Konfiguration Viren/Malware-Scanner

Die Dateischleuse von TightGate-Pro kann durch einen Malware-Scanner serverseitig überwacht werden. TightGate-Pro kann hierzu serienmäßig mit vorinstalliertem Malware-Scanner geliefert werden. Eine nachträgliche Installation ist ebenfalls möglich. In jedem Fall ist eine Lizenz einzuspielen, mit der der Malware-Scanner über den gebuchten Lizenzzeitraum aktualisiert werden kann. Der Lizenzablauf wird über die Statusseite von TightGate-Pro sowie über den entsprechenden Prüfpunkt der Nagios-Systemüberwachung angezeigt.

Hinweis

Downloads, welche aus dem Internet in das Transfer-Verzeichnis von TightGate-Pro herunter geladen werden, werden nicht vom Virenscanner geprüft. Erst beim Schleusen von Dateien vom TightGate-Pro zum Arbeitsplatz wird der Virenscanner befragt.
Beim Upload von Dateien vom Arbeitsplatz zu TightGate-Pro wird der Virenscanner ebenfalls nicht befragt.

Installation des AV-Scanners

TightGate-Pro kann mit werksseitig installiertem und lizenziertem Malware-Scanner geliefert werden. Sollte dies nicht der Fall sein, kann das Produkt bei Bedarf nachinstalliert werden.

So geht's

- Anmeldung als Administrator ***update*** und Auswahl des Menüpunktes **Optionale Pakete hinzufügen**.
- Es können folgende Virenscanner installiert werden:
  Für den Virenscanner der Firma Avast ist das Paket **avast** auszuwählen.
- Nachfolgend noch das **RSBAC-Restore** und **config-Anwenden** im Installationsdialog ausführen.

Die Installation des Malware-Scanners startet. Nach Abschluss der Installation bitte neu als Administrator ***config*** anmelden. Unter dem Menüpunkt **Dienste** ist der installierte Maleware-Scanner verfügbar und kann konfiguriert werden.

Konfiguration des AV-Scanners

Die Konfiguration des Malware-Scanners erfolgt als Administrator ***config***.

Das wird benötigt

- Installierter Virenscanner

So geht's

- Anmeldung als Administrator ***config*** und Auswahl des gewünschten Virenscanners im Menü

Dienste > Malware-Scanner. Es öffnen sich dadurch weitere Menüpunkte, die konfiguriert werden müssen.

- In dem Menüpunkt **Extra-Text** kann ein Freitext eingegeben werden, welcher auf dem Bildschirm der Benutzer als POP-Up-Fenster angezeigt wird, sofern der Virenscanner eine Datei beanstandet.
- In dem Menüpunkt **Lizenzschlüssel** ist ein gültiger Avast-Lizenzkey für das Produkt "Avast Business Antivirus für Linux" einzutragen. Den Key erhalten Sie im Rahmen des Support-Vertrags zu TightGate-Pro vom technischen Kundendienst der m-privacy GmbH.
- In dem Menüpunkt **Max. genutzte CPU-Kerne** ist festzulegen wie viele CPU-Kerne der Virenscanner zur Prüfung verwenden darf. Die Nutzung von 4 CPU-Kernen sollte ausreichend sein. Es wird empfohlen nicht mehr als 20% der verfügbaren Kerne zuzuweisen.
- In dem Menüpunkt **Max. RAM-Disk-Größe in GB** ist festzulegen wie groß die RAM-Disk ist, in die TightGate-Pro Archive selbstständig auspackt. Mit der RAM-Disk wird das Scan-Ergebnis des Virenscanners optimiert. Der empfohlene Wert ist **4**, was einer RAM-Disk von 4 GB entspricht. Die maximal mögliche Eingabe ist auf 1/3 des insgesamt zur Verfügung stehenden Arbeitsspeicher begrenzt. Wird der Wert **0** eingetragen, so wird keine RAM-Disk verwendet.
- In dem Menüpunkt **Verschlüsselte Archive ablehnen** ist festzulegen, ob der Virenscanner verschlüsselte Archive (z.B. Passwortgeschützte ZIP-Dateien) grundsätzlich ablehnt oder zulässt. Wird der Wert auf **Ja** gesetzt, so werden alle verschlüsselten Archive in der TightGate-Schleuse blockiert.
  Hinweis: Die m-privacy GmbH empfiehlt grundsätzlich keine verschlüsselten Archive zu erlauben. Im TightGate-Pro besteht für die Nutzer die Möglichkeit verschlüsselte Archive selbstständig zu entschlüsseln, bevor diese in das interne Netzwerk geschleust werden sollen. Dazu kann man im Dateimanager mit der rechten Maustaste auf das verschlüsselte Archiv klicken und es entschlüsseln.
- In dem Menüpunkt **Immer gleich auspacken** ist festzulegen, ob Archive, welche durch den Virenscanner zu prüfen sind schon durch TightGate-Pro ausgepackt werden, bevor der Virenscanner das erste Mal die Dateien scannt. Dies kann zu einem beschleunigten Transfer führen, sofern vermehrt Archive geschleust werden.
- In dem Menüpunkt **Max. Archiv-Auspack-Ebenen** ist festzulegen, bis zu welcher Tiefe TightGate-Pro Archive auspackt, bevor der Virenscanner aufgibt und die Datei als fehlerhaft blockiert. Mit dieser Einstellung sollen Angriff über Archivbomben verhindert werden. Die m-privacy GmbH empfiehlt einen Wert von 5 hier zu setzen.
- Über den Menüpunkt **Malware-Scanner starten** kann der Malware-Scanners aktiviert oder deaktiviert werden.
  Achtung: Es empfiehlt sich, diese Option abschließend zu kontrollieren und ggf. korrekt zu setzen, um das System nicht versehentlich mit deaktiviertem Malware-Scanner zu betreiben.
- In dem Menüpunkt **Malware-Scanner-Proxy** kann eingestellt werden, dass der Virenscanner seine Singnaturupdates nicht direkt bezieht, sondern über einen Proxy. Der Proxy ist in der Form IP-Adresse:Port anzugeben. Die Signaturen des Malwarescanner Avast werden über folgende Domäne bezogen: **linux-av.u.avcdn.net**
- Im Anschluss an das Setzen der Einstellungen sind als Administrator ***config*** die Einstellungen über die Menüpunkte **Speichern** und **Anwenden** aufzurufen. Bei der Verwendung des Virenscanners von der Firma Avast empfiehlt die m-privacy GmbH das **Anwenden** zweimal laufen zu lassen, da manchmal die benötigten SSL-CAs nachgeholt werden müssen.
- Zur Kontrolle, ob der Virenscanner richtig läuft bitte als Administrator ***maint*** anmelden und den Menüpunkt **Malware-Scanner > Status** aufrufen. Es erscheint eine Anzeige, ob der Virenscanner ordnungsgemäß läuft und die Signaturen aktuell sind.

