduce the system's attack surface. Such devices will however not protect the system against network-based attacks that do not violate the protocol specification of permitted protocols. Filtering devices are also unable to perform fine-grained filtering of common services requiring dynamic port negotiation, such as VoIP, Windows RPC-services etc.

Application firewalls are able to inspect and interpret information at the application layer. Most application firewalls do only support application layer inspection for a subset of protocols. For unsupported protocols, the filtering is performed at the network layer. In such cases the application firewall is limited to network filtering.

Common examples of application firewall functionality are;

- URL-filtering
- Dynamic opening and closing of UDP port used by media streams in SIP and H.323 applications
- Dynamic opening of TCP ports for the data channel in FTP

The filtering device shall:
a. stop malformed packets
b. stop information flows where packets are out of state
c. support access lists to control information flow based on protocol, session state, and source and destination ports and addresses

Application firewalls shall in addition:
d. inspect and make decisions based on information at all OSI layers up to and including the application layer

Filtering devices can be used to enforce flow-control with mechanism strength at moderate level. Application firewalls can be used to enforce flow-control up to, and including standard level, except connections to other systems.

4.4.2 Proxy and Application Level Gateway (ALG)

A proxy service acts on behalf of the client or user for access to a network service and shields each side from a direct peer-to-peer connection[6]. In network Infosec, the different proxy services can be divided into two categories; transparent proxy services and application proxy services.

To protect the devices running Proxy and Application Level Gateway services, these devices shall implement filtering mechanisms according to the filtering device requirements, or be protected by external filtering devices.

4.4.2.1 Transparent Proxy services and ALG

A transparent proxy or application level gateways (ALG) can enforce detailed control on allowed or denied traffic flows by authenticating users and services. If the network flow is permitted by the security policy after authentication, a communication pipe is opened between the communication parties. In a security context the transparent proxy service or ALG can be seen as an advanced filter device, because the information flow between the communication parties are not inspected or filtered on the application layer after the communication pipe has been established.

An application level gateway or Transparent Proxy shall:
a. Enforce detailed control on allowed traffic flows
b. Break up and prevent direct network connectivity across the device
c. Be able to allow or deny traffic through the device based on user authentication, location and requested service
d. Be able to inspect traffic flow through the device and drop malicious traffic, i.e. malware inspection
e. All allowed and denied flows through the device shall be logged

[6] S. Northcutt et.al., “Inside Network Perimeter Security”, p 85, SANS GIAC 2003

Transparent Proxy services and ALG can be used to enforce flow-control between information systems with mechanism strength up to, and including standard level, except connections to other systems.

4.4.2.2 Application proxy services

As for transparent proxy services the application proxy service can enforce detailed control on traffic flows between users and services. But instead of establishing a transparent communication between the application and the service, the application proxy service actively takes part in all stages of the communication. Because of this active involvement, the application proxy prevents a direct communication path between the parties also at the application layer, and can thereby shield the protected service from attacks at the application layer after a communication path has been established. Moreover, this active involvement enables very fine-grained policy enforcement on the information flow through the proxy.

An application proxy shall:

a. Enforce detailed control on allowed traffic flows at the application level
b. Break up and prevent any direct connectivity across the device
c. Be able to allow or deny traffic through the device based on user authentication, location and requested service
d. Be able to inspect all traffic through the device and drop malicious traffic, i.e. malware inspection
e. Support fine-grained policy enforcement using standard or custom profiles
f. All allowed and denied flows through the device shall be logged

Application proxy solutions can be used to enforce flow-control between information systems with mechanism strength up to, and including enhanced level

4.4.3 One-way flow

One-way flow devices provide a high assurance mechanism where information can only be transported from one side to the other. The devices range from simple pseudo-wire solutions to more complex solutions providing content and integrity checking, simulation of application responses etc.

To prevent malicious use of the one-way flow solution to manipulate the information system on the other side and prevent malware, the solution needs to implement content and integrity check of all information. Because it is very hard to implement effective countermeasures against all type of attacks and malware, it is often necessary to deny certain types of information through the solution, e.g. runnable code.

