Excellence in Digital Security.

genua.

vs-top

Security Laptop mit VS-NfD-Zulassung

Technische Informationen

Inhalt

1. IT-Sicherheit für mobiles und flexibles Arbeiten

Diese Informationsbroschüre richtet sich an IT-Sicherheitsverantwortliche, die für die externe bzw. mobile IT-Infrastruktur und deren Absicherung zuständig sind. Sie bietet Ihnen einen kompakten Überblick, wie Sie mit Hilfe des Security Laptops vs-top Mitarbeitern innerhalb und außerhalb des Unternehmens Zugriff auf Firmendaten gewähren können, ohne dass die IT-Sicherheit im Unternehmensnetzwerk gefährdet wird. Dabei bietet vs-top wesentliche Vorteile:

Vorteile von vs-top	
VS-NfD-konforme Datenverarbeitung und -transfers für mobile Anwender	✓
Hohe Sicherheit durch strikt separierte Arbeitsbereiche auf einem Laptop	✓
Kompaktes, einfach zu bedienendes Laptop mit gewohnten Anwendungen	✓
Hochsichere Festplattenverschlüsselung	✓
Vollständige Infrastruktur zentral administrierbar	✓

vs-top ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für VS-NfD (Verschlusssache – Nur für den Dienstgebrauch) zugelassen.

1.1. Herausforderung

In einer globalisierten und digitalisierten Arbeitswelt steigt der Anteil reisender Mitarbeiter, die von unterwegs per Laptop auf Geschäftsdaten zugreifen müssen. Die Verbindungen werden flexibel aufgebaut: Ethernet, WLAN und Mobilfunk. Dazu kommt eine zunehmende Zahl von Heimarbeitsplätzen. Es zeichnet sich bereits ab, dass zukünftig immer mehr Büros regelmäßig leer stehen werden und unsere Zusammenarbeit zunehmend per E-Mail, Groupware und Online-Konferenzen stattfindet.

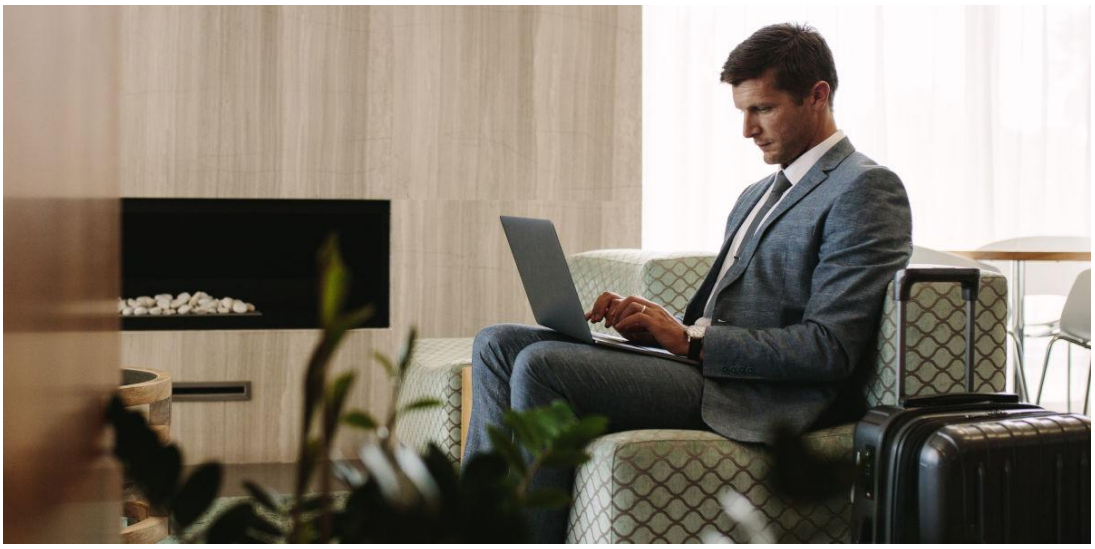
Der technische Fortschritt ermöglicht diese mobile und dezentralisierte Arbeitsweise. Doch diese Entwicklung bringt auch Herausforderungen mit sich: Wie lassen sich Flexibilität und Usability mit zuverlässiger IT-Sicherheit kombinieren? Organisationen müssen beispielsweise an allen Arbeitsplätzen ausschließen, dass Dritte vertrauliche Daten mitlesen, manipulieren oder das Firmennetz infiltrieren.

