Alle Zugriffswege abgesichert

Dr. Götz Güttich

Mit Pulse Connect Secure bietet PulseSecure eine VPN-Lösung der Enterprise-Klasse für mobile Geräte und Desktops unter Android, ChromeOS, iOS, Linux, MacOS und Windows, die einen einfachen und sicheren Zugriff von jedem Endpoint auf Anwendungen und Ressourcen im Unternehmen sicherstellen soll. Dabei ist es unerheblich, ob diese im Rechenzentrum, in der privaten Cloud, der öffentlichen Cloud oder als SaaS zur Verfügung stehen. Wir haben uns im Testlabor angesehen, wie die Arbeit mit diesem Produkt für den hybriden Secure Access abläuft.

Pulse Connect Secure arbeitet als Appliance oder als virtuelle Appliance im Unternehmensnetz und regelt den Zugriff der Anwender von externen Netzen auf die vorhandenen Dienste. Bei Bedarf ist es auch möglich, das Produkt in einer Private oder Public Cloud (AWS oder Azure) zu betreiben. Damit alle Benutzer jederzeit die Services ihrer Organisation verwenden können, bietet die Lösung eine große Zahl an Funktionen. Dazu gehören der Schutz von Anwendungen und Daten, die sich an beliebigen Orten befinden, einschließlich SaaS-Applikationen wie Office 365. Dazu kommen außerdem der Clientenlose Zugriff über ein Web-Interface, die Integration von Diensten wie Active Directory und LDAP sowie Unterstützung für Zwei- Faktor- Authentifizierung, SAML 2.0, PKI und IAM beziehungsweise digitale Zertifikate.

Ein so genannter Host Checker, der sicherstellt, dass das sich verbindende Gerät den Security-Anforderungen des Unternehmens entspricht, gehört ebenfalls zum Leistungsumfang. Dazu stuft das System die Endgeräte vor der Authentifizierung anhand vordefinierter Policies ein und lässt den Zugriff nur zu, wenn die in den Policies festgelegten Bedingungen erfüllt werden. Dazu kommen noch ein sicherer Zugriff auf die Virtual Desktop-Lösungen (VDI) der führenden Hersteller (Citrix XenApp/XenDesktop und Vmware Horizon), ein granulares Auditing zum Sicherstellen der Compliance, die Integration von Mobile Device Management-Produkten (MDM) und ein universeller Client für den Einsatz sowohl remote als auch onsite, um ein problemloses Roaming sicher zu stellen. Das Management der Lösung erfolgt über ein zentrales Web-Interface.

Konkret arbeitet Pulse Connect Secure als Layer 3-, 4- und 7-SSL VPN mit granularer Zugriffsteuerung und als Application VPN, das den Verkehr zwischen spezifischen Anwendungen bestimmten Zielen tunnelt. Es existiert auch ein IPSec/IKEv2 Support für mobile Geräte. Dazu kommen noch Split Tunneling-Features, Authentifizierungen über Hardware Token, Smart Cards, Soft Token, One Time-Passwords und Zertifikate sowie RDP-, Telnet- und SSH-Sitzungen auf Basis von HTML5. Eine granulare SSL Cipher-Konfiguration ist ebenfalls möglich.

Der Test

Im Test installierten wir in unserem Netz eine virtuelle PCS-Appliance, konfigurierten sie und griffen anschließend über das von ihr bereitgestellte VPN auf unsere Backend-Dienste zu. Außerdem nahmen wir die Authentifizierung mit einem lokalen Benutzerkonto, die Zwei-Faktor-Authentifizierung mit einem lokalen Benutzerkonto und einem One-Time-Passwort über Google Authenticator und das Host Checking sowie das Enterprise Onboarding unter die Lupe. Zu-

dem arbeiteten wir mit verschiedenen Connection Sets und analysierten das Konfigurationswerkzeug mit seinem Funktionsumfang und seinen Wizards.

Installation

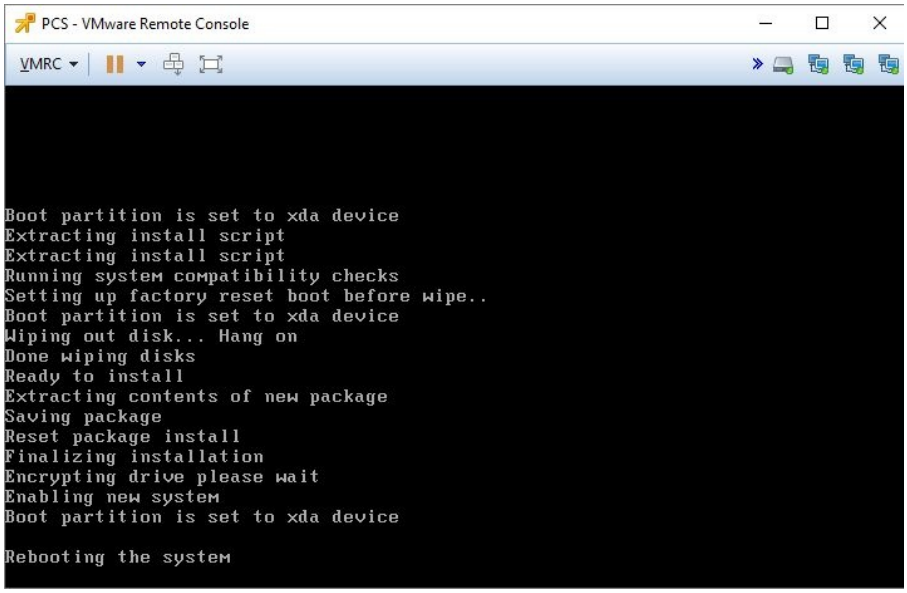
Die Installation der virtuellen Appliance gestaltet sich verhältnismäßig einfach. PulseSecure stellte uns zu diesem Zweck eine vorkonfigurierte Virtuelle Maschine (VM) im OVF-Format zur Verfügung, die wir auf einem Vmware ESXi-Host importierten, der unter Version 6.7 lief. Dieser Host arbeitete mit 32 GByte RAM und einer Intel i7-CPU mit acht Kernen. Für die VM benötigten wir allerdings nur vier GByte Arbeitsspeicher und zwei virtuelle CPUs. Nachdem wir die VM nach dem Import eingeschaltet hatten, mussten wir lediglich das License Agreement akzeptieren und die Netzwerkkonfiguration für den internen Port angeben. Außerdem war es noch erforderlich, ein Konto für den Administrator zu definieren und die Informationen zum Erzeugen eines Self Signed-Certificate für den Web Server anzugeben, also den Common Name und den Organization Name. Sobald das erledigt und die Installation durchgelaufen war, was ein paar Minuten in Anspruch nahm, konnten wir über die URL "https://{IP-Adresse der Appliance}/admin" auf das Verwaltungsinterface der Lösung zugreifen. Bei diesem meldeten wir uns nun mit dem zuvor definierten Administratorkonto an, nahmen die Zeiteinstellungen vor und fügten dem System die uns vom Hersteller bereitgestellte Testlizenz hinzu. Danach spielten wir noch einen Patch ein, um die Installation auf die zum Testzeitpunkt aktuelle Version 9.0R1 zu bringen, damit war das Setup abgeschlossen und wir konnten mit dem Test beginnen.

