

Overview of selected KPN Security Policies

Creation date: Wednesday, November 7, 2018 8:10:45 PM

Selected by: Ruud Leurs

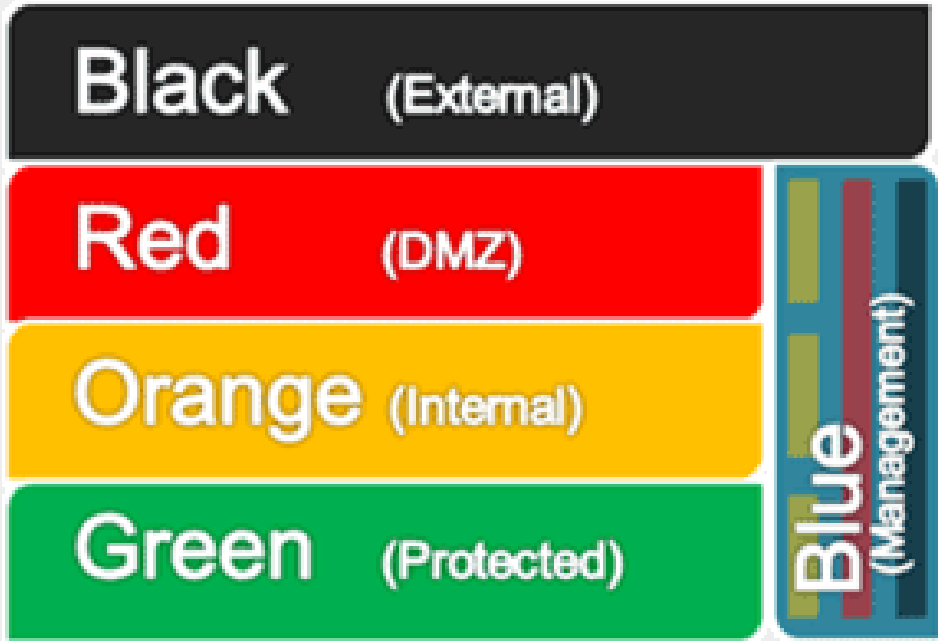
Requirement	Logical network separation and services
Description	<p>Services must be separated from each other by usage of logical network separation. If a service spans multiple zones, it must have a separate logical network for every zone.</p> <p>If a service is composed out of multiple (smaller) sub-services, the services must be separated from each other.</p> <p>For infrastructures identified as vital infrastructure the network separation must not be performed nor dependent upon a hypervisor or container.</p> <p>Example technology:</p> <p>VLAN's, Q-in-Q, VXLAN, Private VLAN, VRF, Oracle Solaris Zones.</p>
ID	KSP-RE-280
Version	1.0
Date	December 11, 2017
Rationale	Separating environments

Requirement	Communication between logical networks
Description	<p>When a system has multiple logical network connections in a zone, routing between them must be disabled by default.</p> <p>Where routing between logical networks is necessary, traffic that passes the boundary between these networks must be filtered.</p>
ID	KSP-RE-281
Version	1.0
Date	December 11, 2017
Rationale	Separating environments

Requirement	Communication between services
Description	Communication between services must be done through a common production zone (i.e. red, orange or green).
ID	KSP-RE-282
Version	1.0
Date	December 11, 2017
Rationale	Separating environments
Rationale	Documenting network infrastructure
Rationale	Encrypting network traffic
Rationale	Business Continuity Management (BCM)
Rationale	Designing to availability level

Requirement	Communication Matrix
Description	<p>For a service a communication matrix must be in place, stored in a CMDB and kept up to date, stating the following for each communication flow the service has:</p> <ul style="list-style-type: none"> * 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
ID	KSP-RE-283
Version	1.1
Date	November 2, 2018
Rationale	Separating environments

Requirement	Requirements for non-production platforms
Description	Platforms for development, testing and acceptance must be separated from the production platform.
Supplement	Testing the change in the production environment poses extra risks because of possible unexpected behaviour due to the change.
ID	KSP-RE-286
Version	1.4
Date	November 2, 2018
Rationale	Separating environments

Requirement	Network segmentation and security zoning
Description	<p>Segments must be defined and implemented for a network environment to support a layered security model.</p> <p>This can be achieved by building services in accordance to a security zoning model. The following is a high-level description of the KPN standard zoning model:</p>  <p>A typical service would have the systems users (who are in the Black zone) need to interact with in the Red zone, systems that are purely for service internal use in the Orange zone and servers containing confidential data in the Green zone. All systems also need a connection into the Blue zone in order to be managed.</p> <p>The internal network KOEN is classified as a black zone.</p>
Supplement	<p>Just as in physical security, not everything happens in one room. Network segments should have a specific purpose and should be separated from other segments with their specific purpose. Segmentation must be done on function and classification of network data.</p> <p>A webserver that is used for serving webpages to internet should not be in the same segment as the backup system for this server.</p>
ID	KSP-RE-287
Version	1.0
Date	December 11, 2017
Rationale	Separating environments

Rationale	Encrypting network traffic
Rationale	WLAN security

Requirement	Network separation
Description	Equipment which is not part of the network infrastructure and has multiple interfaces, must be configured such that routing or forwarding is not possible. This is also required for VPN interfaces on a system.
Supplement	This ensures that unintended network traffic is prevented.
ID	KSP-RE-277
Version	1.2
Date	November 2, 2018
Rationale	Separating environments

Requirement	Network filtering
Description	Between network segments a network filter must be in place through which only necessary traffic can pass.
Supplement	<p>Network segments are defined because of their different uses, security wise and functionality wise. To keep these separated, filtering of networking traffic is necessary.</p> <p>A webserver may need a database server backend to be able to serve content to clients. This communication must be limited to only the necessary database communication to prevent misuse. This communication is registered in a communication matrix.</p>
ID	KSP-RE-288
Version	1.0
Date	December 11, 2017
Rationale	Separating environments

Requirement	System interfaces
Description	<p>System interfaces must be exclusively assigned to one production zone.</p> <p>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.</p> <p>When physical or logical zoning is not possible in for instance a phpmyadmin site, the logical zoning must incorporate a method like whitelisting the management stations in order to only allow management stations to address the management portal.</p>
ID	KSP-RE-278
Version	1.0
Date	December 11, 2017
Rationale	Separating environments

Requirement	Applications sharing a platform
Description	When more than one application is hosted on a platform, the security measures needed for each application must be implemented for all hosted applications; applications must not share the same platform when they do not have approximately the same function.
Supplement	<p>Applications sharing a platform may influence each other or may be an attack surface for each other.</p> <p>When two web applications with different risk classification share a system, the web application with the lowest risk classification must have the same security measures as the web application with the highest risk classification; otherwise it can be attacked to reach the highest classified information on the system. The Security Architecture Guidelines give more insight in how to protect cloud solutions with regard to this requirement.</p>
ID	KSP-RE-289
Version	1.0
Date	December 11, 2017
Rationale	Separating environments

Requirement	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.
ID	KSP-RE-279
Version	1.0
Date	December 11, 2017
Rationale	Separating environments