Es reicht also nicht mehr aus, das LAN mit einer Firewall abzuschotten. Auch die externen Clients müssen sicher abgeschirmt und Datentransfers zuverlässig verschlüsselt werden. Geht ein mobiles Gerät verloren, muss sichergestellt sein, dass Unberechtigte keinen Zugriff auf vertrauliche Daten erhalten. Denn bei Abfluss solcher Informationen drohen finanzielle Schäden, der Verlust von Kundenvertrauen sowie Strafen wegen vernachlässigter gesetzlicher Bestimmungen.

1.2. Anforderungen an einen Security Laptop

Ein mobiles Gerät, auf dem sich firmenvertrauliche Daten befinden und mit dem auf solche im Unternehmensnetz zugegriffen wird, muss demnach deutlich höhere Schutzanforderungen erfüllen als ein rein privat genutztes. Ein besonders hohes Sicherheitsniveau erfordert mobiles Arbeiten mit eingestuften Informationen.

Generell kommen zum Schutz der Daten verschiedene Sicherheitskomponenten in Betracht wie beispielsweise eine Firewall, die das mobile Gerät vor unerwünschten Zugriffen schützt und eine VPN-Lösung zur Verschlüsselung der übertragenen Daten. Darüber hinaus ermöglicht eine Festplattenverschlüsselung das lokale Speichern vertraulicher Informationen zur Offline-Bearbeitung und schützt vor unbefugtem Datenzugriff bei Verlust des Laptops. Für den Zugang zum VPN und den Zugriff auf die lokal gespeicherten Daten muss für hohe Sicherheit eine Zwei-Faktor-Authentifizierung verwendet werden.



Arbeiten unterwegs und im Home Office erfordert den Schutz vertraulicher Informationen

Soll der Anwender mit seinem Gerät gleichzeitig auf vertrauenswürdige und weniger vertrauenswürdige Ressourcen, wie beispielsweise zu Recherchezwecken, uneingeschränkt auf das Internet zugreifen dürfen, benötigt er dazu eine zweite, strikt abgeschottete Arbeitsumgebung. Diese Trennung bietet den Vorteil, dass beispielsweise eine per Webbrowser eingedrungene Schadsoftware keinen Zugriff auf Daten der vertraulichen Arbeitsumgebung oder gar auf das Unternehmensnetz erlangt.

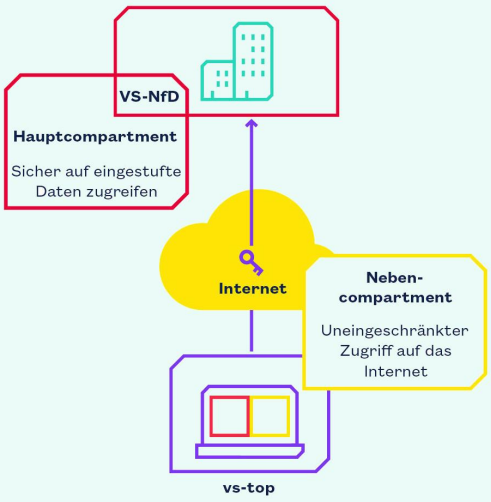
2. Die Lösung: Security Laptop vs-top mit VS-NfD-Zulassung

2.1. Konzept

Das Security Laptop vs-top ermöglicht dem Anwender rundum sicheres mobiles Arbeiten. Es erlaubt den Zugriff auf vertrauliche Daten im Firmennetz und deren

Verarbeitung. Außerdem kann damit z. B. auf einen privat genutzten E-Mail-Client sowie auf einen Webbrowser zugegriffen werden, der aktive Inhalte erlaubt, ohne Risiken für die vertraulichen Informationen einzugehen. Die erforderlichen Sicherheitskomponenten sind im Security Laptop integriert. Zur sicheren Zwei-Faktor-Authentifizierung benötigt der Anwender lediglich eine Smartcard.

Dazu bietet vs-top auf einem Laptop zwei strikt separierte Arbeitsbereiche, die sogenannten Nutzercompartments: In ein Haupt- und ein Nebencompartment kann z. B. Windows oder Linux installiert und parallel, aber hochsicher voneinander getrennt, betrieben werden. Per Tastenkombination kann zwischen dem Haupt- und dem Nebencompartment umgeschaltet werden.



Flexibel und sicher durch strikt separierte Arbeitsbereiche

Ein weiteres Compartment beinhaltet eine Firewall zum Schutz der Nutzercompartments sowie eine VPN-Lösung zur Absicherung von Netzwerkverbindungen, die mit vs-top hergestellt werden.