Erstkonfiguration

Um unser System in Betrieb zu nehmen, machten wir uns zu diesem Zeitpunkt daran, diverse Benutzerkonten anzulegen, die aus dem WAN auf unterschiedliche Ressourcen in unserem LAN zugreifen durften. Dazu erzeugten wir zunächst die Accounts, definierten dann die freigegebenen Ressourcen wie Web-Applikationen, Shares und SSH-Zugänge und legten zum Schluss fest, wer welche Ressource nutzen konnte. Die Konfiguration dieser Punkte gestaltet sich verhältnismäßig einfach, da der Hersteller einen Guide für die Erstkonfiguration in das Web-Interface integriert hat, den man lediglich abarbeiten muss.

Der erste Konfigurationsschritt besteht darin, einen Authentifizierungs-Server festzulegen. An dieser Stelle unterstützt das System neben einer lokalen Authentifizierung, bei der die Benutzerdaten direkt auf der PCS-Appliance gespeichert werden, auch das Microsoft Active Directory, sowie Authentifizierungen über NIS, ACE, LDAP, Radius, SiteMinder, SAML, MDM-Dienste und vieles mehr.

Im Test richteten wir erst einmal einen lokalen Authentifizierungsserver direkt auf der Appliance ein. Bei der Konfiguration dieses Servers haben die Administratoren unter anderem die Möglichkeit, die Länge und Zusammensetzung der von den Benutzerkonten verwendeten Passwörter vorzugeben. Außerdem sind sie bei Bedarf dazu in der Lage, den Benutzern zu verbieten, ihr Passwort zu ändern. Während der Definition des lokalen Authentifizierungsservers richteten wir im Test auch gleich die ersten beiden Benutzerkonten mit Namen und Passwörtern ein, wobei es zu keinen Überraschungen kam.

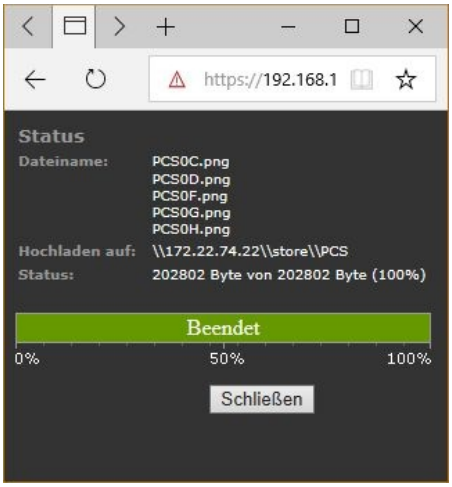


Die virtuelle Appliance während des Installationsvorgangs

Die Benutzerrolle

Im nächsten Schritt ging es an die Definition der Benutzerrolle. Über die User Roles definiert PulseSecure Sitzungsparameter wie Session Settings, Personalisierungseinstellungen (wie Benutzer-Bookmarks, die auf frei-

gegebene Ressourcen verweisen) und Zugriffsfunktionen. Bei den Zugriffsfunktionen legt die Benutzerrolle lediglich fest, welche Ressourcen ein User nutzen kann, wie beispielsweise SSH-Zugriffe oder Web-Anwendungen. Sie definiert aber nicht, mit



Die PulseSecure-Lösung nach dem Hochladen von Dateien auf ein Windows-Share

welchen Servern genau die Anwender kommunizieren können, diese Konfiguration führten wir später im Rahmen der Ressource Profiles durch. Im Test gaben wir unserer Benutzerrolle einen Namen, legten fest, dass Zugriffe via Web, SSH und Windows Shares freigegeben werden sollten und definierten einen Timeout. Zu den sonstigen Ressourcen, die das System an dieser Stelle anbietet, gehören NFS Shares, Telnet, Terminaldienste, virtuelle Desktops, VPN-Tunnel, HTML5 und ähnliches. Im Rahmen der Rollendefinition sind die zuständigen Mitarbeiter auch dazu in der Lage, vorzugeben, ob die Anwender Roaming nutzen dürfen (also ob es erlaubt ist, den Zugangspunkt während der Arbeit zu wechseln) oder nicht.

Der User Authentication Realm

Der nächste Konfigurationsschritt befasst sich mit dem User Authentication Realm. Als Authentifizierungsserver für diesen Realm verwendeten wir die zuvor erstellte lokale Authentifizierung. Außerdem definierten wir zu diesem Zeitpunkt auch unsere Role Mapping Rules. Diese legen beispielsweise fest, welcher User welche Benutzerrollen zugewiesen bekommt. In unserem Fall erzeugten wir eine Regel, die sicherstellte, dass der User "gg" mit unserer gerade erzeugten User Role arbeiten konnte. Die Role Mapping Rules arbeiten aber nicht nur mit Benutzernamen, sondern ermöglichen auch die Zuweisung von Rollen über Zertifikate oder Ausdrücke eine Zeichenkette. Das System ist also sehr flexibel.

