Mobile-Sicherheit –
Sicheres arbeiten von unterwegs mit Check Point Abra

Stefan Schurtz

Check Point Software Technologies Ltd. ist weltweit für seine Firewall- und VPN-Produkte bekannt und stellt mit Abra, einen USB-Stick für sicheres mobiles Arbeiten zur Verfügung

IN DIESEM ARTIKEL ERFAHREN SIE…

- Wie man mit Check Point Abra sichere Mobile-Arbeitsplätze für Mitarbeiter oder externe Dienstleister zur Verfügung stellen kann

WAS SIE VORHER WISSEN SOLLTEN…

- Kenntnisse in der System- und Netzwerk-Sicherheit
- Kenntnisse in der Konfiguration von Check Point Produkten
- Kenntnisse in der TCP/IP Netzwerktechnik

Heimarbeitsplätze bzw. Arbeiten von unterwegs ist seit Jahren eine wichtige Anforderung von Firmen an die IT und stellt nach wie vor eine große Herausforderung für die IT-Sicherheit dar.

Etabliert für den Zugriff von fremden/unsicheren Netzen und Systemen in ein Firmennetzwerk, haben sich Virtuelle Private Netzwerke per IPSec oder SSL-VPN. Der sichere Zugriff bzw. eine gesicherte Verbindung von Privat-/Fremdsystemen in das Unternehmensnetzwerk sind damit weitestgehend gewährleistet. Problematisch ist jedoch, dass kaum die Möglichkeit der Kontrolle besteht, beispielsweise bei externen Dienstleistern, was auf diesen Systemen installiert ist und/oder welche Verbindungen noch vorhanden sind. Auch die allgemeine Sicherheit (Patches usw.) dieser Systeme kann wohl kaum garantiert werden. Sicher wäre es ebenso nicht von Vorteil, wenn interne, womöglich vertrauliche Dokumente auf solchen Systemen abgespeichert und dann von Unbefugten gelesen oder gar kopiert werden.

Auf einem firmeneigenen Host-PC, lässt sich dem Problem der Sicherheit, der Systemupdates und aktivierter Virenscanner, möglicherweise noch mit einer Endpoint-Security entgegenwirken, doch den Anwender soweit Einzuschränken, dass ein Arbeiten von unterwegs kaum mehr möglich ist, wird früher oder später wohl eher problematisch und zu hitzigen Diskussionen führen.

Abra

Check Point stellt mit Abra, einen (**SanDisk)** FIPS 140-2 Level 2 zertifizierten USB-Stick zur Verfügung, welcher zum einem die Sicherheit der Daten auf dem Stick durch moderne Kryptographie (AES 256-bit hardware