Darüber hinaus verfügt vs-top über eine integrierte Festplattenverschlüsselung, die Offline-Bearbeitung vertraulicher Dokumente ermöglicht und die Daten vor unbefugtem Zugriff schützt. Da diese für die Nutzercompartments komplett transparent ist, ist keine Installation von Zusatzsoftware erforderlich.

Zur Administration bietet genua die zentrale Management-Lösung genucenter. Damit lässt sich über die Security Laptops hinaus eine vollständige, skalierbare Infrastruktur effizient verwalten.

2.2. Die Sicherheitsarchitektur im Überblick

Strikte Separation der Compartments sowie zuverlässige Sicherheitskomponenten bilden die Voraussetzung für das hohe Sicherheitsniveau von vs-top. Doch wie können diese bei einem Software-basierten Produkt realisiert werden?

Hochsichere Separation: Mit zunehmender Größe und Komplexität von Software wächst nachweislich die Fehlerrate – und damit steigt die Gefahr von Sicherheitsproblemen. Aus diesem Grund basiert vs-top zur Durchsetzung der strikten Separation auf dem Microkernel L4. Dieser besteht aus weniger als 100.000 Zeilen Code und bietet daher eine sehr geringe Angriffsfläche. Mit dem Microkernel kann definiert werden, welche Ressourcen einem Compartment zur Verfügung stehen und welche Zugriffsrechte es darauf hat.

Die Vorteile der L4-Separation machen vs-top damit deutlich sicherer als herkömmliche Virtualisierungslösungen. Doch auch bei Performance und Usability bietet die Separation wegen der Durchreichung von Hardware-Ressourcen an die Nutzercompartments Vorteile: So erhält bei vs-top beispielsweise ein Nutzercompartment Zugriff auf die Hardwarebeschleunigung der Grafikkarte. Damit lassen sich deutlich anspruchsvollere Anwendungen ausführen, als dies mit Virtualisierungslösungen möglich ist.

Zuverlässige Sicherheitskomponenten: Die Sicherheitskomponenten des Firewall/VPN-Compartments basieren auf einem gehärteten Open Source-Betriebssystem. Sie bilden die Basis zahlreicher zertifizierter und zugelassener Sicherheitslösungen von genua und sind daher hervorragend evaluiert.

Vertrauenswürdige Verschlüsselung: Für die sichere Verschlüsselung der Festplatte und der Netzwerkkommunikation kommen ausschließlich Komponenten zum Einsatz, die zu 100 Prozent von genua in Deutschland entwickelt werden oder auf von genua überprüften Software-Bausteinen basieren.

BSI-Zulassung: Das System hat das VS-NfD-Zulassungsverfahren beim Bundesamt für Sicherheit in der Informationstechnik (BSI) durchlaufen und erfolgreich bestanden. Darüber hinaus wird genua beim BSI als „Qualifizierter Hersteller“ geführt. Die Weiterentwicklung der Security Laptops wird von einem kontinuierlichen Qualitätssicherungsprozess begleitet.

2.3. Nutzercompartments

2.3.1. Hauptcompartment

Das Hauptcompartment von vs-top stellt die hochsichere Arbeitsumgebung dar, in der vertrauliche Daten verarbeitet werden dürfen. Aus dem Hauptcompartment kann der Anwender VPN-Verbindungen zu vertrauenswürdigen Netzen aufbauen, also beispielsweise auf Ressourcen im Firmennetzwerk zugreifen.

Während die Arbeit mit Remote Desktop-Lösungen nur bei bestehender Internetverbindung möglich ist, erlaubt vs-top auch den Transfer vertraulicher Daten in das

Hauptcompartment. So kann der Anwender beispielsweise lokal auf Dokumente zugreifen, wenn keine Internetverbindung besteht. Im Hauptcompartment können zudem lokal im Firmennetz oder über VPN Domänen-Anmeldungen durchgeführt und Netzwerkressourcen wie z. B. Netzlaufwerke genutzt werden.

Das im Hauptcompartment verwendete Betriebssystem kann wie gewohnt beispielsweise per System Center Configuration Manager (SCCM) zentral ausgerollt und administriert werden.

