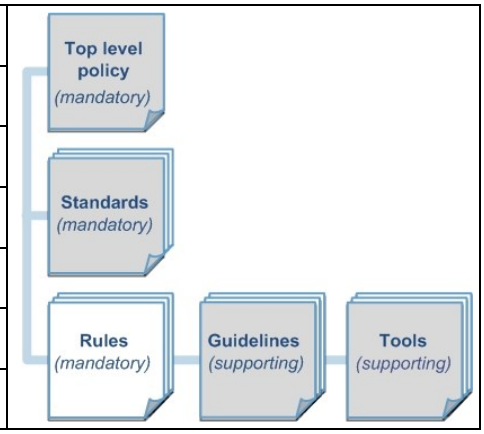
# KPN Security Policy

## KSP – Rule

| | |
|---|---|
| Title | **Network Segmentation** |
| ID | **KSP-FA05-RL08** |
| Funct. Area | 05 – System and Network security |
| Date | 29 July 2016 |
| Version | v1.6 |
| 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.

**Version history**

| *Version* | *Date* | *Comments* |
|---|---|---|
| v1.0 | 3 September 2013 | Approved in SSM |
| v1.1 | 9 October 2013 | Updated based on consistency check |
| v1.2 | 1 August 2014 | Minor update to R01 |
| v1.3 | 20 July 2015 | Adjusted document summary |
| v1.4 | 13 November 2015 | R03 clarified |
| v1.5 | 5 February 2016 | Added R07 |
| v1.6 | 29 July 2016 | R03 and R04: replaced VLAN for logical network separation<br>R07: clarified (split tunnel) |

| | |
|---|---|
| **ID** | KSP-FA05-RL08-R01 |
| **Title** | System interfaces |
| **Description** | System interfaces must be exclusively assigned to one production zone.<br>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** | Logical network separation and services |
| **Description** | Services must be separated from each other by usage of logical network separation. If a service spans multiple zones, it must have a separate logical network for every zone.<br>If a service is composed out of multiple (smaller) sub-services, the services must be separated from each other.<br><br>For infrastructures identified as vital infrastructure the network separation must not be performed nor dependent upon a hypervisor or container.<br><br>Example technology:<br>VLAN's, Q-in-Q, VXLAN, Private VLAN, VRF, Oracle Solaris Zones. |
| **Relating document** | KSP-FA05-GL03 - Security Architecture Guidelines |

| | |
|---|---|
| **ID** | KSP-FA05-RL08-R04 |
| **Title** | Communication between logical networks |
| **Description** | When a system has multiple logical network connections in a zone, routing between them must be disabled by default.<br>Where routing between logical networks is necessary, traffic that passes the boundary between these networks 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:<br>• Originating and target System name;<br>• Originating and target System IP address;<br>• Originating and target System Ports used (TCP/UDP);<br>• Originating and target System Protocol used (ICMP, VRRP, HTTP);<br>• Originating and target System VLAN;<br>• Originating and target System Service name;<br>• 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. (no routing between the (vpn) 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 |