Die Ressource Profiles

Sobald wir mit der Definition unseres Test-Realms fertig waren, wandten wir uns der Konfiguration unserer Ressource Profiles zu. Diese legen – wie bereits angesprochen – fest, auf welche konkreten Ressourcen die Benutzer zugreifen können. Im Test erzeugten wir zunächst ein Ressource Profile, das den Zugriff auf den bei uns im lokalen Netz arbeitenden Netzwerk Monitoring-Server PRTG von Paessler freigab. Da dieser über ein Web-Interface verwaltet wird, selektierten wir an dieser Stelle den Ressourcen-Typ "Web App". Für unsere Web App-Regel war es erforderlich, einen Namen sowie die zu verwendende URL anzugeben und die Regel unserer Benutzerrolle zuzuweisen. Außerdem müssen die zuständigen Mitarbeiter einen Typ angeben, an dieser Stelle stehen unter anderem "Custom", "Citrix", "OWA", "Lotus Notes" und "Sharepoint" zur Verfügung. Nachdem das erledigt war, konnten wir uns mit Hilfe eines Test-Clients unter Windows 10 über die externe Schnittstelle der PCS verbinden, uns mit einem zuvor angelegten Test-Benutzerkonto anmelden und anschließend auf den PRTG-Server im lokalen Netz zugreifen.

Weitere Bookmarks

Auf die gleiche Art und Weise fügten wir dem System anschließend auch noch den angesprochenen SSH-Zugriff auf einen Linux-Server im lokalen Netz und ein Windows-Share hinzu. Bei dem Share fragte die Appliance nach dem Verbindungsaufbau noch nach den Zugriffsdaten zum Login beim Share selbst, danach konnten wir die darin gespeicherten Dateien nutzen. Das lässt sich über Single-Sign-On-Funktionen, die das Produkt ebenfalls anbietet, verhindern, dazu später mehr. Das ganze Vorgehen zum Einrichten Client-loser Zugriffe gestaltet sich unter dem Strich recht gradlinig und ist gut erklärt. Im Test benötigten wir für die Konfiguration des Systems bis zu diesem Punkt lediglich eine halbe Stunde.

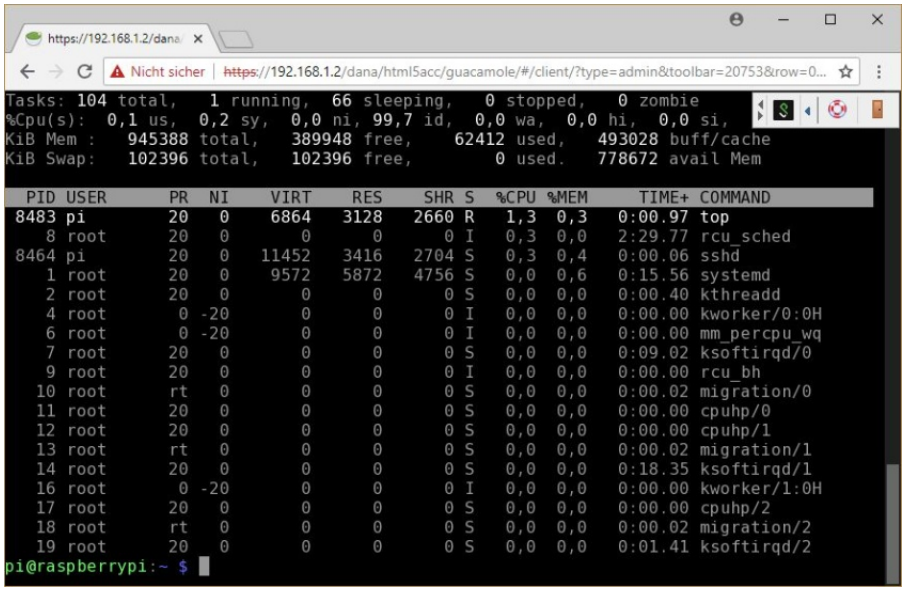
Die Arbeit mit einem zweiten Authentifizierungs-Server

Nach dem Abschluss der Erstkonfiguration gingen wir daran, unser Setting zu perfektionieren. Dazu änderten wir die Benutzerauthentifizierung so, dass neben der Angabe von Username und Passwort auch der Google Authenticator zum Einsatz kam. Dazu spielten wir zunächst auf einem Smartphone vom Typ Huawei P9 unter Android 7 die Google Authenticator App ein. Anschließend definierten wir unter "Authentication" einen neuen Authentifizierungsserver vom Typ "Google Authenticator". Da-

bei war keine weitere Konfiguration erforderlich, bei Bedarf sind die Administratoren dazu in der Lage, die Zahl der erlaubten Authentifizierungs-Versuche zu begrenzen und ähnliches. Nachdem das erledigt war, öffneten wir die Konfiguration unseres Authentication Realms und fügten diesem einfach den neuen Server hinzu. Die Konfiguration zusätzlicher Authentifizierungs-Server gestaltet sich folglich sehr einfach, da wir die sonstigen Einstellungen dazu nicht anrühren mussten. Jetzt loggten wir uns wieder mit unseren User-Credentials bei der PCS-Appliance ein. Das Web-Interface präsentierte uns daraufhin nicht wie zuvor die Webseite mit den Links auf die freigegebenen Ressourcen, sondern stellte einen QR-Code dar, den wir mit unserem Test-Smartphone scannen mussten, um in der Authenticator App das Konto für den PCS-Zugriff hinzuzufügen. Danach zeigte uns die App einen Zahlencode an, der regelmäßig wechselte und der nach dem Login mit den Anwender-Credentials im Web-Interface als zweiter Authentifizierungsschritt eingegeben werden musste, um den Zugriff auf die freigegebenen Ressourcen zu ermöglichen. Im Test funktionierte dies wie erwartet.