2.3.2. Nebencompartment

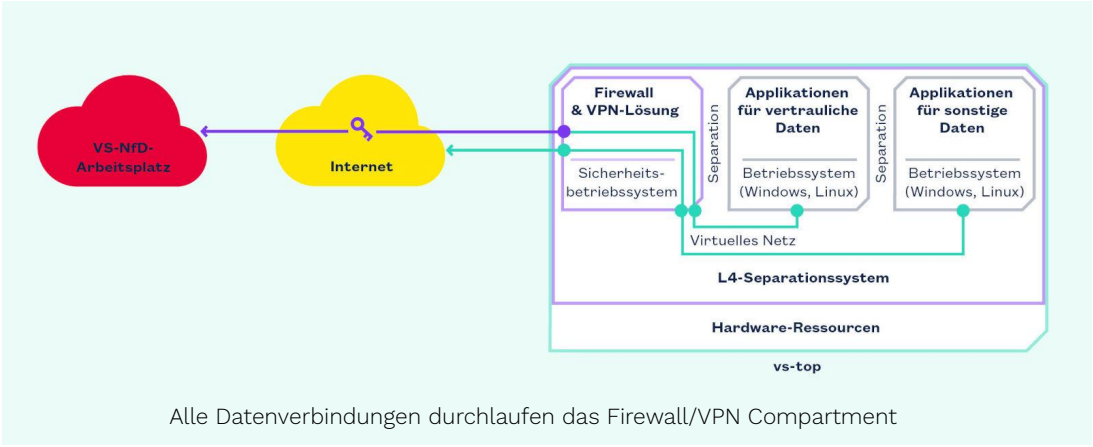
Das Nebencompartment wird im Hauptcompartment als separates Fenster dargestellt, der Wechsel zwischen den Nutzercompartments erfolgt per einfacher Tastenkombination.

Es ermöglicht dem Anwender z. B. die Bearbeitung privater Dokumente oder die Nutzung eines Webbrowsers mit aktiven Inhalten wie beispielsweise JavaScript. Verschlusssachen dürfen hier nicht verarbeitet werden.

Mit dem Nebencompartment können auch Verbindungen zum Internet über sogenannte Captive Portals hergestellt werden, anschließend kann das Hauptcompartment wie gewohnt mit einem VPN verbunden werden.

2.4. Firewall/VPN Compartment

Die im Firewall/VPN Compartment enthaltenen Sicherheitskomponenten des Security Laptops sind den Nutzercompartments vorgelagert und setzen auf ein eigenes, gehärtetes Betriebssystem auf. Sämtliche Datenverbindungen der Nutzercompartments werden über virtuelle Netzwerkschnittstellen durch das Firewall/VPN Compartment geleitet. Firewall-Regelsätze und VPN-Konfigurationen werden zentral administriert und den Security Laptops zugewiesen.



Alle Datenverbindungen durchlaufen das Firewall/VPN Compartment

2.4.1. Paketfilter

Die in vs-top integrierte Firewall basiert auf dem vom Bundesamt für Sicherheit in der Informationstechnik nach CC EAL 4+ zertifiziertem Stateful Packet Filter der Firewall & VPN-Appliance genuscreen. Sie kontrolliert alle Netzwerkverbindungen des Haupt- und Nebencompartments. Direkte Außenverbindungen am Firewall/VPN Compartment vorbei oder direkte Netzwerkverbindungen zwischen Haupt- und Nebencompartment werden nicht zugelassen. Anhand der separaten internen Netzwerkinterfaces zum Firewall/VPN Compartment wird Netzwerk-Traffic des Haupt- und Nebencompartments getrennt verarbeitet.

2.4.2. VPN

Die VS-NfD-konforme VPN-Komponente von vs-top fungiert als Layer 3-basiertes IPsec-Gateway. Damit können zur sicheren Datenübertragung über das Internet VPN-Verbindungen aufgebaut werden. Es kommen ausschließlich starke Verschlüsselungsalgorithmen und große Schlüssellängen zum Einsatz.

2.5. Konnektivität

vs-top unterstützt die Ethernet-Varianten 10/100/1000 Mbit/s Base-T. Zur Kommunikation in Funknetzwerken kommen gängige WLAN-Standards zum Einsatz. Ein integriertes Modem ist kompatibel zu den Mobilfunksystemen LTE, UMTS und GPRS.

2.6. Festplattenverschlüsselung

vs-top bietet eine integrierte Festplattenverschlüsselung. Diese schließt die kompletten Partitionen des Hauptcompartments und des Nebencompartments sowie die Konfiguration des Firewall/VPN Compartments ein. Das Gesamtsystem ist inklusive der integrierten Festplattenverschlüsselung für VS-NfD zugelassen. Daher ist die Installation einer zusätzlichen Festplattenverschlüsselung nicht notwendig. Für den Zugriff auf die verschlüsselten Daten hat der Anwender eine persönliche Smartcard mit einem individuellen privaten Schlüssel. Der Wechsel des symmetrischen Schlüssels des Security Laptops erfolgt automatisch und verursacht somit keinen administrativen Aufwand.