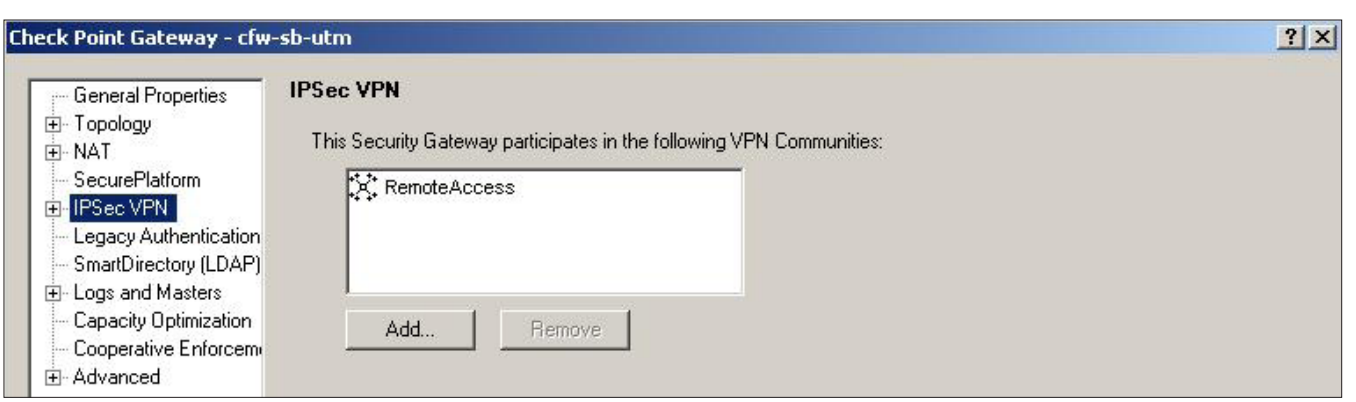

Abbildung 1. *Konfiguration der VPN-Community für RemoteAccess*

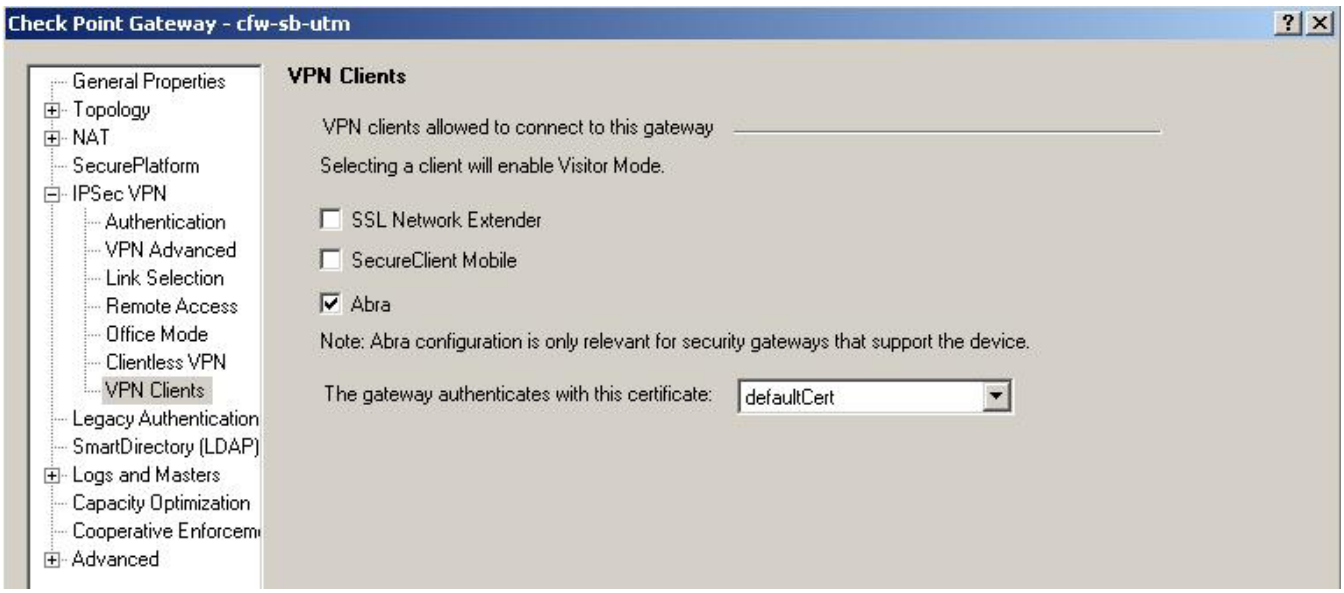

Abbildung 2. *Konfiguration der VPN Clients*

Abbildung 3. *Firewall-Regel für Abra Zugriff*

encryption), z. B. gegen Verlust oder Diebstahl sicherstellt und der zum anderen, einen passwortgeschützten „virtuellen", vom Host-PC getrennten, Arbeitsbereich (ohne Installation) zur Verfügung stellt.

Darüber hinaus, ist es durch das Einbinden in ein Check Point Management möglich, Einfluss auf den Import/Export von Dateien und auf die in der virtuellen Umgebung nutzbaren Anwendungen, zu nehmen. Diese konfigurierbare, so genannte „*Secure Workspace Policy*", bewirkt letztlich mehr Sicherheit für den Zugriff von Fremdsystemen und lässt dem Anwender trotzdem noch die Möglichkeit komfortabel von unterwegs zu arbeiten.

Secure Workspace Policy

Folgende Secure Workspace bzw. Endpoint Policy wird in diesem Artikel mit Hilfe von Abra umgesetzt:

Der Import bzw. Export von Dateien wird nur von und zu vertrauenswürdigen Systemen (Trusted Hosts – Host im internen Netz bzw. ein Host der sich einmal dort befunden hat) zugelassen. Das Drucken von Dokumenten sowie das Kopieren über die Zwischenablage wird nicht erlaubt. Ein Umschalten zwischen dem „Host-Desktop" und dem „Abra-Desktop" soll möglich sein. Darüber hinaus soll nach 60 Minuten Inaktivität ein automatischer Logout erfolgen.

Auf dem Host-PC wird geprüft ob Virenscanner, Anti-Spyware-Tools, Personal Firewalls, aktuelle Windows Service Packs und Windows Update vorhanden bzw. aktiviert sind. Entspricht der Host-PC diesen Sicherheitsanforderungen wird der Zugriff gestattet bzw. erhält der Anwender eine Warnung welche Anforderungen nicht erfüllt sind.

Sind bestimmte Kriterien nicht erfüllt, wird der Zugriff verweigert. So sind zum Beispiel eine fehlende Personal Firewall bzw. ein fehlendes Anti-Spyware-Programm, zwar ein Grund zur Warnung, der Zugriff wird dennoch gestattet. Bei fehlendem AntiVirus Programm, fehlendem aktuellen Windows Service Pack und/oder deaktiviertem Windows Update wird der Zugriff jedoch komplett verweigert.

Security Management

Damit überhaupt mit Abra gearbeitet bzw. eine VPN-Verbindung hergestellt werden kann, müssen auf dem Security Management folgende Vorbereitungen getroffen sein.

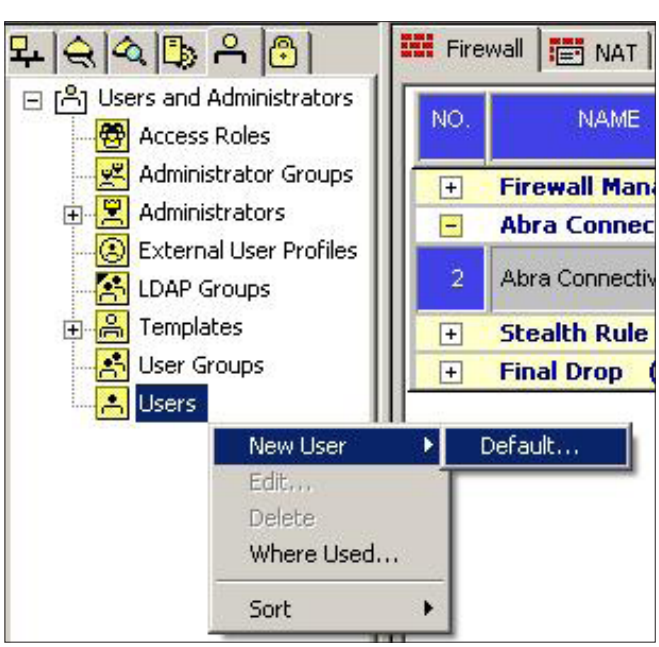

Abbildung 4. *Benutzer Konfiguration*

Abbildung 5. *Global Properties – Abra*

VPN

Im Check Point Gateway Objekt muss unter „*Network Objects -> Check Point -> Gateway Object → General Properties → Network Security*„ der Punkt „IPSec VPN“ aktiviert sein und das Objekt „*RemoteAccess*“ muss der VPN-Community angehören. Dies wird über „*Network Objects -> Check Point -> Gateway Object -> IPSec VPN*“ konfiguriert (Abbildung1).

Zum Abschluss der VPN Konfiguration auf dem Management, muss Abra als VPN-Client erst noch erlaubt werden, diese Einstellung nimmt man unter „*Network Objects -> Check Point -> Gateway Object -> IPSec VPN -> VPN Clients*“ vor (Abbildung2).