Viren-Signaturen manuell aktualisieren und Malware-Status prüfen

Die Schadcode-Signaturen sind ein integraler Bestandteil eines Malware-Scanners. Für eine optimale Erkennungsleistung des Scanners müssen die Signaturen stets auf dem neuesten Stand sein. TightGate-Pro lädt die jeweils aktuellen Definitionen täglich direkt vom Update-Server des Herstellers, sodass sich ein manueller Eingriff in der Regel erübrigt. Sollen die Signaturen manuell erneuert werden, so ist folgendermaßen vorzugehen.

Viren-Signaturen manuell aktualisieren

- Anmeldung als Administrator ***maint***.
- Auswahl der Menüoption **Malware-Scanner > Update**. Die Schadcode-Definitionen werden aktualisiert, was einen Augenblick dauern kann.
- Zur Überprüfung der Aktualität und Funktionalität des Virenscanners kann der Status, wie nachfolgend beschrieben überprüft werden.

Hinweis

Sollte die Aktualisierung fehlschlagen, sind Netzwerkprobleme die häufigste Ursache. Weiterhin ist eine gültige Lizenz für den Malware-Scanner erforderlich.

Status des Malware-Scanners prüfen Einzelsystem

Um sicherzustellen, dass der Malware-Scanner ordnungsgemäß läuft, gibt es auf TightGate-Pro mehrere Wege. Der schnellste und zuverlässigste Weg den Status des Virenscanner auf einem TightGate-Pro zu prüfen ist:

- Anmeldung als Administrator ***maint***.
- Aufruf des Menüpunkts **Malware-Scannner > Status**. Es wird angezeigt, ob der Virenscanner läuft und die Signaturen aktuell sind. Sofern Sie einen gültigen Software-Pflegevertrag für TightGate-Pro haben, wird die Lizenz des Virenscanners vom System automatisch 72 Stunden vor Ablauf erneuert.

Status des Malware-Scanners prüfen im Cluster

In TightGate-Pro Clustersystemen ist es aufwändig jeden einzelnen TightGate-Pro Server dahingehend zu prüfen, ob der Virenscanner und die Signaturen aktuell sind. Hier kann die Prüfung auf den Zustand auch über die Funktion des Netzwerk prüfen überprüft werden.

- Anmeldung als Administrator ***config***.
- Aufruf des Menüpunkts **Cluster > Scanner-Status zeigen (*)**. Dort ist der Wert **Ja** auszuwählen.
- Die Einstellungen danach **Speichern** und **Anwenden**.
- Über den Menüpunkt **Netzwerk prüfen** wird nun für jeden Server im Cluster separat angezeigt, ob der Virenscanner zuverlässig läuft.