2.7. Einfache Bedienung

vs-top unterscheidet sich in der Anwendung kaum von herkömmlichen Laptops und erfordert keine besondere Einweisung. Es ermöglicht das Arbeiten mit gewohnten Betriebssystemen und Anwendungen. Alle wesentlichen Vorgaben werden zentral verwaltet, wodurch Fehlkonfigurationen durch unerfahrene Anwender ausgeschlossen sind.

Über eine vs-top-Applikation für Windows oder Linux können Anwender Verbindungen zum Internet und einem VPN aufbauen und beenden. Dazu stehen verschiedene Verbindungs- und Zugriffsprofile zur Verfügung. So können Anwender ei-

gene Verbindungsprofile anlegen wie z. B. ein WLAN-Profil zu Hause bzw. im Hotel oder ein LTE-Profil mit eigener SIM-Karte und PIN.

Die Zugriffsprofile werden mit der zentralen Management-Lösung verwaltet. Aus Sicherheitsgründen sind nur Administratoren berechtigt, Zugriffsmöglichkeiten der Nutzercompartments auf VPN- oder offene Netze anzulegen, zu ändern oder zu löschen.

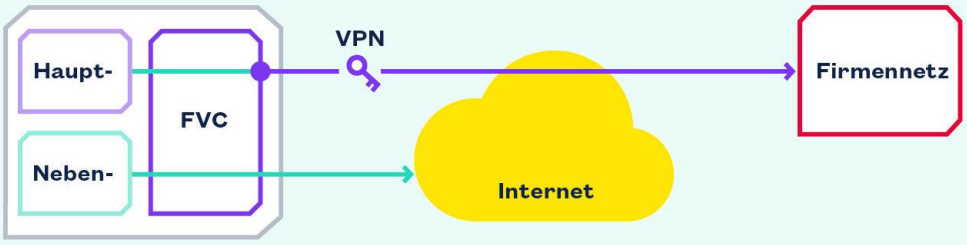
2.8. Einsatzszenarien und Zugriffsprofile

vs-top kann in unterschiedlichen Umgebungen zum Einsatz kommen: Unterwegs, zu Hause und am Arbeitsplatz im Unternehmen.

Die Anforderungen der unterschiedlichen Einsatzszenarien lassen sich über Zugriffsprofile erfüllen, also über unterschiedliche Firewall- und VPN-Konfigurationen für die beiden Nutzercompartments. Die Zugriffsprofile lassen sich wie bereits erwähnt in der zentralen Management-Lösung genucenter erstellen und einzelnen oder mehreren vs-tops gleichzeitig zuweisen. Dabei schließt die zentrale Management-Lösung Konfigurationen aus, bei denen Haupt- und Nebencompartment auf dasselbe Netz zugreifen.

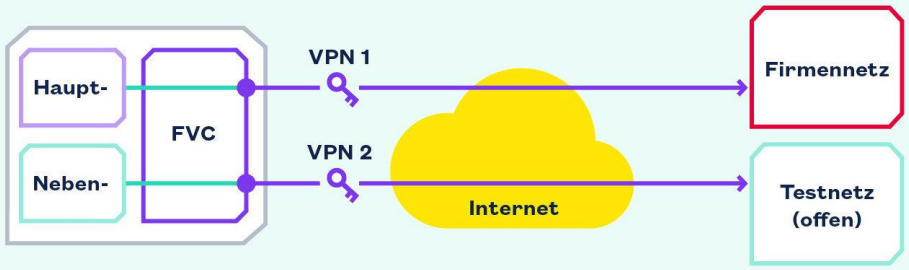
2.8.1. Einsatzszenario „Am Heimarbeitsplatz oder unterwegs“

Wird das Laptop außerhalb des Unternehmensnetzwerks als mobiler Arbeitsplatz verwendet, werden alle Verbindungen des Hauptcompartments per VPN verschlüsselt und authentifiziert. Das Nebencompartment kann dagegen unverschlüsselte Netzwerkverbindungen zu beliebigen Kommunikationspartnern aufbauen.



