

PSAM 2.2 Network Segregation

You can decide how to distribute the services of PrivateServer using the "network segregation". You can access the configuration page via **Services** link in the **main menu**.

2.1 Services

Edit Applications

Network interfaces

	eth0	eth1
db	<input type="checkbox"/>	<input type="checkbox"/>
http	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ssh	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
asterisk	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
asterisk_trunk	<input type="checkbox"/>	<input type="checkbox"/>
nrpe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>


 **Update**

figure 1. Application Matrix

The page is divided in three parts: the first one is actually about the network segregation itself.

It shows a simple matrix made from services and NICs ([figure 1. Application Matrix](#)) thus you can choose which service would be accessible on which interface and in this way profile your network design accordingly.

The NICs are automatically detected.



The NIC are listed even if they are not configured, so please check your Network configuration before assigning or diverting a service from a NIC.

The Applications are the following:

- **db**: remote access to the DBE (Data Base Engine), useful for exporting views and access data used by the appliance
- **http**: the very same web administrative console you are actually using
- **ssh**: the well known text console for remote administration
- **asterisk**: the core of the secure VoIP service
- **asterisk-trunk**: part of the VoIP service used to connect the PrivateServer appliance to another PBX
- **nrpe**: monitoring service via Nagios

After you're done, just press the "Update" button.

2.2 Certificates

The second part is about certificate assign. When you divide your services amongst the NIC you are using them on different IPs as well. This implies you might choose different certificates each one related to each IP of the NIC your service is bound to.

TLS certificates

	Certificate
http	<input type="text" value="Built-in key pair (*.madama.at)"/>
asterisk	<input type="text" value="privatewave.com (rendezvous.privatewave.com)"/>


 **Update**

figure 2. Certificates management

Two are the services that need a valid certificate:

- Asterisk or Secure VoIP
- HTTP or Administration Web Interface

You can load as many certificates as you need and then assign one of them to one of the two above services, as it suites you better. After you're done, just press the "Update" button.



Please consider that the certificates are strictly bounded to the name they are released for, so you make sure you assigned via DNS the proper name to the IP where the service is published

2.3 Hostnames

The third part is about configuring the hostnames that would be used for the provisioning.

Hostname configuration


Asterisk hostname:	<input type="text" value="privatewave.moseo.fr"/>
Provisioning full path:	<input type="text" value="https://adm-privatewave.moseo.fr"/>
	

figure 3. hostnames configuration

The **Asterisk hostname** is the name of the PBX which would be included into the provisioned configuration to be sent to the client.

The **Provisioning full path** is the base URL for downloading both the PrivateGSM application and its configuration. It will be used to fulfill the proper fields in the automatic activation.

[PSAM 2.1 Network Configuration](#)

[PSAM 2.3 Certificates configuration](#)