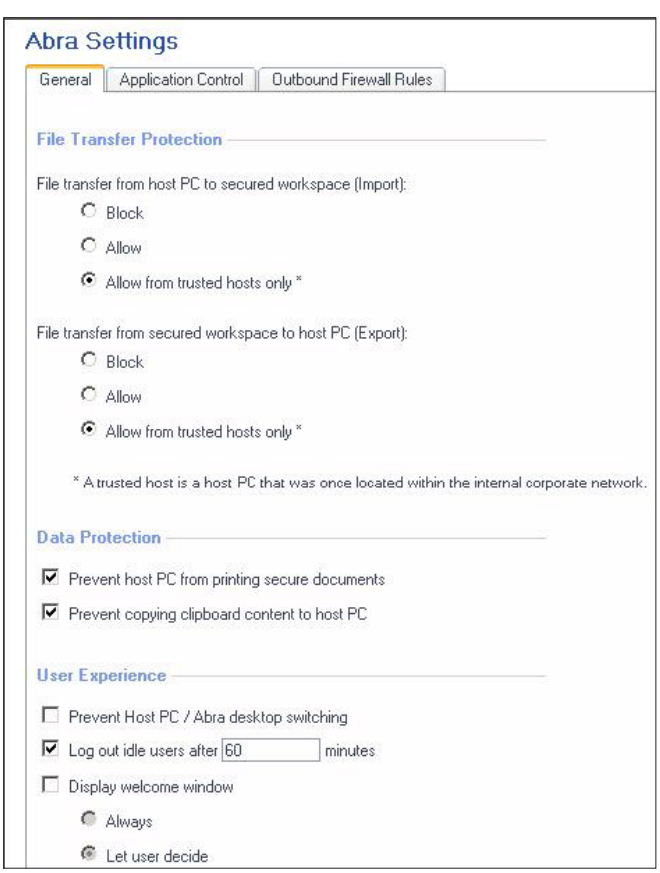

Abbildung 6. *General Abra Settings*

Firewall-Rule

Eine Firewall-Regel, welche HTTPS-Verbindungen auf das Security Gateway zulässt, muss ebenfalls

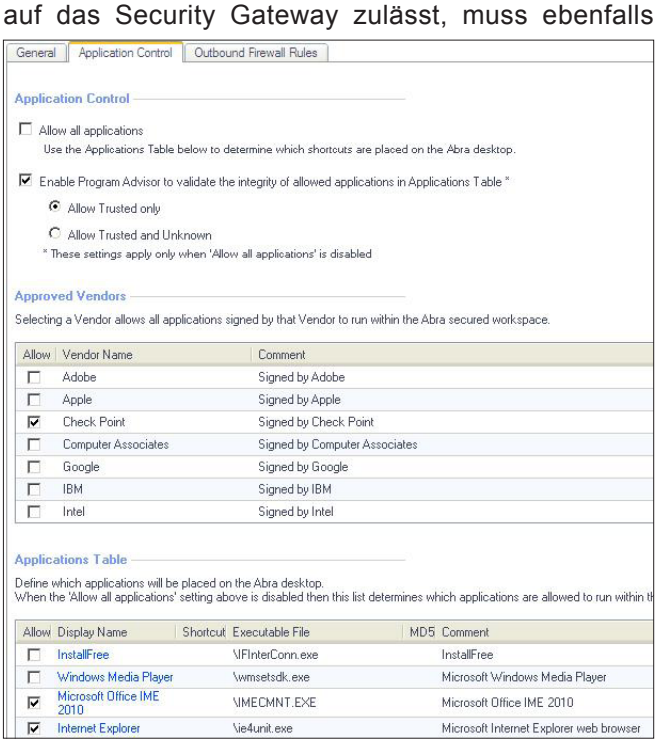

Abbildung 7. *Abra - Application Control*

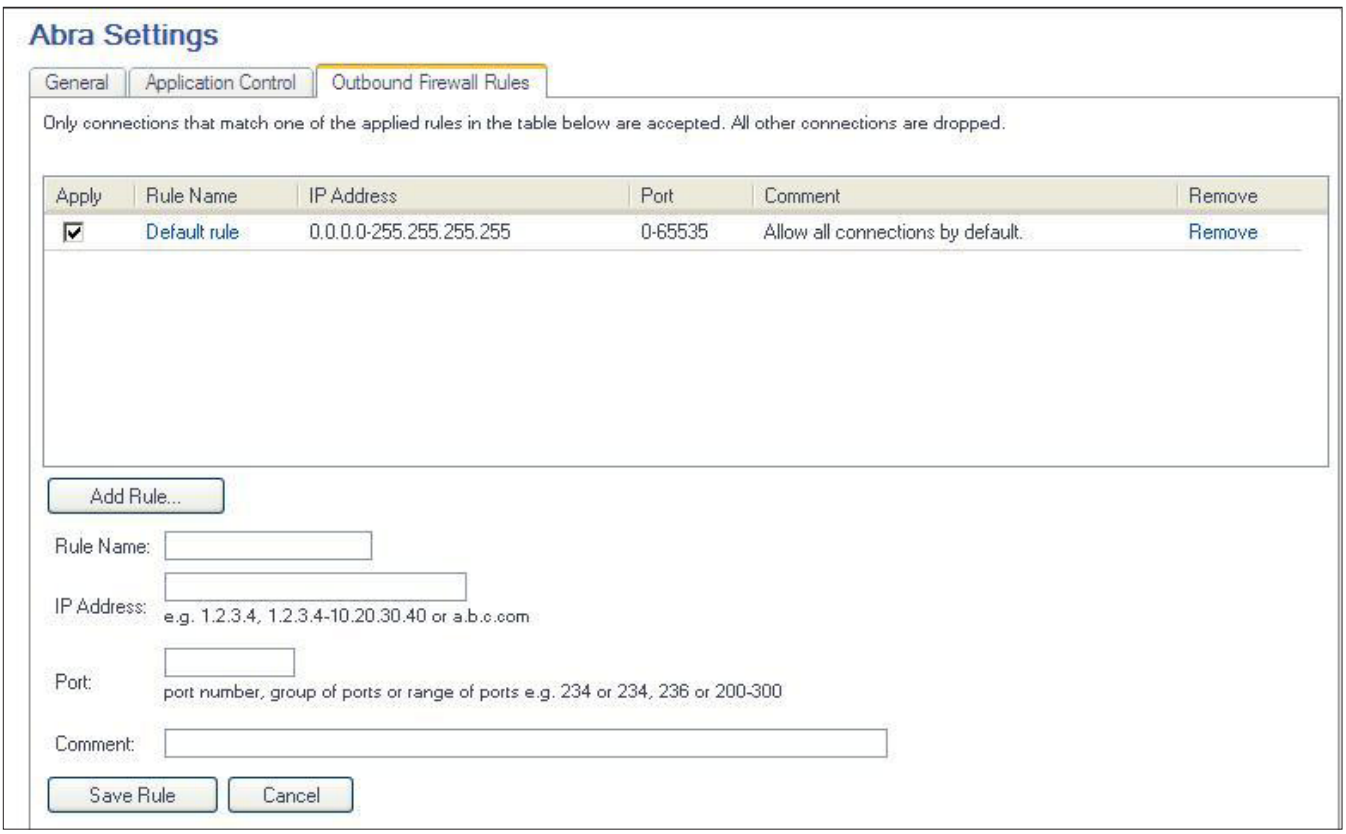

Abbildung 8. *Abra - Outbound Firewall Rules*

existieren, da diese von Abra genutzt werden (Abbildung 3).

