Overview of selected KPN Security Policies

Creation date: Wednesday, December 4, 2019 1:31:44 PM

Selected by: Ruud Leurs

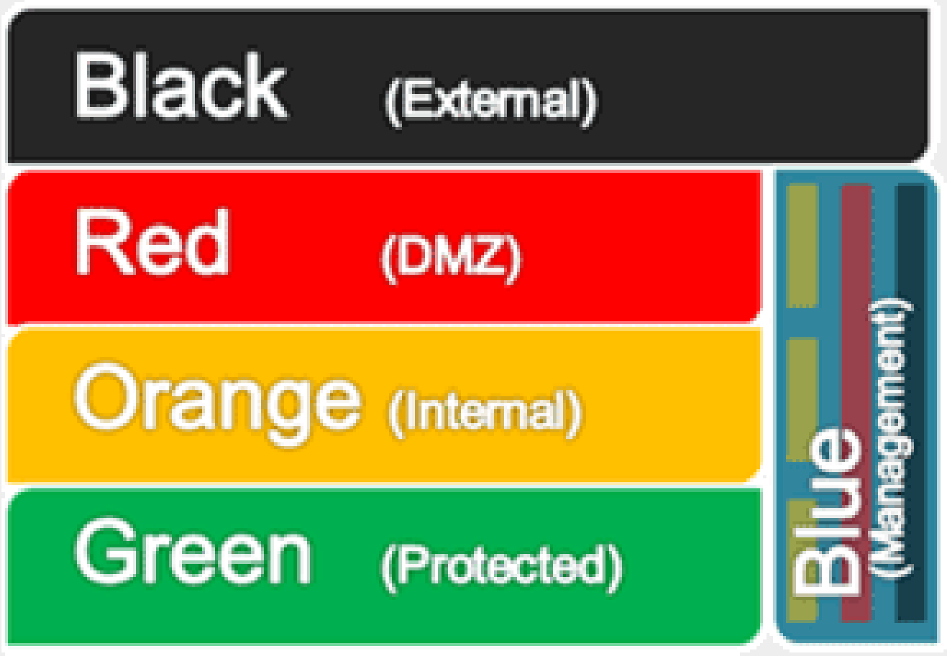
Requirement	**Logical network separation and services**
Description	Services must be separated from each other by usage of logical network separation. If a service spans multiple zones, it must have a separate logical network for every zone. If a service is composed out of multiple (smaller) sub-services,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

Requirement	**Communication between logical networks**
Description	When a system has multiple logical network connections in a zone, routing between them must be disabled by default. Where routing between logical networks is necessary, traffic that passes the boundary between these networks must be filtered.
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). An alternative is possible when communicating to central services, e.g. Microsoft Active Directory for authentication and account synchronisation. The communication must be configured with a stateful firewall in such a way that the establishment of the connection's initiative is exclusively from the relying service to the central service.
ID	KSP-RE-282
Version	2.0
Date	February 1, 2019
Rationale	Separating environments
Rationale	Documenting network infrastructure
Rationale	Encrypting network traffic
Rationale	Designing to availability level

Requirement	**Communication Matrix**
Description	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: * 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 or testing, and platforms for acceptation of operational software must be separated in sufficient degree of each other and of the live environment. The acceptance environment need to resemble the live platform in architecture and setup. Tests must be conducted on a test platform. The use of sensitive information (e.g. privacy, business obligations) in a development and test environment is explicitly forbidden. In an acceptance environment that meets the KSP, and that has the same security level as the production environment, use is allowed.
Supplement	Testing the change in the production environment poses extra risks because of possible unexpected behaviour due to the change. The use of real customer and user date exposes this data to loss, disclosure and access to this by not authorised people. When test data will not reveal enough assurance (e.g. compare test results with operational results) so real data must be used; then all security measures for production data must be taken for the test platform and permission from the Operational Security Manager or, depending on the datatype, Senior Security Officer or Privacy officer must be obtained prior to the start of the test activities.
ID	KSP-RE-286
Version	1.5
Date	December 7, 2018
Rationale	Separating environments

Requirement	**Network segmentation and security zoning**
Description	Segments must be defined and implemented for a network environment to support a layered security model. 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:  Black (External) Red (DMZ) Orange (Internal) Green (Protected) Blue (Management) 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. Communication between services is prescribed in KSP-RE-282. The internal network KOEN is classified as a black zone. Customer IaaS and PaaS environments must be segmented.
Supplement	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. Segmentation can be applied using a variaty of technologies which includes and is not limited to MPLS tags, VLAN, VXLANs, virtual networks and other overlay technology. Direct communication to generic services, e.g. Active Directory, is conditional to KSP-RE-282. A webserver that is used for serving webpages to internet should not be in the same segment as the backup system for this server.

ID	KSP-RE-287
Version	1.2
Date	November 1, 2019
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	Traffic between zones must pass through the designated network filters. A host which may be connected in multiple zones, either by physical or logical connection and which is not designated as the network filter, must not form a(n) routing facility.
Related info	
ID	KSP-RE-277
Version	1.3
Date	February 1, 2019
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	Network segments are defined because of their different uses, security wise and functionality wise. To keep these separated, filtering of networking traffic is necessary. 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.
ID	KSP-RE-288
Version	1.0
Date	December 11, 2017
Rationale	Separating environments

Requirement	**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. 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.
ID	KSP-RE-278
Version	1.0
Date	December 11, 2017
Rationale	Separating environments

Requirement	**Applications sharing a platform**
Description	Applications must not share the same platform when they do not have the same data-classification. When more than one application is hosted on a platform, the highest security demanding application will determine the minimal security requirements.
Related info	
ID	KSP-RE-289
Version	1.1
Date	February 1, 2019
Rationale	Separating environments

Requirement	**Filtering traffic**
Description	Traffic that passes a zone boundary inbound or outbound must be filtered with firewalls. Any traffic that isn’t explicitly allowed and registered in a communication matrix must be denied and logged. Cloud resources must be segmented and zoned using stateful firewalls. Changes to the traffic filters must follow change management rules for the asset and the change to be registered.
ID	KSP-RE-279
Version	1.2
Date	November 1, 2019
Rationale	Separating environments

Requirement	**Wireless connectivity to control and maintain objects**
Description	It is forbidden to control or maintain any object used for services, service components, or applications using any type of wireless connectivity past the stepping stone (i.e. wireless connectivity is allowed upto the stepping stone, after the stepping stone the connection must be wired). Examples of forbidden wireless connectivity is: Wi-Fi Bluetooth Infra-red Mobile network Other radio-based solutions using any type of antenna NFC-based solution with a maximum usage of 20 centimeters or less from (virtual) card to reader is allowed.
Supplement	Radio based control and maintenance is susceptible to security, safety and continuity risks due to electro-magnetic disturbances and unable to control the object, man-in-the-middle attacks, circumvention of physical (access) controls and barriers due to radio leakage through walls.
ID	KSP-RE-754
Version	1.1
Date	August 9, 2019
Rationale	WLAN security
Rationale	Separating environments

Requirement	**Maintenance of services**
Description	Technical management must be performed through a stepping-stone or a dedicated maintenance interface supplied by the cloud provider. Functional maintence can be performed both through the technical management interface as per production interface. For functional maintenance, segregation of duties must be applied between normal user accounts and administative accounts.
Supplement	There is no separate interface, nor a blue zone, in various cloud solutions. Functional and technical management tasks can be located through the front-end interfaces.
ID	KSP-RE-776
Version	1.0
Date	August 9, 2019
Rationale	Remote access
Rationale	Public Cloud
Rationale	SaaS provider