OPSWAT - Dateibereinigung für die TightGate-Schleuse

Die Firma OPSWAT bietet mit dem Produkt MetaDefender eine Möglichkeit Dateien mit multiplen Virenscannern auf Schadcode zu prüfen und weiterhin auch potentiell gefährlichen Code aus Dateien zu entfernen (Dateibereinigung). Bei der Dateibereinigung ist es z. B. möglich Makros aus Office-Dokumenten zu entfernen, ohne dabei das Office-Dokument als solches unbrauchbar zu machen. Die m-privacy GmbH hat die Möglichkeiten von OPSWAT erkannt und bietet allen Kunden, die das Produkt OPSWAT nutzen eine Schnittstelle, um damit die Qualität der TightGate-Schleuse zu verbessern. Die nachfolgende Anleitung beschreibt, wie die OPSWAT-Schnittstelle in TightGate-Pro zu konfigurieren ist.

Hinweis

Die Menüpunkte und Funktionalität von OPSWAT ist nur verfügbar, sofern das optionale Paket **opswat-integration** installiert wurde.

Änderung der Funktionsweise der Dateischleuse

Mit der Aktivierung von OPSWAT (als ***config***) wird die Funktionalität der TightGate-Schleuse geändert und folgende Einstellungen werden dabei fest umgesetzt:

- Die MIME-Typen-Prüfung für den Datei-Download am TightGate-Pro wird automatisch deaktiviert und es werden alle MIME-Typen zur Übergabe an OPSWAT zugelassen, sodass nur noch das Produkt OPSWAT darüber entscheidet, ob ein Dateityp zum Schleusen zugelassen wird.
- Der Datei-Download selbst erfolgt bei der Nutzung von OPSWAT immer nur über die Auto-Schleuse. Ein manueller Datei-Download von TightGate-Pro auf den lokalen Arbeitsplatz mittels der TightGate-Schleuse ist nicht mehr möglich.
- Der Datei-Upload von einem lokalen Arbeitsplatz zu TightGate-Pro erfolgt nach wie vor manuell über die TightGate-Schleuse oder das Kontextmenü **Senden an…** Die MIME-Typen-Prüfung für den Datei-Upload wird wie bisher auf dem TightGate-Pro konfiguriert und dort werden auch die Berechtigungen (MIME-Typen) vergeben.

Konfiguration von OPSWAT auf TightGate-Pro

Die Konfiguration der API-Schnittstelle, damit TightGate-Pro mit OPSWAT kommunizieren kann ist mit wenigen Einstellungen vorgenommen. Die nachfolgende Tabelle beschreibt, wie die Einstellungen zu setzen sind.

Achtung

Stellen Sie sicher, dass sich der OPSWAT-Server nicht im Klientennetzwerk befindet, da sonst keine

Verbindung zum OPSWAT-Server aufgebaut werden kann!

Das wird benötigt

- IP-Adresse oder Name des OPSWAT-Servers.
- CA-Zertifikat vom OPSWAT-Server, sofern eine verschlüsselte HTTPS-Verbindung zur Kommunikation von TightGate-Pro zum OPSWAT-Server verwendet werden soll.
- Der API-Port, auf dem der OPSWAT-Server lauscht.
- Die verwendeten OPSWAT-Rules.

So wird OPSWAT konfiguriert

Die Konfiguration von OPSWAT erfolgt am TightGate-Pro als Administrator ***config*** im Untermenü **Dienste**. Dort gibt es folgende Menüpunkte:

Menüpunkt	**Beschreibung**
OPSWAT-Integration*	Schaltet den Download über die lokale Schleuse ab und nutzt für den Dateitransfer ausschließlich das Zusatzprodukt OPSWAT. Sobald der Menüpunkt auf **Ja** gesetzt wurde, öffnen sich darunter weitere Menüpunkte zur Eintragung der OPSWAT-Details.
OPSWAT-Host*	Angabe der IP-Adresse oder des Hostnamen des OPSWAT-Servers. Wird eine verschlüsselte Verbindung per HTTPS verwendet, so ist immer der Hostname anzugeben.
OPSWAT-API-Port*	Port über den der OPSWAT-Server angesprochen wird, der Standardport ist 8008.
OPSWAT-Rules*	Anlegen der Regeln (rules), welche auf dem OPSWAT-Server benutzt werden sollen. Die Regeln müssen exakt dem Namen auf dem OPSWAT-Server entsprechen!
Importiere OPSWAT-SSL-Custom-CA*	Sofern die Verbindung zum OPSWAT-Server über das verschlüsselte HTTPS-Protokoll erfolgen soll, so ist hier die SSL-CA von OPSWAT-Server zu hinterlegen. Die CA muss vorab in das Transfer-Verzeichnis des Administrators ***config*** geschleust worden sein. Ist eine CA importiert und angewendet, so wird immer versucht über das HTTPS-Protokoll mit dem OPSWAT-Server zu kommunizieren. **Achtung:** Alle Zertifikate müssen einzeln importiert werden, es ist nicht möglich eine Zertifikatskette in einer Datei zu importieren!
Entferne OPSWAT-SSL-Custom-CA*	Sofern eine Custom-CA importiert ist, kann über diesen Menüpunkt die Custom-CA wieder entfernt werden.
OPSWAT-Extra-Text	In dem Menüpunkt kann ein Freitext eingegeben werden, welcher auf dem Bildschirm der Benutzer als Pop-up-Fenster angezeigt wird, sofern OPSWAT eine Datei beanstandet.
OPSWAT-Klienten-Ordner*	Hier kann festgelegt werden, wo auf dem Klienten die von OPSWAT gesäuberten, bzw. geprüften Dateien von der TightGate-Schleuse hin übertragen werden.

Nach dem Setzen der Einstellungen sind diese über die Menüpunkte **Speichern** und **Anwenden** zu aktivieren.

Einstellungen testen

Nachdem die Einstellungen zu OPSWAT gesetzt, gespeichert und angewendet wurden, können diese als Administrator ***config*** über den Menüpunkt **Netzwerk prüfen** überprüft werden.

Beim **Netzwerk prüfen**, wird als letzter Test ein Test durchgeführt, ob die Kommunikation vom TightGate-Pro zum OPSWAT-Server über die konfigurierten Einstellungen möglich ist. Nur wenn der Test **OPSWAT API** mit einem grünen OK bestanden wurde, ist davon auszugehen, dass die Kommunikation mit OPSWAT funktioniert.

Schlägt der Test fehl (rotes FAILED), prüfen Sie bitte folgende Einstellungen und wiederholen den Test, bis dieser OK ist.

- Ist die IP-Adresse des OPSWAT korrekt?
- Ist der API-Port korrekt?
- Befindet sich der OPSWAT-Server im Klientennetzwerk? (Wenn ja, muss er da raus)
- Bei HTTPS-Verbindungen: Ist die CA die richtige?
- Beim Wechsel des OPSWAT-Servers: Sind die alten CAs alle gelöscht und die neuen eingespielt?
- Beim Wechsel von HTTPS zu HTTP: Sind alle CAs entfernt?

Benutzereinstellungen für OPSWAT

Damit Nutzer von TightGate-Pro OPSWAT richtig nutzen können, müssen ihnen die dafür richtigen Voreinstellungen gesetzt werden. Nachfolgend wird beschrieben, welche Einstellungen bei der Benutzerverwaltung via Active Directory und bei Anmeldungen via Benutzerzertifikat oder Passwort zu setzen sind.

Einstellungen bei Active Directory

Damit ein Benutzer auf TightGate-Pro den Download über OPSWAT durchführen kann, muss er Mitglied in den folgenden AD-Sicherheitsgruppen sein:

- **TGProUser**
- **TGtransfer**
- **TGtransferN** (N steht für die Nummer der Transfer-Gruppe auf TightGate-Pro. Die Gruppe regelt die erlaubten MIME-Typen für den Datei-Upload)
- **TGopswat**
- **TGopswatN** (N steht für die Nummer der OPSWAT-Rule, welche für den Benutzer verwendet werden soll)

Eine Übersicht über alle AD-Sicherheitsgruppen findet sich hier: Übersicht AD-Sicherheitsgruppen für TightGate-Pro.