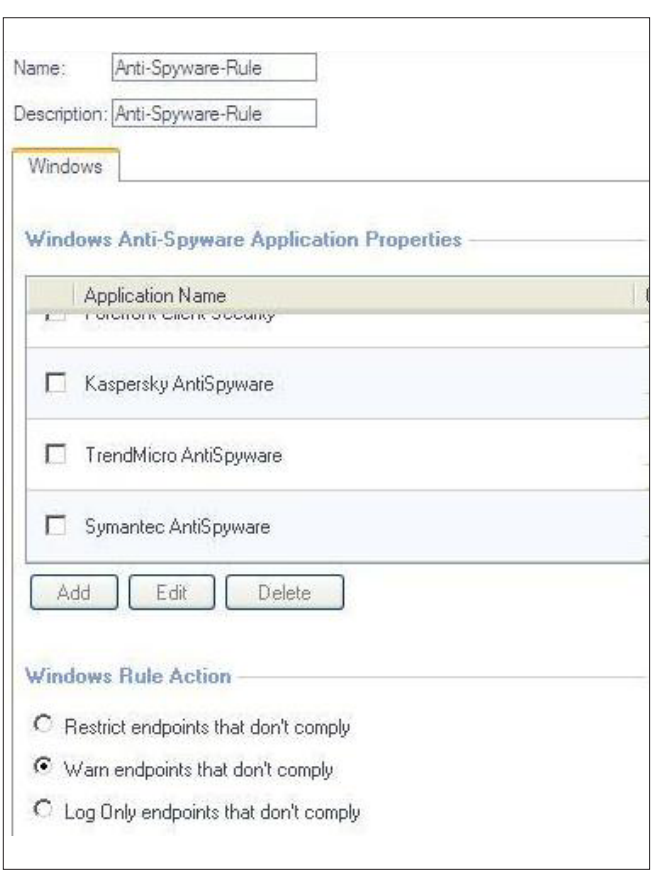

Abbildung 9. *Anti-Spyware Regel*

Benutzer anlegen

Damit sich ein Benutzer mit Abra per VPN zum Security Gateway verbinden kann, muss dieser auf dem Management angelegt sein. Die Konfiguration erfolgt über den Menüpunkt „*Users and Administrators -> Users*

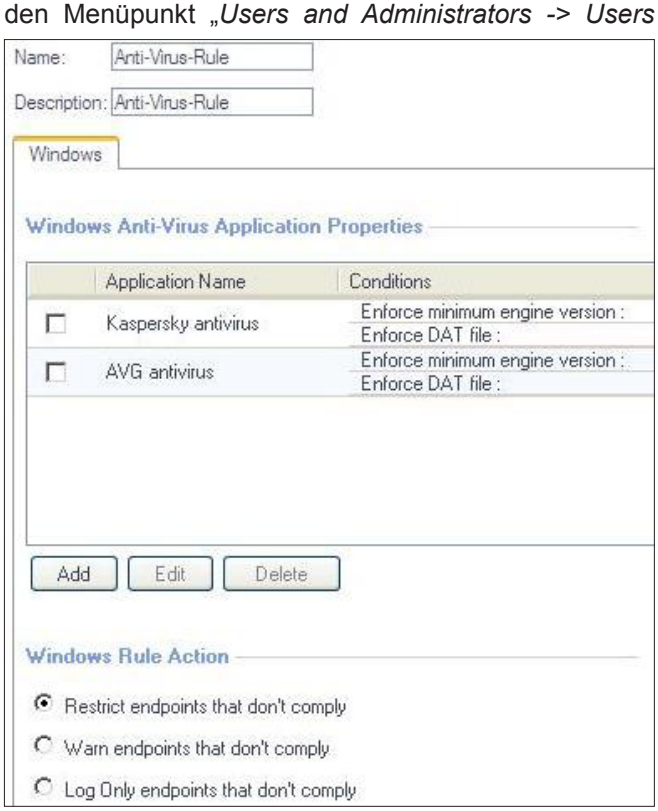

Abbildung 10. *Anti-Virus Regel*

-> Rechte Maustaste -> New User -> Default“ (Abbildung4).

Damit sind die Voraussetzungen für eine erfolgreiche VPN-Verbindung gegeben und es kann mit der Konfiguration der Secure Workspace Policy begonnen werden.

Secure Workspace Policy

Die Einstellungen der Secure Workspace Policy erfolgen im Check Point Management unter „*Policy -> Global Properties -> Abra -> Secure Workspace Policy*“ (Abbildung5).

General

Unter *General* werden die beiden Punkte „*File transfer from host PC to secure workspace (Import)*“ und „*File transfer from secured workspace to host PC (Export) auf „Allow from trusted hosts only*“ gestellt. Unter „*Data Protection*“ wird „*Prevent host PC from printing secure documents*“ und „*Prevent copying clipboard content to host PC*“ aktiviert. Der Punkt „*Log out idle users after*“, unter „*User Experience*“ wird auf 60 Minuten eingestellt. Alle weiteren Punkte werden deaktiviert. (Abbildung 6)

Application Control

Unter *Application Control* wird der „*Program Advisor*“ aktiviert und auf „*Allow Trusted only*“ eingestellt. Des Weiteren wird unter den „*Approved Vendors*“ nur Check Point zugelassen. In der Liste „*Applications Table*“ werden, alle Anwendungen, außer Office- und Browser-Anwendungen, deaktiviert (Abbildung7).