One-way flow solutions shall

a. have high assurance that information can only flow in one direction
b. only permit information from defined applications and protocols to flow from one side to the other
c. log all information transported through the solution
d. enforce a dedicated destination for all information allowed through the solution
e. implement content and integrity check of all information flowing through the solution
f. have dedicated security zones on both sides

One-way flow solutions can be used to enforce flow-control between information systems with mechanism strength at all levels

4.4.4 Information Exchange between information systems

In many organizations there are increased requirements for information exchange between internal and external information systems to support different business processes. To mitigate the security risk introduced by these interconnections, and provide a framework to secure information exchange, a set of basic principles and requirements has been established.

a. All information exchange shall be conducted through application proxies
b. The solution shall implement content and integrity check of all information flowing through the solution, e.g. prevent executable files and malware from entering the system
c. The solution shall implement information protection services to prevent information leakage
d. Connected systems and users using the solution shall be authenticated
e. All information transported through the solution shall be logged
f. The solution shall implement flow control mechanisms to allow only permitted services through the proxy solution
g. Security monitoring and incident handling functionality shall be implemented to detect and prevent attacks from systems connected through the solution

Information exchange solutions can be used to enforce flow-control between information systems with mechanism strength at all levels

4.5 Network Device Management

Management capabilities play an important role in maintaining network and system security. To perform this task, the network management capability relies on situational awareness and effective management processes. Fragmented management might cause reduced situational awareness, resulting in new security threats. To prevent this from happening, network management shall be under centralized control. When the network is considered an integrated part of an information system, the network management should be an integrated part of the system management.

Unauthorized access to devices and management traffic is considered a serious threat to the network and system security.

a. The management process shall be well defined and structured, e.g. following the ITIL process
b. All devices shall support centralized management, operation monitoring and logging
c. Physical access to devices shall be restricted to authorized personnel only
d. Management access to devices shall be restricted to authorized personnel only
e. Only individual user admin accounts shall be used
f. The management traffic shall be protected

4.6 Network monitoring

Because of the large number of events and the different types of security incidents in modern information systems, security monitoring based only on manual analysis of security events will neither be effective or efficient. Security monitoring tools are used to support the secure operation and maintenance process by help detecting, collecting, filtering, correlating, prioritizing, and presenting security relevant events.

Effective and efficient security monitoring cannot be implemented by monitoring tools alone, but need to be supported by appropriate management processes and qualified personnel.

In the following, only requirements for security monitoring tools are covered.

4.6.1 Intrusion detection

Intrusion detection systems (IDS) are automated systems which monitors information systems for suspicious activity. They are often divided into two types of IDS, network-based (NIDS) and host-based (HIDS). In general, IDS sensors watch for predefined signatures of bad events, and might

perform statistical and anomaly analysis to detect bad events. NIDS are designed to examine the network traffic to identify threats by detecting scans, probes, and attacks.[7]

This document only covers requirements for NIDS.

Although an IDS is expected to have built-in functionality for common probes and attacks, they have to be updated to support detection of new types of vulnerabilities and attacks as they emerge. The IDS should also allow administrators to attach custom scripts and signatures to monitor and detect system- and scenario-specific security events that are not covered by the standard signatures. Anomaly-based detection capabilities would also improve the detection rate of new types of attacks as these attacks normally will introduce new network traffic with its own characteristics which differ from the characteristics seen in the network before. In a CIS of a certain size, support of a system-wide Security Incident Event Management (SIEM) service are normally needed to collect, correlate and analyze the detected events in an effective and efficient manner.

To mitigate threats from attacks who utilize IDS evasion techniques, the IDS solution is required to detect and handle such events.

The IDS shall
a. utilize signatures to detection to detect known attacks
b. have mechanisms to update signatures in a timely, efficient and secure manner
c. support custom signatures to allow administrators to monitor and detect system- and scenario-specific attacks
d. support anomaly-based detection
e. support extensive logging of security-related events, and possible and actual intrusion attempts
f. have mechanisms to alert and report on detected attacks in near real-time
g. be able to detect and handle well known IDS evasion techniques

In a CIS of a certain size, functions described in e and f should interoperate and/or integrate with a system-wide Security Incident Event Management (SIEM) service