Zugriffsprofil mit einem VPN für mobile Nutzung

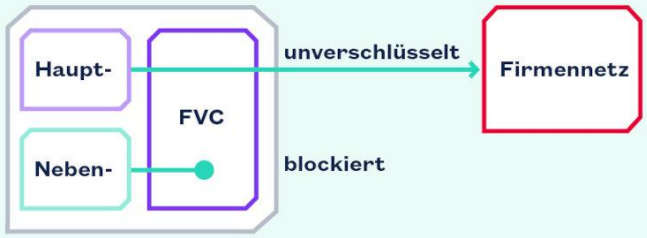
Mit einem alternativen Zugriffsprofil können beispielsweise beide Nutzercompartments ausschließlich über VPN-Tunnel mit unterschiedlichen Netzen kommunizieren: Das Hauptcompartment kommuniziert mit dem Firmennetz, das Nebencompartment mit einem Netzwerk, in dem keine vertraulichen Daten verarbeitet werden (z. B. Testnetz innerhalb einer Organisation).



Zugriffsprofil mit zwei VPN für mobile Nutzung

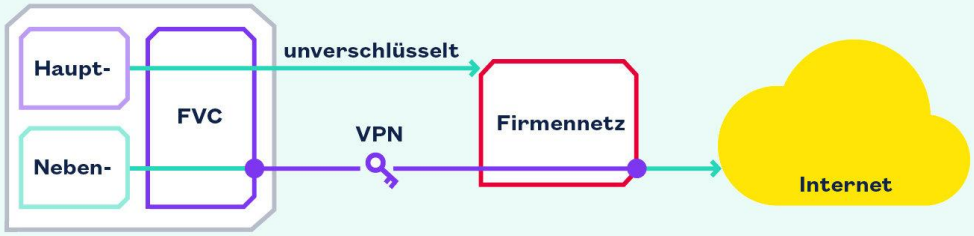
2.8.2. Einsatzszenario „Im Firmennetz“

Für den Fall, dass sich das Laptop im Firmennetz befindet, lassen sich Zugriffsprofile definieren, die direkte Netzwerkverbindungen des Hauptcompartments ohne VPN-Tunnel erlauben. Dazu verfügt das Firewall/VPN Compartment (FVC) über eine Funktionalität, die es erlaubt festzustellen, ob vs-top direkt an ein vertrauenswürdiges Firmennetz angeschlossen ist. Dies wird als Friendly Net Detection (FND) bezeichnet. Dazu muss ein FND-Server per SSH erreichbar sein. Für das Nebencompartment ist in diesem Fall die Kommunikation komplett blockiert.



Zugriffsprofil im Firmennetz, Nebencompartment-Kommunikation blockiert

Alternativ wird die Kommunikation durch einen VPN-Tunnel aus dem Firmennetz hinausgeleitet. So bleibt gewährleistet, dass das Nebencompartment keinen Zugriff auf das Firmennetz hat.



Zugriffsprofil im Firmennetz, Nebencompartment-Kommunikation verschlüsselt

2.9. Hardware

vs-top ist derzeit auf der Hardware HP EliteBook 830 G6 erhältlich (Stand Q2/2021).

Darüber hinaus unterstützt genua aktuell u. a. folgende Hardware:

- Fujitsu Lifebook U748
- Fujitsu Lifebook E746
- HP EliteBook 830 G5
- HP Elitebook 820 G3
- HP Probook 640 G2

Einen Überblick zu den aktuellen Hardware-Varianten inklusive technischer Daten finden Sie auf der Produkt-Webseite von genua: www.genua.de/vs-top

vs-top unterstützt unterschiedliche Hardware

3. Zulassung

vs-top ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen für die Geheimstufen VS-NfD, NATO RESTRICTED und RESTREINT UE/EU RESTRICTED. Mobile Mitarbeiter von Behörden, der Bundeswehr und geheimschutzbetreuter Unternehmen können mit dem Security Laptop somit eingestufte Daten verarbeiten.

4. Infrastruktur

4.1. Smartcard

Die Benutzer-Authentisierung für die Festplattenverschlüsselung sowie die Speicherung der Langzeitschlüssel für die VPN-Verbindungen erfolgt per Smartcard. Auf diese Weise ist das Schlüsselmaterial nicht nur geschützt, sondern kann auch vom Anwender aus dem Laptop entfernt werden, wenn dieser das Laptop gerade nicht verwendet.