Abbildung 11. *Compliance Report*

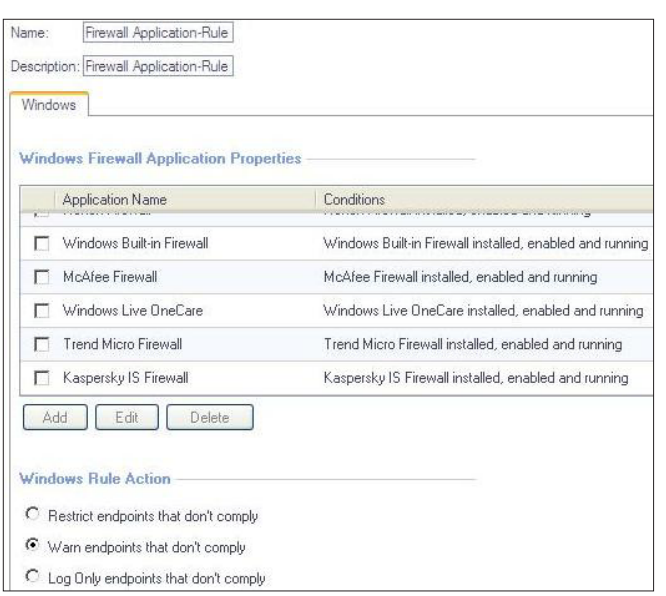

Abbildung 12. *Firewall-Application Regel*

Outbound Firewall Rules

Mit den *Outbound Firewall Rules* werden (ausgehend) erlaubte Verbindungen zu IP-Adressen und Ports konfiguriert, welche von den Anwendungen im Secure Workspace genutzt werden dürfen, alle anderen werden verworfen (Abbildung8).

Scan Endpoint for spyware and Compliance

Die Regeln zur Prüfung des Host-PC, unter anderem, nach installierten Virenscannern, Personal Firewall und Windows-Update werden unter dem, zuvor aktivierten, Menüpunkt „Scan endpoint for spyware and compliance → Configure“ eingerichtet.

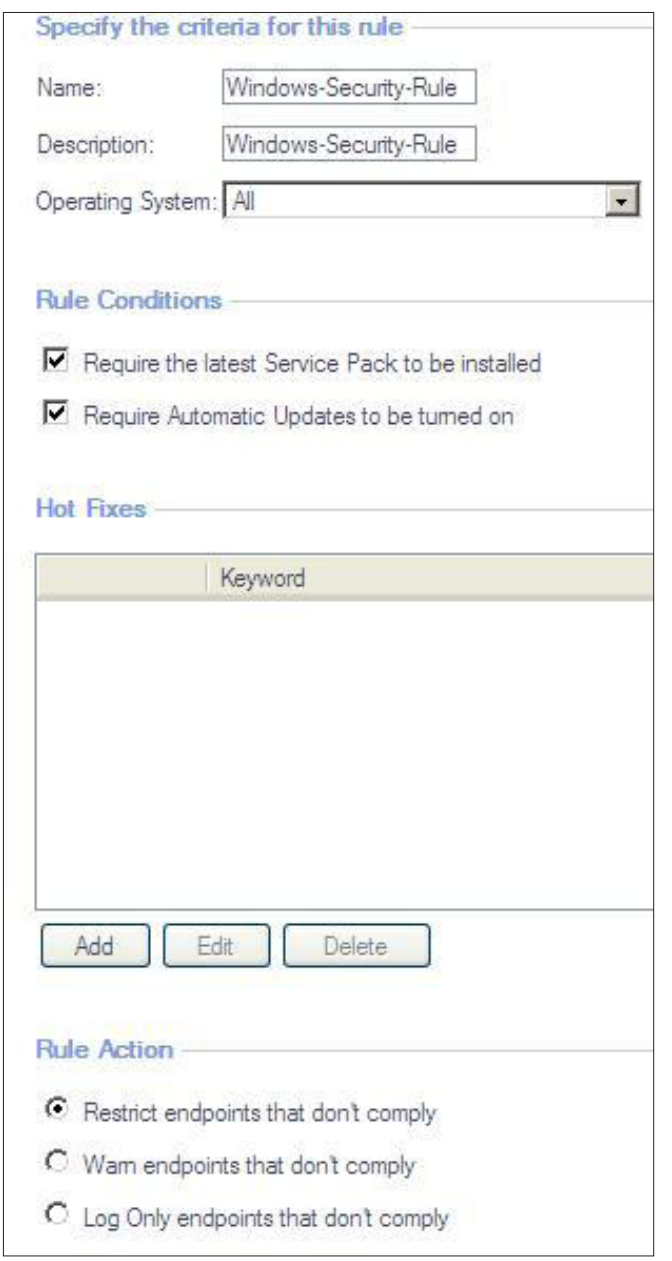

Abbildung 13. *Windows-Security Regel*

Anti-Spyware-Rule

Zur Konfiguration der Anti-Spyware Rule wählt man den Punkt „*Scan endpoint for spyware and compliance -> Configure -> New Rule -> Anti-Spyware Application*“ aus. Neben dem Namen für die Regel, werden unter dem Punkt „*Windows Anti-Spyware Application Properties*“ nun alle zur Verfügung stehenden Anwendungen ausgewählt und der Punkt „*Windows Rule Action*“ auf „*Warn endpoints that don´t comply“* gestellt (Abbildung9). Damit wird nun bei fehlenden Anti-Spyware-Anwendungen, im Compliance Report, eine Warnung an den Benutzer ausgegeben, der Zugriff aber trotzdem gestattet.

Abbildung 14. *Abra - First Time Configuration Wizard*

Abbildung 15. *Abra - Lizenzbestimmungen*

Abbildung 16. *Abra - Passwort Eingabe*

Anti-Virus-Rule

Die Anti-Virus Regel wird per „*Scan endpoint for spyware and compliance -> Configure -> New Rule -> Anti-Virus Application*“ angelegt. Diese wird auf die beiden Virescanner „*Kaspersky antivirus*“ und „*AVG antivirus*“ eingeschränkt. Im Gegensatz zur Anti-Spyware-Rule wird diese Regel allerdings auf „*Restrict endpoints that don't comply*“ gestellt (Abbildung10). Damit wird, ist keiner der beiden Virenscanner auf dem Host-PC installiert, der Zugriff verweigert (Abbildung11).

