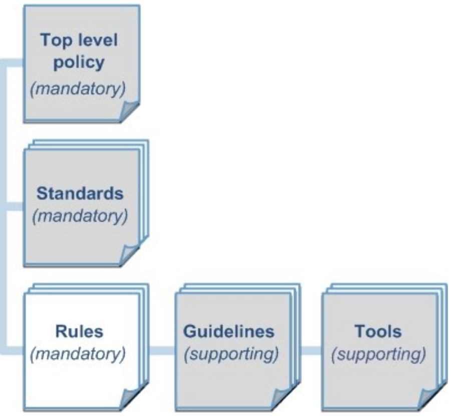
KPN Security Policy

KSP – Rule

Title	**Network Segmentation**	
ID	**KSP-FA05-RL08**	
Funct. Area	05 – System and Network security	
Date	5 February 2016	
Version	v1.5	
Status	Approved	
Owner	CISO	

Summary

This document describes rules that must be taken into account while building services (for instance a Voice, TV, internet or internal IT- service) within service infrastructures (like datacenters).
The rules are a breakdown of parts of the Network and Communication (KSP-FA05-ST03) standard.
This document does not cover TI-infrastructure, e.g. networks for office networks or other transport networks.

Disclaimer

The content of this document is to describe KPN's policy on this specific topic. If and when this document is partly or fully disclosed to parties outside of KPN, it's important to hereby note towards those parties that this contains KPN's intended policy and cannot in any way be read or construed to be an explicit or implied formal guarantee or promise that its content can always be fully executed or complied to.

ID	KSP-FA05-RL08-R01
Title	System interfaces
Description	System interfaces must be exclusively assigned to one production zone. In addition, systems must have a separate management interface in a management zone (physically or logically). Additional system interfaces must be added to the same configured zones.
Relating document	N/A

ID	KSP-FA05-RL08-R02
Title	Filtering traffic
Description	Traffic that passes a zone boundary inbound or outbound must be filtered. This can be done by either ACLs or Firewalls. Any traffic that isn’t explicitly allowed and registered in a communication matrix must be denied and logged.
Relating document	N/A

ID	KSP-FA05-RL08-R03
Title	VLANs and services
Description	Services must be separated from each other by usage of VLANs. If a service spans multiple zones, it must have a separate VLAN for every zone. If a service is composed out of multiple (smaller) sub-services, the services must be separated from each other.
Relating document	N/A

ID	KSP-FA05-RL08-R04
Title	VLAN routing
Description	When a system has multiple VLAN connections in a zone, routing between them must be disabled by default. Where routing between VLANs is necessary, traffic that passes the boundary between VLANs must be filtered.
Relating document	N/A

ID	KSP-FA05-RL08-R05
Title	Communication between services
Description	Communication between services must be done through a common production zone (i.e. red, orange or green).
Relating document	KSP-FA05-ST03 - Network and Communication Security

ID	KSP-FA05-RL08-R06
Title	Communication Matrix
Description	For a service a communication matrix must be in place and kept up to date, stating the following for each communication flow the service has: • Originating and target System name; • Originating and target System IP address; • Originating and target System Ports used (TCP/UDP); • Originating and target System Protocol used (ICMP, VRRP, HTTP); • Originating and target System VLAN; • Originating and target System Service name; • Originating and target System Owner.
Relating document	N/A

ID	KSP-FA05-RL08-R07
Title	VPN usage from user-devices
Description	Using one or more VPN connections from a user-device must exclusively communicate to and from the user-device. The user-device must not facilitate communication between the available connections. The end-users must ensure sufficient measures have been taken to prevent this and the user-device must be protected according to the KSP.
Relating document	N/A