vs-top

Facts & Features

Security Laptop

Definition

The compact vs-top security laptop meets two major requirements of mobile users: secure access to classified data in protected networks via the Internet, and an easy to operate working environment to browse the Internet, work with e-mails etc. This is achieved by a separation system, which creates two working environments on the laptop. A main compartment is exclusively used for classified data and a secondary compartment for potentially insecure data processing.

Both compartments can be equipped with Windows or Linux operating systems and individual applications. They are strictly separated, so that the sensitive data is well protected. But both components can be used in parallel. Access to sensitive networks via Internet is enabled by an integrated and underlying VPN. Furthermore all personal, critical or confidential data on the vs-top's hard disc is encrypted and the key is secured on a smart card. The vs-top is approved for the classification levels German VS-NfD, NATO RESTRICTED, and RESTREINT UE/EU RESTRICTED.

Reasons to Choose vs-top

- Secure connections for mobile users
- Two strictly separated working environments on one laptop
- High usability on familiar laptop platforms
- High security VPN connections via cell network, WLAN, and Ethernet
- VPN technology made in Germany
- Reliable hard drive encryption
- Approval for classification levels German VS-NfD, NATO RESTRICTED, and RESTREINT UE/ EU RESTRICTED
- Convenient administration via central management solution

Typical Use

- Connecting mobile users to classified networks of companies and public authorities

Throughput Volume:

- Up to 1 Gbit/s

Customer Service

- Service directly from the manufacturer
- Security system management
- Hotline service/update service
- Comprehensive training courses

SecurITy made in Germany

Excellence in Digital Security

Firewall	
Stateful packet filter	State of the art firewall for manageable rulesets
Network Address Translation (NAT)	Masquerade networks behind one address
Network bridging	Bridging compartment into the local area network without losing packet filter capability
Filter criteria	Filtering decision can be based on IP address, network protocol, port, interface, flags, and state
Filter action	Choice of packet handling: pass, block, drop
Spoofing protection	Block forged packets
Packet normalization	Reassemble fragmented packets, generate random IP identification, enforce IP header settings such as TTL and MSS
Management	Centrally managed by the administrator with genucenter

Virtual Private Network	
General	
IPsec VPN	Operated and enforced by separation layer
Authentication	
RSA	De facto public-key standard
Elliptic curves	Fast key exchange
IKEv1 and IKEv2 authentication	Authentication with keys or certificates using a PKI
Smart card	Key handling via smart card

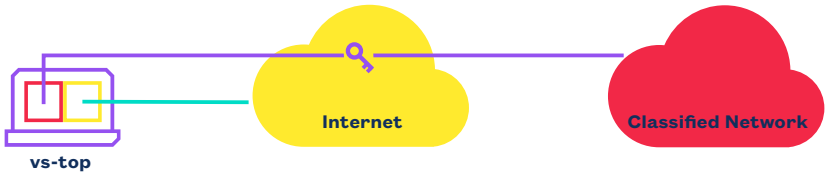
Networking	
Uplinks	
Ethernet	10/100/1,000 Mbit/s Base-T
WLAN	802.11a/b/g/n
LTE/UMTS/GPRS	Integrated modem
Friendly Net Detection	Different access profiles depending on location of the laptop

Separation	
Compartments	Two separate compartments
Network	Parallel network access possible for each compartment through separate network connections
Graphics performance	Native 3D graphics acceleration in primary compartment
Sound	Integrated sound card assignable to one of the compartments at a time
USB peripherals	USB devices such as mouse, keyboard, headset, etc. can be used dynamically in each of the compartments
Smart card	Available for VPN connections and user compartments

Central Management with genucenter	
General	
Configuration	Easy management of several (thousand) systems
Monitoring	See the health of your systems at a glance
Logging	Easily collect and analyse logs
Software distribution	Patch distribution via Central Management Station genucenter can also be delegated to deployment servers
Rollout management	Rollout possible from both heaquarters and remote locations via deployment servers
Web GUI	Powerful web-based user interface secured with TLS/SSL (HTTPS)
Online help	Instant help in the user interface
Patch Management	
GUI	Get and install patches via GUI
Automatic updates	Automate the process of fetching updates for the appliance
Logging	
Local cache	For short term logs
Central	Use genucenter to concentrate the logs on one system

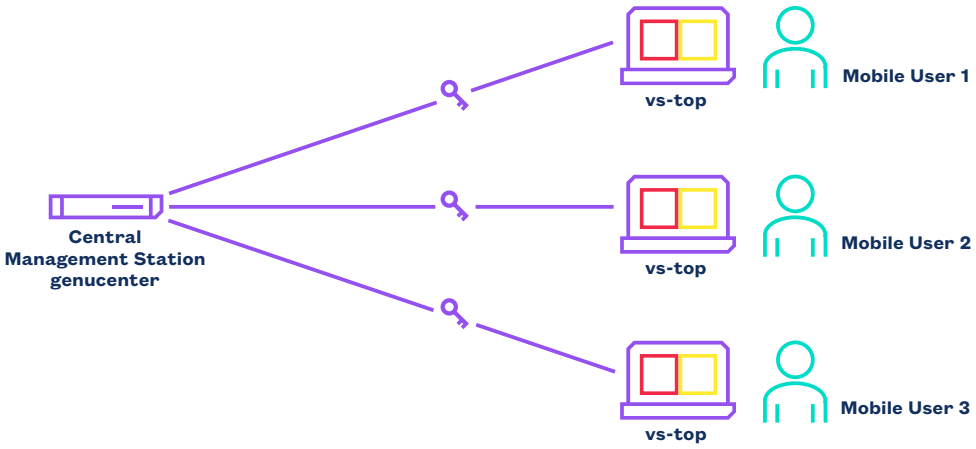
More product information

Use Cases



Connecting Mobile Users to Classified Networks

Mobile users can access classified data in the protected LAN, edit and store the data on the laptop – and at the same time can browse the Internet, work with e-mails etc. All this is performed comfortably and securely, as the compact vs-top provides strictly separated working environments. The connections to the LAN via Internet and the hard drive of the vs-top are strongly encrypted so that the classified data cannot be stolen or manipulatetd by attackers.



Central Administration from a Management Station

The vs-top security laptop is centrally administered using the Central Management Station genucenter. This means that you can keep an eye on a number of users' laptops from a central location and modify the configuration or install updates at any time. Thus you can ensure consequent implementation of your security policy and achieve a high level of mobile security in practice.

VS-FS-0821-01-E

Further Information:

www.genua.eu/vs-top

genua GmbH
Domagkstrasse 7 | 85551 Kirchheim | Germany
T +49 89 991950-0 | E info@genua.eu | www.genua.eu