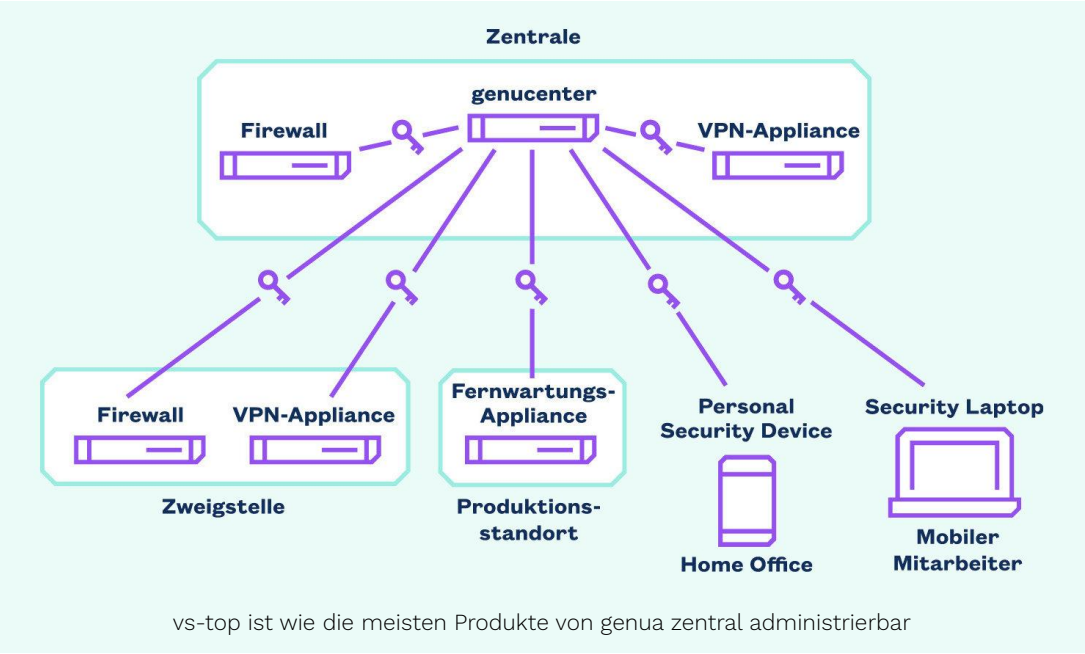
Das Entfernen der Smartcard versetzt vs-top in den Ruhezustand. Beim Resume muss die Festplatte erneut via Smartcard entschlüsselt werden.

Für den Fall, dass ein Anwender seine Smartcard verliert, können einem vs-top vom Administrator zusätzliche Smartcards zugeordnet werden, sodass sich mit diesen die Festplatte wieder entschlüsseln lässt.

Auf Anfrage besteht die Möglichkeit, bereits in der Organisation eingesetzte Smartcards mit vs-top zu verwenden.

4.2. Zentrale Management-Lösung

Rollout und Administration mehrerer Security Laptops erfolgen komfortabel mit der Central Management Station genucenter. Änderungen, Updates und Patches können über praktische Gruppierungs-Funktionen gleichzeitig auf beliebig viele Geräte übertragen werden.



vs-top ist wie die meisten Produkte von genua zentral administrierbar

Mit genucenter ist die konsequente Durchsetzung von Sicherheitsrichtlinien bezüglich Firewall und VPN-Einwahl bei allen Geräten möglich, die sich im internen und externen Einsatz befinden. In wachsenden Installationen können die zusätzlichen Laptops ganz einfach in die Central Management Station integriert und mit bewährten Konfigurationen ausgestattet werden.

4.3. VPN-Gateway

Als VPN-Gegenstelle bietet genua die Firewall & VPN-Appliance genuscreen mit VS-NfD-Zulassung und Zertifizierung nach Common Criteria (CC) EAL 4+ des Bundesamts für Sicherheit in der Informationstechnik. genuscreen lässt sich wie vs-top mit der zentralen Management-Lösung genucenter administrieren.

4.4. Kommunikationsserver

Da die Security Laptops gegebenenfalls nur über temporäre IP-Adressen verfügen oder von außen gar nicht erreichbar sind – etwa weil sie sich hinter einem NAT-Gateway befinden – muss die Verbindung von den Laptops aus aufgebaut werden. Damit die zentrale Management-Lösung nicht direkt an ein unsicheres Netzwerk wie das Internet angebunden werden muss, ist es im VS-NfD-Einsatz erforderlich, einen Kommunikationsserver in einer DMZ zwischenzuschalten.