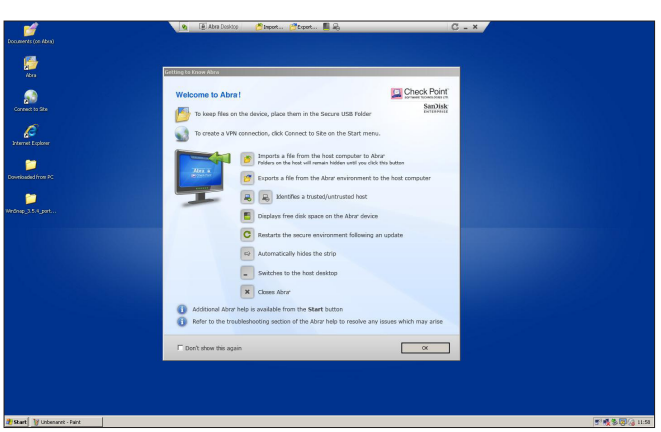

Abbildung 17. *Abra - Secure Workspacce*

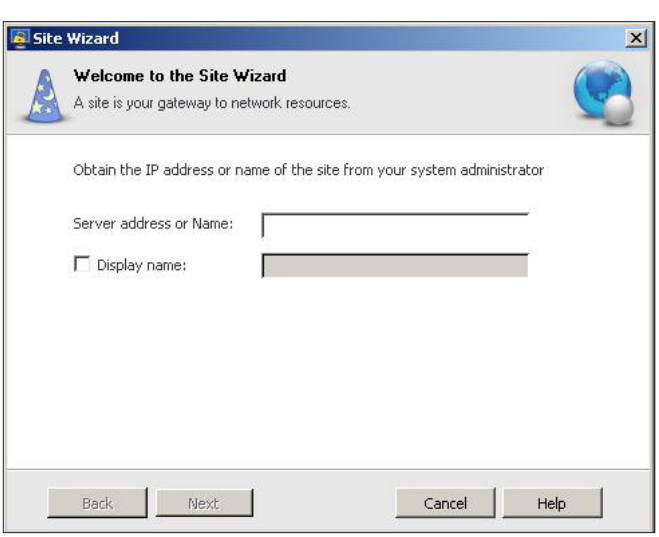

Abbildung 18. *Site Wizard – IP / Hostname Konfiguration*

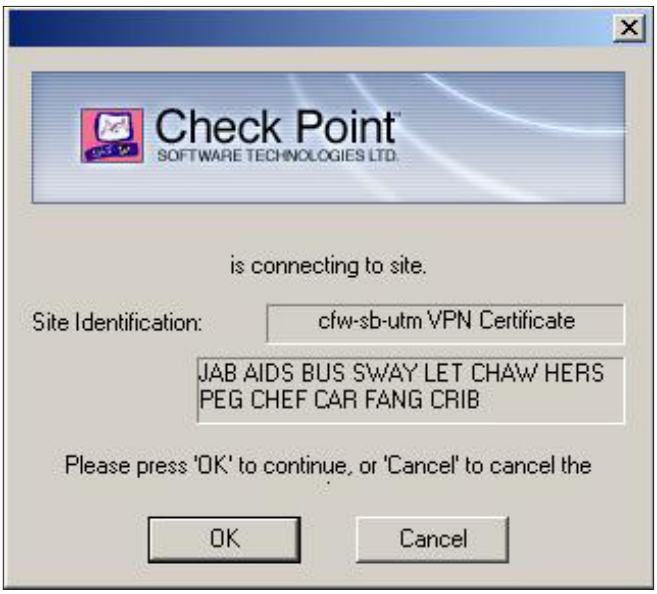

Abbildung 19. *Site Wizard – Fingerprint*

Abbildung 20. *Site Wizard – Authentication Method*

Firewall-Application-Rule

Analog zu den beiden oben erstellten, wird als vorletztes, eine Regel für Firewall-Applications über „*Scan endpoint for spyware and compliance -> Configure -> New Rule -> Firewall Application*“ erstellt. Bei dieser Regel werden ebenfalls alle vorhandenen Anwendungen hinzugefügt und die Windows Rule Action auf „Warn endpoints that don't comply gestellt (Abbildung12).

Windows-Security-Rule

Als letzte Regel wird die Windows-Security-Rule über „*Scan endpoint for spyware and compliance -> Configure -> New Rule -> Windows Security*“ erstellt und lediglich die beiden Punkte „*Require the latest Service Pack to be installed*“ und „*Require Automatic Updates to be turned on*“ aktviert. Die Rule Action wird auf „*Restrict endpoints that don´t comply*“ gestellt (Abbildung13).

Da nun die zuvor definierte Secure Workspace Policy umgesetzt wurde, wird im nächsten Schritt die eigentliche Konfiguration des Abra-Stick in Angriff genommen.

Installation

Nach dem Verbinden mit dem Host-PC und dem Ausführen der „Abra.exe“ auf dem USB-Stick, starte der „Abra First Time Configuration Wizard“ (Abbildung14). Nach dem Bestätigen der Lizenzbestimmungen (Abbildung15) muss im nächsten Schritt das Passwort für den Abra-Stick eingegeben werden. Hierzu steht zum Schutz vor Keyloggern ein „Virtual Keyboard“ zur Verfügung (Abbildung16). Nach der Eingabe eines sicheren Passwortes, wird das Device initialisiert und der Secure Workspace automatisch gestartet (Abbildung17).

VPN

Im Secure Workspace startet mit einem Klick auf „*Connect to Site*“ die Konfiguration für VPN mit der Abfrage von IP bzw. Hostnamen des Security Gateways (Abbildung18). Nach der Bestätigung des Fingerprints (Abbildung19), steht zuletzt die Auswahl der „*Authentication Method*“ an, in diesem Fall „*Username and Password*“ (Abbildung20). Ist das VPN erfolgreich erstellt, erscheint eine entsprechende Meldung und im nächsten Fenster werden zum endgültigen Abschluss der VPN-Konfiguration, Benutzername und Passwort abgefragt (Abbildung21).