To protect the security of the information system, the attacks need to be not only detected but also stopped. To stop detected attacks, and thereby minimize the security impact of the attack, the IDS needs mechanisms to control the information flow, either as an integrated IPS-solution or through automatically updating rules in flow control devices. Manually updating rule sets will normally not be sufficient to stop many attacks, because of the increased reaction time. Automated responses should be used with caution, because when implemented wrong they can result in DoS of the protected service.

h. To act upon detected attacks, the IDS should have mechanisms to stop such attacks, either as an integrated IPS-solution or through automatically updating rule sets in flow control devices

4.6.2 Operation monitoring

System and network monitoring involves anomaly detection but concentrates on availability and performance parameters of resources. In the context of network Infosec, system and network monitoring primarily gives administrators awareness of the state of the protected system; i.e. the system helps detection of interruptions in availability, changes in performance and detection of unexpected changes in the environment that might adversely impact the effect of the security measures.

The operation monitoring system shall:

[7] S. Northcutt et.al., “Inside Network Perimeter Security”, SANS GIAC 2003

a. detect interruptions in service availability
b. detect changes in performance and availability of the system
c. detect bottlenecks and shifts in performance of the infrastructure
d. detect unexpected changes in the environment that might adversely impact the effect of the security measures

4.6.3 Security Incident Event Management (SIEM) tools

IDS, firewall and network device logs, traffic flow information, security relevant server and application logs etc, all provide security relevant data which are necessary to build a complete picture of the security state in an information system. The wide range of data formats from the different sources makes it a hard to analyze and correlate the data into useful information.

The main task of a SIEM solution is to help this process through collection, normalization and correlation of the data from the different sources into information. A SIEM solution will normally use signature and anomaly detection engines to detect attacks. By visualizing the collected information both log-analysis efficiency and reaction time will normally be improved. The SIEM solution can also use information from these engines to produce automated responses.

The SIEM solution shall:
a. be able to collect security relevant data from relevant sources in the system, e.g. IDS, firewall and network device logs, traffic flow information, relevant server and application logs etc
b. be able to normalize collected data
c. be able to correlate log events
d. have functionality to visualize log events to improve log-analysis efficiency
e. be able to use signatures to detect and visualize attacks in real time
f. be able to detect and visualize system anomalies which can be indication of attacks
g. provide automated response to reduce reaction time for detected attacks
h. have mechanisms to configure and update attack signatures

5 Incident Handling and Recovery

Incident handling and recovery is an important part of Infosec to restore a secure state after a security incident. Preventive actions can lower the number of incidents, but it is in reality impossible to prevent all incidents.

Incident handling is an action plan for dealing with misuse of an information system. In this context, incidents are intrusions, malicious code, information theft, DoS, and other security related events. Recovery is the plan on how to restore the secure state of the information system after an incident.

Creation of incident response plans, policies, and procedures are important to perform the complex task of incident handling and recovery effectively, efficiently, and consistently. The plan, policies, and procedures should cover both technical and non-technical aspects of the incident handling process. Examples of such aspects are standard operation procedures (SOPs) on how to handle a technical task, definitions of what an incident is, how to classify and prioritize incidents, how to interact with other parts of the organization, authority, etc.

After an incident, it is important to use the lessons learned from the incident to improve the incident handling process, and help prevent similar incidents in the future.

a. The network shall be supported by incident handling and recovery capabilities
b. The establishment of the incident handling and recovery capabilities shall be supported by incident response plans, policies, and procedures
c. The incident response team shall be given sufficient authority and resources to handle incidents effectively and efficiently
d. A lessons learned process shall be implemented to improve the incident handling process, and help prevention of similar incidents in the future

Annex A Document check

Date	*Changes*
13.04.2011	First internal review
17.08.2011	Version 0.9
17.11.2011	Version 0.95 – rewrite based on internal review and removal of some duplication from the G-series guidance.
19.04.2012	Version 0.96 – rewrite based on internal review.
27.06.2012	Version 1.0 – First official version
28.08.2012	Version 1.1 – minor layout changes
12.06.2013	Version 1.2 – Adding new requirements in 4.4.2, 4.5, 4.6.1, and 4.6.3 to clarify intended requirements.
22.08.2014	Version 1.3 – Adding logging requirements in 4.2.1, 4.2.1, 4.4.2, 4.4.3, and 4.4.4 to better support detection of security violations and incident handling