Das Enterprise Onboarding

In der nächsten Phase des Tests befassten wir uns mit der Enterprise Onboarding-Funktion. Enterprise Onboarding bedeutet, dass Geräte, die mit dem System Verbindung aufnehmen, auf einfache Weise in die Unternehmensumgebung integriert und dann über diese verwaltet werden. Konkret können sich die Anwender mit einem neuen Device bei der PCS-Lösung anmelden und erhalten dann automatisiert Wifi- und VPN-Verbindungsdefinitionen beziehungsweise Zertifikatsprofile, mit denen sie dann im Betrieb die Unternehmensressourcen nutzen. Dazu sind bei einer korrekt konfigurierten Umgebung keine Aktivitäten von Seiten der IT-Abteilungen erforderlich. PulseSecure unterstützt Enterprise Onboarding für Geräte unter Android 4 oder neuer, iOS 6 oder neuer, MacOS X und Windows seit Windows 7. Im Test setzten wir wieder unser Test-Smartphone vom Typ Huawei P9 unter Android 7 ein, um das Onboarding zu analysieren. Die Enterprise Onboarding-Funktion wird auf Ebene der Benutzerrollen definiert. Dabei haben die zuständigen Mitarbeiter die Möglichkeit, entweder die Auto Launch-Funktion zu aktivieren, die direkt nach dem Login einen Download-Link für die Client-Software anbietet, oder den Client automatisch auf Windows-Systemen einzuspielen. Alternativ lässt sich auch ein externes Mobile Device Management-System für das Onboarding einbinden. Im Test verwendeten wir die Auto Launch-Funktion. Um das Onboarding zu nutzen, müssen sich die Anwender zunächst mit Benutzername und Passwort bei der PCS-Appliance anmelden. Danach wird die Client-Software – falls erforderlich, bei iOS und MacOS funktioniert das Onboarding auch ohne – entweder manuell oder automatisch installiert und das Onboarding läuft durch. Das heißt, die neuen Geräte erhalten die vordefinierten Profile für VPN- und Wifi-Verbindungen und die Zertifikate. Letztere lassen sich nutzen, um die Devices nach dem Onboarding direkt bei den VPN- und Wireless-Systemen zu authentifizieren. Alternativ kann diese Authentifizierung auch mit Login-Credentials erfolgen, in dem Fall müssen die Administratoren kein Onboarding von Zertifikatsprofilen konfigurieren.



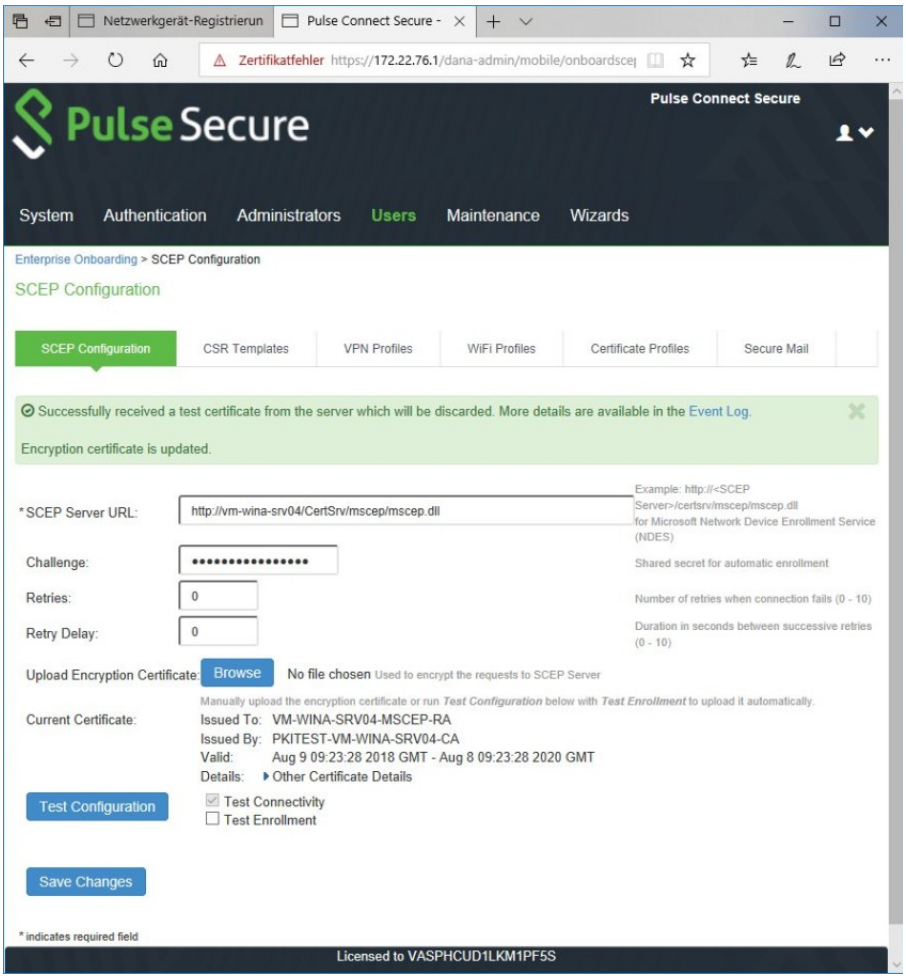
Der SSH-Zugriff mit HTML5 auf einen Raspberry Pi unter Linux

Die Konfiguration der Zertifikatsverteilung

Damit die Clients automatisch Zertifikate für die Authentifizierung erhalten können, benötigt das System einen im Netz vorhandenen SCEP-Server (Simple Certificate Enrollment Protocol). Im Test verwendeten wir dazu eine entsprechend konfigurierte

Windows Zertifizierungsstelle, die auf einem Windows Server 2012 lief. Damit dieser Server mit unserer PCS-Appliance kommunizieren konnte, trugen wir seine URL im Web-Interface der Lösung ein, legten ein Certificate Signing Request-Template (CSR) an (das Funktioniert ebenfalls über das PCS-Web Interface) und luden dieses über die "Test Configuration"-Funktion der Enterprise Onboarding-Funktion auf den SCEP-Server hoch. Das System quittierte diesen Upload mit einer grün gestalteten Meldung, die besagte, dass alles in Ordnung war und dass die Appliance mit dem SCEP-Server kommunizieren konnte. Dieser Konfigurationsschritt ist beim Einsatz der Passwort-basierten Authentifizierung wie gesagt nicht erforderlich.

Egal welche Authentifizierungsmethode im Betrieb zum Einsatz kommt, die Administratoren müssen immer eine VPN-Verbindung anlegen, damit die mobilen User, die sich über das Enterprise Onboarding anmelden, anschließend via VPN auf das Netzwerk zugreifen können. Die Konfiguration dieser VPN-Profile erfolgt im Bereich "Users / Enterprise Onboarding". Im Wesentlichen besteht ein solches Profil aus einem Namen, der Server-URL (der VPN-Server war in unserem Test die PCS selbst), der Benutzerrolle mit den Mapping Rules und der Authentifizierungsmethode, also Passwörtern oder Zertifikaten. Für die Passwort-basierte Authentifizierung war unsere Konfiguration damit bereits abgeschlossen und wir konnten uns mit Hilfe des Browsers unseres Android-Devices bei der PCS-Appliance einloggen, worauf uns die Appliance wie erwartet einen Link zur Installation des PulseSecure Clients anzeigte. Nachdem wir diese Software eingespielt hatten, führte das System das Onboarding durch und baute die Verbindung auf. Danach griffen wir ohne Probleme via VPN auf das Netzwerk zu. Unter Windows funktionierte das ähnlich.



Das PCS-Verwaltungsinterface nach dem erfolgreichen Hinzufügen des SCEP-Servers zu unserer Konfiguration

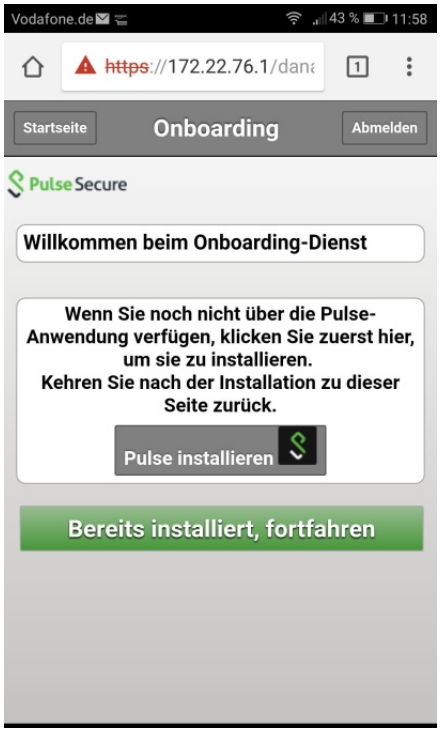
Um die Zertifikat-basierte Authentifizierung für unsere VPN-Verbindung zu nutzen, mussten wir noch etwas zusätzliche Arbeit leisten und ein "Certificate Profile" einrichten. Dazu wechselten wir nach "Users / Enterprise Onboarding / Certificate Profiles" und generierten einen entsprechenden Eintrag. Dieser benötigt wieder einen Namen. Außerdem müssen die zuständigen Mitarbeiter angeben, für welche Client-Typen das Profil Gültigkeit besitzen soll (Android, iOS, MacOS und Windows). Zusätzlich möchte das System auch wissen, wo das Zertifikat herkommt. Dafür gibt es drei unterschiedliche Optionen: "Import and User Global Certificate" bedeutet, dass das globale Zertifikat der Pulse Connect Secure-Lösung zur Authentifizierung des Client-Geräts zum Einsatz kommt.

Bei "Import and User CA Certificate" verwendet das System stattdessen ein vorgegebenes Zertifikat, das importiert und auf die Clients heruntergeladen werden muss. Das ergibt beispielsweise bei der Arbeit mit Wifi-Profilen Sinn. Die letzte Option, "Generate per User Certificate" kam bei uns im Test zum Einsatz.

Dabei finden der SCEP-Server und das CSR-Template Verwendung, um für jeden Client ein Zertifikat zu generieren. Zum Abschluss der Konfiguration gaben wir noch das zu verwendende – zuvor definierte – CSR-Template an und legten fest, für welche Benutzerrollen das Profil gültig sein sollte. Damit war die Konfiguration abgeschlossen und wir konnten die Onboarding-Funktion mit Zertifikaten nutzen.

Der Host Checker

Jetzt war es an der Zeit, auf den Funktionsumfang des Host Checkers einzugehen. Dieser überprüft wie gesagt, ob auf dem Endgerät Sicherheits-Applikationen wie Antivirus und Firewall arbeiten und analysiert zudem auch die Betriebssystemversion, den Patch Level, den Browser-Typ und viele andere Anforderungen. Darüber hinaus führt er auch ein Vulnerability Assessment durch, um erfolgreiche Malware-Angriffe auszuschließen. Stellt sich ein Endgerät als nicht compliant heraus, so versucht der Host Checker, durch Updates der betroffenen Softwarekomponenten Compliance herzustellen. Gelingt das nicht, so kann das Endgerät in Quarantäne verschoben werden. Alternativ wird ihm – je nach Konfiguration – der Zugriff erlaubt oder komplett gesperrt.



Bei aktiviertem Enterprise Onboarding erhält der Benutzer unter Android nach dem ersten Login einen Installations-Link für die PulseSecure-App

Um die Host Checking-Funktion zu testen, erzeugten wir über das Konfigurationswerkzeug unter "Authentication / Endpoint Security / Host Checker" eine dementsprechende Regel, die sicherstellen sollte, dass auf unserem Windows 10-Client eine Firewall aktiv war. Dieser Regel mussten wir zunächst einen Namen geben, außerdem wählten wir das Firewall-Produkt aus, das auf dem Client installiert war. Dafür hat PulseSecure bereits eine große Zahl unterstützter Firewalls in die Sicherheitslösung integriert, so dass die Selektion schnell und einfach ablief.

Im Rahmen der Regeldefinition konnten wir zusätzlich noch dafür sorgen, dass das System den Client ständig überwachte und so nicht nur bei der Anmeldung sondern auch im laufenden Betrieb dazu in der Lage war zu erkennen, ob die Firewall aktiviert oder deaktiviert wurde. Im nächsten Schritt aktivierten wir die Regel über den User Authentication Realm. Als die Regel aktiv war, loggten wir uns mit dem Test-Client bei der Sicherheits-Appliance ein, woraufhin sich erwartungsgemäß der PulseSecure Host-Checker installierte und uns erst ins Netz ließ, als die Überprüfung des Endgeräts erfolgreich abgeschlossen war.

Connection Sets

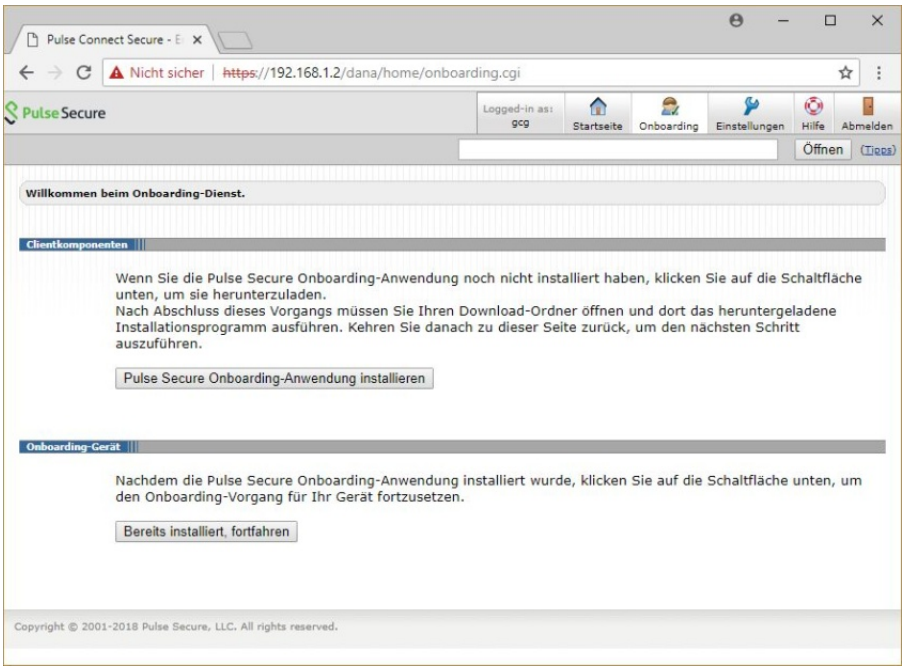
Ein Connection Set bestimmt, auf welche Art und Weise das System Verbindungen aufbaut, zum Beispiel abhängig von der verwendeten Benutzerrolle oder dem Ort, an dem sich der Client befindet. So kann man mit Hilfe von Connection Sets beispielsweise einem mobilen Client, der sich bereits im LAN befindet, den direkten Zugriff auf das Internet über den Unternehmensrouter erlauben, während der gleiche Client gezwungen wird, sämtlichen Internet-Verkehr über eine VPN-Connection in die Zentrale abzuwickeln, wenn er sich von außen über ein unsicheres WLAN verbindet.

Die Connection Sets lassen sich unter „Users / PulseSecure Client / Connections“ konfigurieren. Auch hier müssen die Administratoren zuerst wieder einen Namen vergeben und können dann diverse Parameter festlegen wie zum Beispiel ob die Login-Informationen gespeichert werden dürfen, ob die Benutzer unbekannten Zertifikaten vertrauen dürfen und so weiter.

Sobald alle diesbezüglichen Angaben vorgenommen wurden, geht es an die Konfiguration der zum Connection Set gehörenden Verbindungen. Auch hier stehen wieder diverse Parameter zur Konfiguration zur Verfügung. So lassen sich beispielsweise Verbindungen auf den Server beschränken, der die Konfiguration geliefert hat und es ist auch möglich, den Benutzern zu erlauben, die Verbindungen zu modifizieren.

Zu den weiteren Konfigurationsparametern innerhalb der Verbindungsdefinition gehören unter

anderem ein automatischer Verbindungsaufbau und eine automatische Reconnect-Funktion nach einem Timeout, die im Test einwandfrei funktionierte. Ebenfalls von Interesse sind noch die „Location Awareness Rules“, die dazu dienen, einem Client die Bestimmung seines aktuellen Standorts zu ermöglichen.



Das Onboarding von einem Windows-System

Ist zum Beispiel ein bestimmter Rechner über ein physikalisches Interface erreichbar, so kann der Client davon ausgehen, dass er sich im LAN befindet. Alternativ lässt sich die Location unter anderem auch über einen bestimmten DNS-Server bestimmten.

Erkennt das System, dass die in den Location Awareness Rules festgelegten Bedingungen zutreffen, so versucht es eine automatische Verbindung aufzubauen. Sind sie nicht mehr wahr, so wird die Verbindung unterbrochen. Auf diese Art und Weise lassen sich über verschiedene Verbindungsdefinitionen für die unterschiedlichsten Szenarien Connections anlegen.

Always-on-VPN

Für unser Test Connection Set konfigurierten wir mit dem dafür vorgesehenen Wizard, auf den wir gleich noch genauer eingehen, zudem auch noch ein Always-on-VPN, das sämtlichen Verkehr von den verbundenen Clients durch unsere PCS-Appliance lenkte. Auf diese Weise stellt das System – wie bereits angesprochen – sicher, dass die Clients nicht über offene oder potentiell ungesicherte Netze direkte Verbindungen ins Internet aufbauen, die dann angegriffen werden könnten. Im Test ergaben sich bei der Arbeit mit dem Always-On-VPN keine Schwierigkeiten und die Client-Systeme konnten problemlos über die PulseSecure-Appliance eine Verbindung ins Internet aufbauen.

In diesem Zusammenhang ergibt es Sinn, noch kurz auf die Option "Always-on-VPN with Lockdown Mode enabled" einzugehen. Kommt ein Always-on-VPN mit Lockdown Mode zum Einsatz, so sorgt letzterer dafür, dass der Anwender keine Möglichkeit hat, an dieser Konfiguration etwas zu ändern, beispielsweise durch eine Modifikation der Einstellungen oder das Deaktivieren des Tunnels.

Für das Always-on-VPN mit Lockdown Mode lassen sich bei Bedarf auch Ausnahmen definieren. Der Hersteller hat bereits Exceptions für die Dienste beziehungsweise Protokolle DHCP, DNS, Kerberos, LDAP, SNMP und Portmapper angelegt. Auf Wunsch haben die Administratoren auch Gelegenheit, eigene Einträge hinzuzufügen. Im Test fügten wir eine Ausnahme für SSH-Traffic hinzu, dabei kann man – ähnlich wie bei der Definition einer Firewall-Regel – die Richtung (inbound/outbound) bestimmen und sagen, ob die Lösung ein Programm oder einen TCP- beziehungsweise UDP-Port zulassen soll. Unter „Custom“ lassen sich bei Bedarf noch weitere Angaben machen, wie etwa zugelassene IP-Ranges.

An dieser Stelle ebenfalls von Interesse: die Captive Portal Detection. Diese Funktion sorgt dafür, dass das Client-System erkennt, wenn es sich über einen Hotspot verbindet. Ist das der Fall, so wird der Aufbau sämtlicher Connections verzögert, bis ein Internet-Zugriff besteht.

Die Konfigurations-Wizards

Um den Administratoren dabei zu helfen, die Konfiguration bestimmter Funktionen durchzuführen, stellt das Management-Tool diverse Assistenten zur Verfügung. Der erste davon dient zur Schritt-für-Schritt Konfiguration der eben erwähnten Always-On-VPNs und wurde bei uns im Test auch dafür verwendet, ohne dass es dabei zu Schwierigkeiten kam.

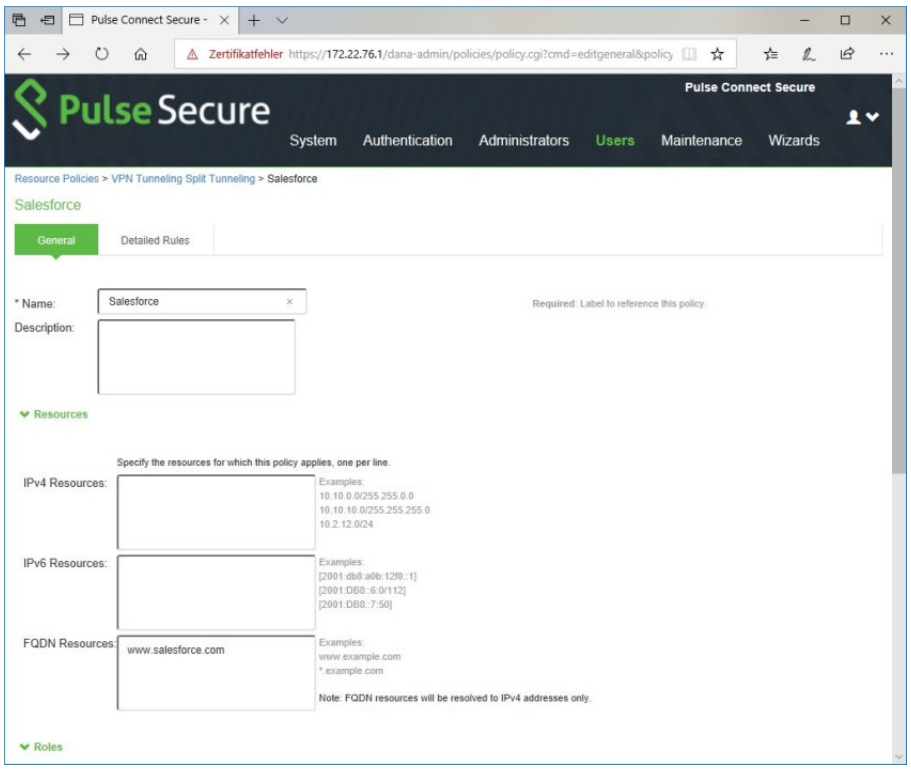
Im ersten Schritt des Wizards fragte uns das System nach dem für die VPN-Verbindung zu verwendenden Connection Set. Danach konnten wir festlegen, ob die Benutzer VPN-Verbindungen aufbauen und unterbrechen konnten oder nicht und ob die einzelnen Verbindungen über den Lockdown Mode abgesichert werden sollten. Anschließend konnten wir noch zusätzliche Ausnahmen für den Lockdown Mode konfigurieren, daraufhin war die Definition des VPNs abgeschlossen und wir konnten es im Betrieb nutzen.

Werden die vorgegebenen Regeln nicht eingehalten, erfolgt auch kein Zugriff auf das Netz

Der zweite Wizard dient zum Erzeugen von User Access-Policies. Diese erlauben es den Endanwendern, über die PCS-Appliance auf freigegebene Ressourcen, wie wir sie bereits zu Beginn des Tests manuell eingerichtet hatten, zuzugreifen. Auch hier wird der zuständige Mitarbeiter Schritt für Schritt durch die Konfiguration geführt. Der Assistent ist sogar noch etwas leistungsfähiger als die Dokumentation zur Erstkonfiguration, die wir zunächst verwendet hatten, da er bei Bedarf gleichzeitig auch Host Checker-Regeln mit anlegt. Im Zweifelsfall würden wir also empfehlen, bei einer neuen Installation auf den Wizard zu setzen.

FQDN-Split-Tunneling

Gehen wir jetzt noch kurz auf das Split-Tunneling ein, das die PulseSecure Appliance bietet. Mit bestimmten IP-Adressen oder Adress-Bereichen ist Split-Tunneling nichts Ungewöhnliches, es lässt sich bei vielen Produkten dazu einsetzen, den Zugriff auf bestimmte Subnetze durch bestimmte Tunnel zu steuern. Bei der PulseSecure-Lösung funktioniert dies aber nicht nur mit IP-Adressen, sondern auch mit FQDN-Ressourcen (Fully Qualified Domain Name). So ermöglicht das Produkt es den IT-Mitarbeitern, sehr einfach eine Regel zu erstellen, die den Usern beispielsweise den direkten Zugriff auf die Webseite www.salesforce.com oder ähnliches erlaubt. Im Test ergaben sich dabei keine Schwierigkeiten.



Die FQDN-Split-Tunneling-Regeln sind schnell erstellt

Single Sign On

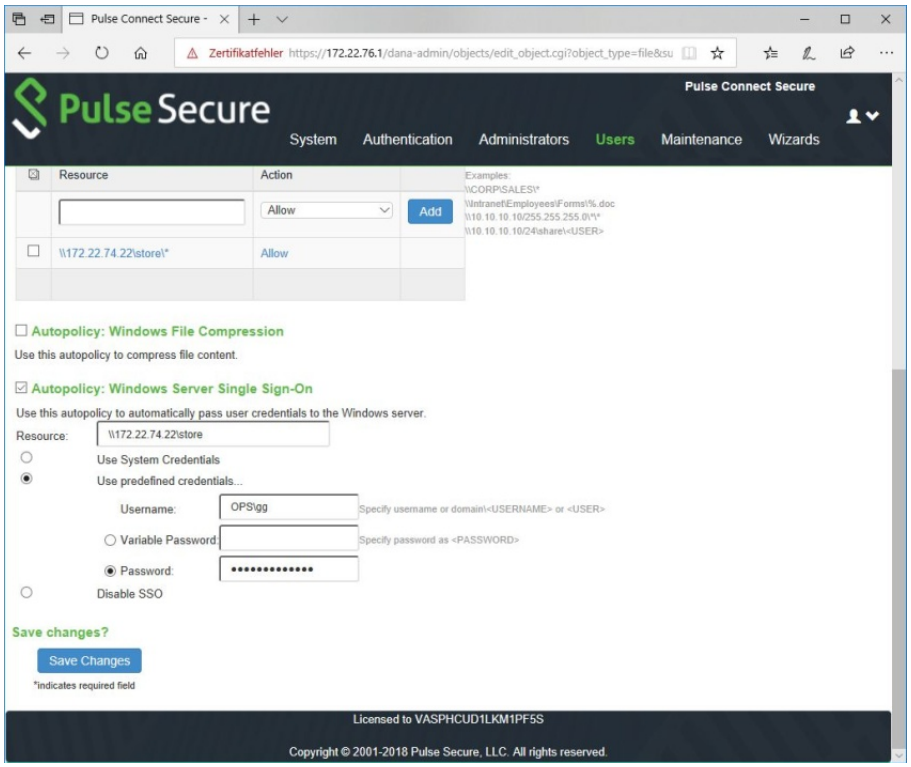
Ebenfalls erwähnenswert ist noch die oben bereits kurz erwähnte Single-Sign-On-Funktion, die dafür sorgt, dass bereits authentifizierte Benutzer freigegebene Ressourcen verwenden können, ohne sich bei diesen erneut anmelden zu müssen. Dieses Feature nutzten wir im Test unter anderem, um dafür zu sorgen, dass wir nach dem Login nicht mehr gezwungen waren, bei dem Zugriff auf das Windows-Share über unser zu Beginn definiertes Bookmark jedes Mal erneut un-

sere Credentials für die Freigabe eingeben zu müssen. Dazu wechselten wir in die Definition des Shares und selektierten den Eintrag „Show ALL autopolicy types“. Danach präsentierte uns das System die Option, vordefinierte Credentials für das Share anzugeben. Anschließend konnten wir als Benutzer ohne weitere Aktionen direkt auf die Freigabe zugreifen. Die Konfiguration dieser Single-Sign-On-Funktion gestaltet sich also sehr einfach.

Die Konfigurationsverwaltung

Zu guter Letzt nahmen wir noch die Optionen zum Import, Export und zum Push von Konfigurationen unter die Lupe. Die Administratoren haben im Betrieb die Möglichkeit, die Systemkonfiguration, die lokalen Benutzerkonten und die Konfiguration des Administrations-Netzwerks zu exportieren. Dazu müssen sie für die jeweiligen Sicherungsdateien Passwörter vergeben. Der Import so gesicherter Konfigurationen erfolgt dann unter Angabe dieses Passworts. Dabei können die Verantwortlichen die PCS-Appliances anweisen, auf den Import bestimmter Angaben wie der IP-Adressen oder der verwendeten Zertifikate zu verzichten. Auf diese Weise lassen sich Konfigurationen schnell und einfach auf unterschiedliche Zielsysteme ausbringen. Bei Bedarf ist es sogar möglich, die Daten Ex- und Importe über XML-Files durchzuführen und genau anzugeben, welche Informationen in der Konfigurationsdatei landen sollen und welche nicht. Das ermöglicht den IT-Verantwortlichen eine sehr große Flexibilität beim Umgang mit den Konfigurationen und hinterließ bei uns im Test einen hervorragenden Eindruck.

Das gleiche gilt für die Push-Funktion, die sich zum einfachen Konfigurationsmanagement innerhalb eines Unternehmens nutzen lässt. Sie versetzt die Administratoren in die Lage, Teile der Konfiguration von einem laufenden System aus auf eines oder mehrere Zielsysteme zu pushen. Dazu müssen die Zielsysteme mit der gleichen Software-Version oder einer neueren als das Quellsystem laufen. Das Pushen funktioniert also sogar über mehrere Versionsstände hinweg. Auf diese Weise lassen sich Konfigurationsänderungen schnell und einfach im Netz verteilen.



Bei Bedarf ist es problemlos möglich, die Zugriffs-Credentials im Rahmen der Ressourcendefinition zu hinterlegen und so eine Single-Sign-On-Umgebung zu realisieren

Fazit

Die Pulse Connect Secure-Appliance eignet sich hervorragend, um sichere Zugriffswege über alle möglichen Arten von Verbindungen auf Unternehmensressourcen herzustellen. Die Lösung konnte im Test mit einem sehr großen Funktionsumfang punkten, in diesem Zusammenhang seien nur die Client-losen und Client-basierten Zugriffsoptionen, das Enterprise Onbording, der Host Checker, die Connection Sets, das FQDN-Split-Tunneling und die flexiblen Umgangsoptionen mit Konfigurationen genannt. Trotz des großen Leistungsspektrums lassen sich Inbetriebnahme und Verwaltung der Systeme relativ problemlos durchführen. Dabei helfen die Wizards genauso wie die umfangreiche Dokumentation. Im Test ließ sich unsere Appliance auch problemlos in das zentrale, cloud-basierte Managementwerkzeug PulseOne integrieren. Administratoren, die nach einer leistungsfähigen Lösung zum Absichern der Zugriffe auf ihre Unternehmensressourcen suchen, sollten auf jeden Fall einen Blick auf das Produkt werfen.

Dr. Götz Güttich leitet das IAIT in Korschenbroich.