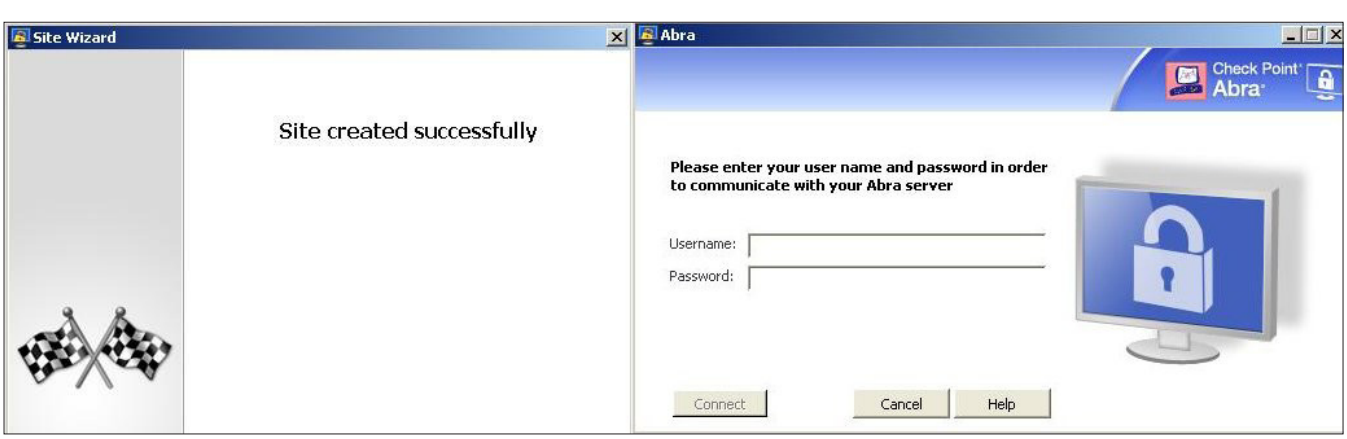

Abbildung 21. *Site Wizard – Erfolgreiche Konfiguration / Login*

ExmpSrv.exe	2448	54.676 K	52.840 K Application login	SanDisk
PWClient.exe	412	5.856 K	7.456 K Check Point Abra Controller	Check Point Software Technologies
PWAccess.exe	4248	15.452 K	15.172 K Check Point Abra VPN Client	Check Point Software Technologies
VDeskSelector.exe	5568	3.824 K	672 K Auxiliary Abra Module	Check Point Software Technologies
VDesk.exe	4656	10.312 K	14.128 K Virtual Workspace	Check Point Software Technologies
ISWMGR.exe	5604	24.004 K	32.544 K Abra Core	Check Point Software Technologies
ISWMGR.exe	5880	24.176 K	1.076 K Abra Core	Check Point Software Technologies
explorer.exe	5036	33.196 K	38.060 K Windows Explorer	Microsoft Corporation
ctfmon.exe	1124	15.456 K	11.336 K CTF Loader	Microsoft Corporation
PWViewer.exe	3652	31.072 K	34.360 K Check Point Abra VPN Client UI	Check Point Software Technologies
imapi.exe	2672	15.680 K	11.496 K Image-Mastering-API	Microsoft Corporation
DH.exe	5216	3.008 K	5.512 K Drive hide utility	SanDisk

Abbildung 22. *Abra im ProcessExplorer*

Abbildung 23. *Abra verbietet die Ausführung einer Anwendung*

Arbeiten im Secure Workspace

Sind alle diese Schritte erfolgreich abgeschlossen, steht der Arbeit per Abra im Secure Workspace nichts mehr im Wege. Durch das gewohnte „Look and Feel“ (im Grunde wird eine Windows Explorer.exe ausgeführt - Abbildung22), kann sich der Anwender schnell mit der neuen Umgebung vertraut machen.

Dennoch müssen einige Dinge beachtet werden, so stehen einem im Windows Explorer, wie gewohnt Laufwerke, Dateien und Ordner zur Verfügung, tatsächlich ist dies aber nur ein „virtuelles Abbild“ der „echten“ Host-PC Umgebung! Im Secure Workspace können Dateien, wenn die Policy die entsprechende Anwendung erlaubt (Abbildung23), des Host-PC geöffnet, scheinbar sogar gelöscht bzw. verändert werden. Dies hat jedoch (hoffentlich ;D) *KEINE* Auswirkungen auf die „echte“ Umgebung des Host-PC. Das bedeutet für einen Benutzer, dass Dateien *NUR* über die Funktionen Import/Export auf bzw. von dem Host-PC kopiert werden können.

Auch hängt ein vernünftiges Arbeiten natürlich davon ab, dass die erlaubten und benötigten Anwendungen auf dem Host-PC verfügbar sind, d. h. Einschränkungen sollten mit Bedacht durchgeführt werden und es