Hinweis

Es ist ratsam den Virenscanner über das Monitoring überwachen zu lassen. TightGate-Pro stellt dafür entsprechende Sensoren bereit.

AV-Scanner Cache leeren

Wird eine Datei vom Virenscanner gescannt, so wird das Ergebnis des Scans für eine Stunde im Cache von TightGate-Pro vorgehalten. Sollte die gleiche Datei innerhalb dieser Zeit erneut gescannt werden, so wird das Ergebnis des Caches verwendet. Sind in diesem Cache Dateien als Schadcode markiert, weil der Virenscanner nicht lief oder veraltete Signaturen hatte (> 3 Tage), so müssen Benutzer eine Stunde warten, bis der Cache geleert wird oder der Administrator ***maint*** den Cache manuell leert. Das Leeren des Caches erfolgt über den Menüpunkt **Malware-Scanner > Cache leeren**. Bitte stellen Sie sicher, dass der Virenscanner richtig läuft und die Signaturen aktuell sind, bevor Sie den Cache leeren.

Das Prüfen, ob ein Scanner aktuell ist, erfolgt wie im Abschnitt Viren-Signaturen manuell aktualisieren beschreiben.

Malwarescanner Weißlisten konfigurieren

Das Scannern von großen Dateien (ISOs, Archive etc.) durch Virenscanner kann zum Teil recht lange dauert und manchmal sogar fehlschlagen. Hat man große Dateien auf TightGate-Pro heruntergeladen und anderweitig sichergestellt, dass diese keinen Schadcode enthalten, so gibt es die Möglichkeit MD5-Prüfsummen von Dateien im TightGate-Pro zu hinterlegen, bei denen der Virenscanner keine Prüfung durchführt. Das Hinterlegen der MD5-Prüfsummen kann entweder manuell erfolgen oder es können auch bereits abgelehnte Dateien aus dem Virenscanner-Log der Weißliste hinzugefügt werden.

MD5-Prüfumme manuell zu Weißliste hinzufügen

Zu Hinzufügen einer MD5-Prüsumme zur Virenscanner Weißliste, gehen Sie bitte folgendermaßen vor:

- Anmeldung als Administrator ***maint***
- Auswahl des Menüpunktes **Malware-Scanner > Neu in Weißliste**
- Die Eintragung **MUSS** die **MD5-Prüfsumme** gefolgt von einer frei wählbaren **Beschreibung** enthalten! Der Dateimanager der TightGate-Pro Sitzung verfügt im Kontextmenü (rechte Maustaste) über den Menüpunkt **Eigenschaften > Prüfsummen**, aus welchem die MD5-Prüsumme kopiert werden kann. Die MD5-Prüfsumme kann aber natürlich auch extern ermittelt werden. Das Einfügen einer kopierten MD5-Prüfsumme in das Auswahlfeld erfolgt über die Tastenkombination **Strg+Shift+v**.

Hinweis

Falls das manuelle Hinzufügen einer neuen MD5-Prüfsumme vom System abgelehnt wird, prüfen Sie bitte dass die **MD5-Prüfsumme nur Kleinbuchstaben und Zahlen** enthält und in der **Beschreibung keine Sonderzeichen** enthalten sind.

MD5-Prüfsumme aus Malware-Scanner Log zur Weißliste hinzufügen

Zur Übernahme von MD5-Prüfsummen aus einer bereits abgelehnten Dateiübertragung gehen Sie bitte folgendermaßen vor:

- Anmeldung als Administrator ***maint***
- Auswahl des Menüpunktes **Malware-Scanner > Abgelehnte Dateien**
- Sie sehen eine Auswahl an MD5-Prüfsummen mit dem zugehörigen Dateinamen, welche innerhalb der letzten 7 Tage durch den Virenscanner blockiert wurden.
- Wählen Sie die MD5-Prpfüsumme, welche in die Weißliste übernommen werden soll mit der Leertaste aus und bestätigen Sie die Auswahl mit **OK**.
- Die MD5-Prüsumme wird damit übernommen. Ein Leeren des Virenscanner-Caches ist nicht erforderlich.

MD5-Prüfsumme aus Weißliste entfernen

Soll eine MD5-Prüfsumme aus der Weißliste entfernt werden, so ist folgendermaßen vorzugehen:

- Anmeldung als Administrator ***maint***
- Auswahl des Menüpunktes **Malware-Scanner > Entferne aus Weißliste**
- Sie sehen eine Übersicht über alle in der Weißliste gespeicherten MD5-Prüfsummen. Sie können einzelne oder mehrerer Prüfsummen mit der Leertaste auswählen. Bestätigen Sie die Auswahl mit **OK**, damit sind die Prüfsummen aus der Weißliste entfernt.