

ViPNet protection during boot process

One of the important characteristics of the ViPNet-software module is the full control over the traffic being exercised already during the boot process. This control is possible due to the interaction of the ViPNet-Module with all drivers of the network adapters.

Windows provides one single service for all the whole boot process. The ViPNet-module exercises control over this service and ensures complete surveillance of the OS booting.

The ViPNet login process takes place BEFORE the Windows-login, including initialisation of the keys: ViPNet uses drivers which are on the lower (2. and 3.) OSI-layers and are activated before the initialization of all Windows services (Win32) (see illustration below).

If in a network a Windows-domain login is necessary, it is only possible to do this through the secured ViPNet-VPN connection, as these drivers have been loaded BEFORE the Windows login.

ViPNet furthermore verifies the following parameters using the checksum:

- integrity of the own files
- integrity of the key data bases
- integrity of the list of applications authorized to access the network

The advantages of these measures are obvious:

- during and after the boot process of the PC no network attacks are possible, as ViPNet has an integrated firewall with IDS.
- Network login is completely secured by the VPN, which itself is totally transparent for all network applications.

Graphical description of solution:

