

2.9 Suggested network configuration

2.9.1 Introduction

Each company has its IT rules and more than often a proper IT staff to apply them. Thus what we are going to suggest to you is not a specific configuration because you have to adapt it to your own business needs. It's more a sort of Rule of Thumb about how we suggest to organise data transport separation.

Basically we'll suggest you to split the services, binding them on multiple interfaces. We found that is far more easy to manage 2 interfaces instead of 3 or 4 of them, still (as said before) this is a matter of your company's network design.

 It can be quite useful to consider PrivateServer as a [Session Border Controller](#), when it comes down to deciding how to configure its network placement.

2.9.2 Rules of thumb

The services separation occurs by considering the following rules:

1. Use two networks interfaces at least and set them up as:
 - a. Internal Interface: private IP, not directly accessible from the extern of the company
 - b. External Interface: public IP, directly accessible from anyone
2. Services should always be split in two categories:
 - a. management
 - b. service provider
3. Each category should be mapped on a different interface:
 - a. management on the Internal Interface
 - b. service provider on the External Interface
4. One amend to rule number 3 is if your company wants to offer the secure voice system to the internal network as well (or to some part of it)
5. Both SIP/TLS and HTTPS-Smartphone Web Services are necessary to run the service on mobile devices
6. public access is needed for with Data packages are involved
7. No point in having Nagios service on the public interface
8. Disable SSH access as soon as you can or keep it as the last resort: you might want to place it on an hidden network or protect it by a firewall rule

2.9.3 Possible implementations

Our standard proposal is to split the VoIP service and the Administration service having the former to respond on the first interface, directly connected to the Internet via public IP address or just NATted from a public one. The latter would respond on the second NIC, an internal interface with a private IP address assigned on it.

So that's a simple schema exemplifying the core of this subject:



Interface Binding		
Service	Public (ens192)	VPN (ens224)
SQL/3306 - DataBase	<input type="checkbox"/>	<input type="checkbox"/>
HTTPS - Management Console	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SSH - Secure Shell	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SIP/TLS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SIP/UDP	<input type="checkbox"/>	<input type="checkbox"/>
TCP/5666 - Nagios Monitoring	<input type="checkbox"/>	<input type="checkbox"/>
HTTPS - Smartphone Web Services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 Update		

figure 1. a typical aggregation of services split on two interfaces

 Please keep in mind that's perfectly possible to enable Secure VoIP Service in your company's network as well, using internal wireless network which could pair the service offered on external address/port. In this scenario there can be issues related to name resolution and certificates. Please contact PrivateWave Italia S.r.l. assistance in case for full service network design support.

[2.8 Software repositories](#)

[2.10 SAML configuration and activation](#)