Beim Kommunikationsserver handelt es sich um eine Firewall & VPN-Appliance genuscreen. Diese ist von außen erreichbar und ermöglicht den Security Laptops, die zur Administration erforderliche sichere Verbindung zur zentralen Management-Lösung genucenter herzustellen.

4.5. Optionaler Prägeserver

Hat eine Organisation keine eigenen Smartcards im Einsatz, die mit vs-top verwendet werden können, müssen diese zunächst initialisiert werden. Die Initialisierung erfolgt mit einem Prägeserver. Als Prägeserver dient die Firewall & VPN-Appliance genuscreen.

4.6. Optionaler Keyserver

Ab einer Stückzahl von etwa 1.000 Security Laptops und je nach Nutzerverhalten, empfehlen wir den Einsatz eines zentralen Keyservers zusätzlich zur zentralen Firewall & VPN-Appliance genuscreen, um Wartezeiten der Anwender zu vermeiden.

Der Keyserver übernimmt die Funktionalität der Smartcard des VPN-Gateways genuscreen und ist bei großen Setups schneller. Damit können z. B. VPN-Infrastrukturen mit einer vierstelligen Anzahl von Außenstellen pro VPN-Gateway genuscreen äußerst performant realisiert werden.

4.7. Optionaler Deployment Server

Wie die meisten Business Laptops wird auch vs-top nach den Anforderungen der jeweiligen Organisation eingerichtet. Dabei kann die Anforderung bestehen, dass die Provisionierung dezentral an verschiedenen Standorten erfolgt. In diesen Fällen werden die Geräte in einem dafür vorgesehenen Netzsegment mit einem Deployment Server verbunden, von dem sie ihre initiale Konfiguration sowie individuelle Schlüssel zur Festplattenverschlüsselung und zur Absicherung der Netzwerkkommunikation erhalten.

Dazu muss eine dauerhafte Verbindung zwischen genucenter und dem Deployment Server bestehen. Eine direkte Verbindung zwischen den Security Laptops und genucenter ist nicht vorgesehen.

Neben der initialen Provisionierung besteht eine weitere Herausforderung in der Update-Versorgung der vs-tops. Hierzu können weitere Deployment Server eingesetzt werden, die als Update-Server fungieren und von den vs-tops angefragt werden. Dies erlaubt einen asychronen Bezug von Updates, nachdem die neue Zielversion durch einen Administrator freigegeben wurde.

4.8. Optionaler FND-Server

Security Laptops können ein vertrauenswürdiges Netzwerk erkennen, um dem Anwender automatisch Zugriffsprofile anzubieten, die nur in dieser Umgebung erlaubt sind. Dazu ist eine als FND-Server konfigurierte Firewall & VPN-Appliance genuscreen erforderlich, die per SSH erreichbar sein muss.

5. Support

5.1. Installations- und Konfigurationsservice

genua und spezialisierte Vertriebspartner unterstützen Sie auf Wunsch bei der Installation, Konfiguration und Inbetriebnahme von vs-top und der Management Station genucenter. Dabei werden die Administratoren ausführlich in die Benutzung und Pflege des Systems eingewiesen.

5.2. Laufender Betrieb – Software Support

Hardwaregarantie: Im Kaufpreis der Security Laptops ist eine Standardgarantie zu den Bedingungen des Hardware-Herstellers inklusive. Dazu ergänzend bieten wir Ihnen eine optionale erweiterte Garantie- und Gewährleistung an.

Update Service: vs-top wird ständig weiterentwickelt. Unser Update-Service sichert Ihnen die automatische Lieferung der neuesten Versionen und Zugriff auf unsere komplette Patch-Datenbank.

Hotline: Zusätzlich zu unserem Update Service bieten wir deutsch- und englischsprachigen Support via Telefon und E-Mail. Sie können unsere Hotline für alle Fra-

gen zu Ihrer Lösung mit vs-top nutzen. Der telefonische Hotline Support steht Ihnen auf Wunsch 24 Stunden an sieben Tagen die Woche zur Verfügung.

5.3. Support von Vertriebspartnern

Support-Leistungen von Vertriebspartnern: Viele autorisierte Vertriebspartner von genua bieten zum Teil erweiterte Support-Optionen an, z. B. Vor-Ort-Austauschservice von Hardware innerhalb garantierter Maximalzeiten.

VT-WP-0721-9-D

genua GmbH

Domagkstraße 7 | 85551 Kirchheim bei München

T +49 89 991950-0 | F +49 89 991950-999 | E info@genua.de | www.genua.de