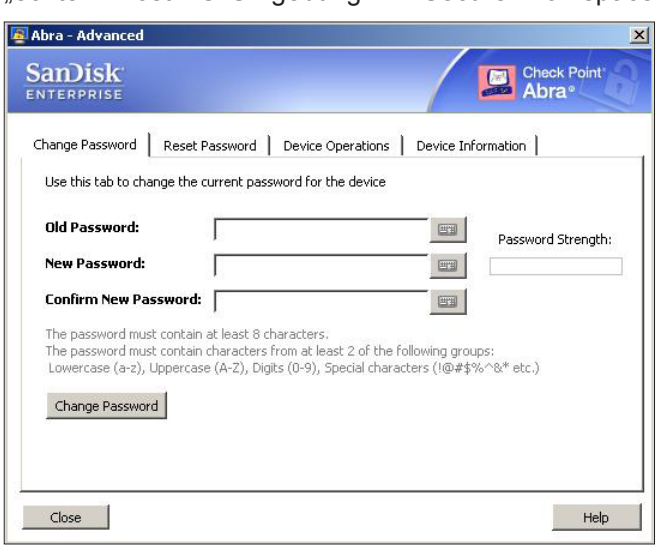

Abbildung 24. *Abra Advanced – Change Password*

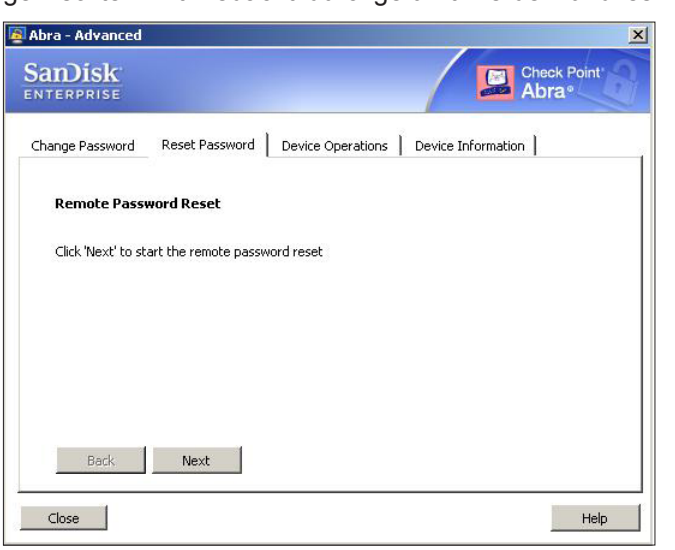

Abbildung 25. *Abra Advanced – Remote Password Reset*

sollten ebenfalls auch mögliche Alternativen, z. B. Microsoft Office ↔ Open Office, erlaubt werden.

Abra Advanced

Unter den erweiterten Einstellungen besteht unter „*Change Password*“, für den Benutzer, die Möglichkeit der „lokalen“ Passwortänderung (Abbildung24). Mit dem Reiter „*Reset Password*“ (Abbildung25) kann,

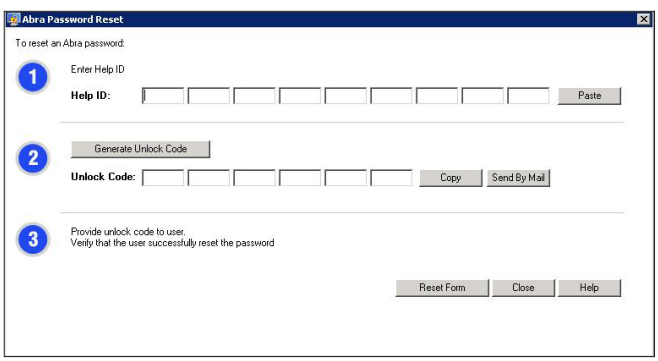

Abbildung 26. *Abra Advanced – Device Operations*

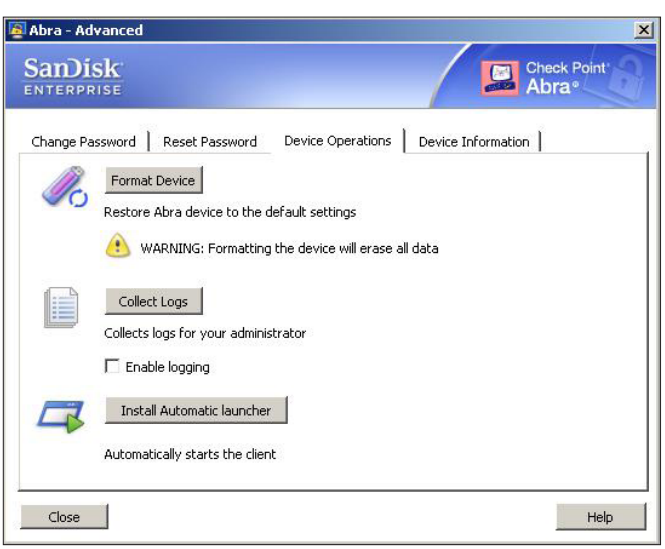

Abbildung 27. *Abra Advanced – Device Information*

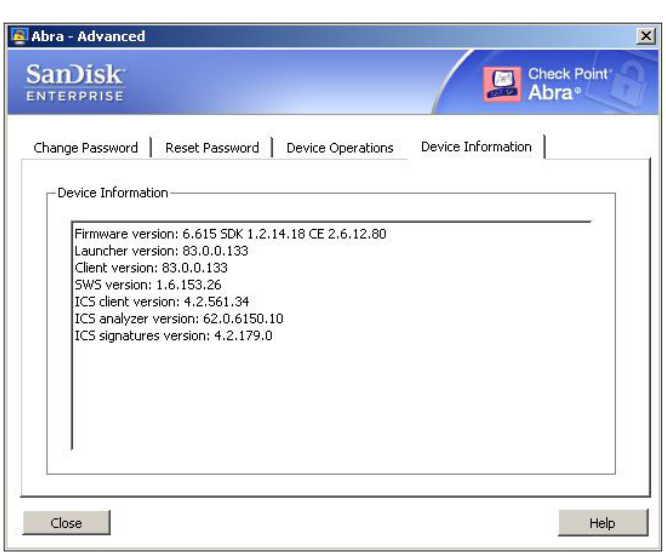

Abbildung 28. *xxxxxxx*

Im Internet

- *http://www.checkpoint.com/products/abra/*
- Abra R70.1 Administration Guide - *http://downloads.checkpoint.com/dc/download.htm?ID=11175*
- Abra R70.1 User Guide - *http://downloads.checkpoint.com/dc/download.htm?ID=11176*

sollte das Passwort vergessen werden, mit Hilfe des Supports und dem „Abra Password Reset“-Tool (Abbildung26), dieses zurücksetzt werden .

Unter den „*Device Operations*“ ist einmal mit „*Format Device*“ das komplette Zurücksetzen des USB-Sticks möglich, darüber hinaus kann hier ein Logging unter „*Collect Logs*“ aktiviert werden. Mit der letzten Konfigurationsmöglichkeit „*Install Automatic launcher*“ ist es möglich Abra automatisch starten zu lassen (Abbildung27).

Zu guter Letzt stehen unter „*Device Information*“, wie der Name vermuten lässt, Informationen unter anderem zur Firmware, Launcher und Client Version zur Verfügung (Abbildung28).

Fazit

Sicherheit bedeutet für Anwender oft Einschränkungen beim Arbeiten, dieses Problem wird auch durch Abra nicht vollständig gelöst. Jedoch kann man in Absprache mit Benutzern, Dienstleistern und einer vernünftigen durchdachten Policy einen guten Kompromiss, für einen sicheren mobilen Arbeitsplatz, schaffen.

STEFAN SCHURTZ

Der Autor arbeitet bei einem saarländischen ISP im Bereich Netzwerk-Sicherheit und beschäftigt sich auch privat mit dem Thema IT-Security

Kontakt mit dem Autor: sschurtz@t-online.de