Ist der Nutzer in all diesen Gruppen Mitglied und meldet sich mit dem TightGate-Viewer an, so bekommt er in seinem transfer-Verzeichnis einen zusätzlichen Ordner OPSWAT angelegt. Legt er dort eine zu übertragende Datei hinein, so wird diese automatisch zu OPSWAT übertragen. Verbietet OPSWAT den Dateitransfer nicht, so wird die geprüfte/bereinigte Datei automatisch über die Auto-Dateischleuse lokal auf den Arbeitsplatz-PC abgelegt. Wurde kein spezieller Ordner konfiguriert, findet sich der Download im Verzeichnis **autotransfer** des normalen Download-Verzeichnisses.

Achtung

Es ist sicherzustellen, dass im TightGate-Viewer der Auto-Download erlaubt ist, da sonst kein Transfer möglich ist. Dies erfolgt in der Klientenkonfiguration des TightGate-Viewers. Siehe hier: Nutzung der

automatischen Dateischleuse

Für den Datei-Upload nutzt der Benutzer die TightGate-Schleuse. Diese öffnet sich wie gewohnt und es können alle (aus der Gruppe **TGtransferN**) erlaubten Dateien hochgeladen werden. Ein Download über die TightGate-Schleuse ist nicht möglich und wird mit einer Fehlermeldung quittiert. Alternativ kann der Nutzer auch die Kontextmenü-Erweiterung **Senden an…** verwenden, um Dateien zum TightGate-Pro hochladen zu können.

Hinweis: Ist der Benutzer nicht in der Gruppe **TGopswat**, so ist ein Datei-Download nicht mehr möglich. Ist der Benutzer nicht in der Gruppe **TGtransfer**, so kann die manuelle TightGate-Schleuse oder die Funktion des Kontextmenüs **Senden an…** nicht mehr verwendet werden und ein Datei-Upload ist nicht möglich.

Einstellungen bei Zertifikats- oder Passwortanmeldung

Damit ein Benutzer auf TightGate-Pro den Download über OPSWAT durchführen kann, muss er als ***maint*** unter dem Menüpunkt **Benutzerverwaltung > Benutzer ändern > [Benutzerkennung]** folgende Einstellungen bekommen:

- **Datei-Transfer erlaubt = Ja**
- **Transfer-MIME-Typen Upload = [Auswahl erlaubter MIME-Typen für den Datei-Upload]**
- **Transfer-MIME-Typen Download = leer** (es ist auch gar nicht möglich dort etwas einzustellen)
- **OPSWAT-Integration = Ja**, mit anschließender Auswahl der für den Nutzer zu verwendenden **OPSWAT-Rule**

Hat der Nutzer all diese Einstellungen und meldet sich mit dem TightGate-Viewer an, so bekommt er in seinem transfer-Verzeichnis einen zusätzlichen Ordner OPSWAT angelegt. Legt er dort eine zu übertragende Datei hinein, so wird diese automatisch zu OPSWAT übertragen. Verbietet OPSWAT den Dateitransfer nicht, so wird die geprüfte/bereinigte Datei automatisch über die Auto-Dateischleuse lokal auf den Arbeitsplatz-PC abgelegt. Wurde kein spezieller Ordner konfiguriert, findet sich der Download im Verzeichnis **autotransfer** des normalen Download-Verzeichnisses.

Achtung

Es ist sicherzustellen, dass im TightGate-Viewer der Auto-Download erlaubt ist, da sonst kein Transfer möglich ist. Dies erfolgt in der Klientenkonfiguration des TightGate-Viewers. Siehe hier: Nutzung der automatischen Dateischleuse

Für den Datei-Upload nutzt der Benutzer die TightGate-Schleuse. Diese öffnet sich wie gewohnt und es können alle als ***maint*** erlaubten Dateien hochgeladen werden. Ein Download über die TightGate-Schleuse ist nicht möglich und wird mit einer Fehlermeldung quittiert. Alternativ kann der Nutzer auch die Kontextmenü-Erweiterung **Senden an…** verwenden, um Dateien zum TightGate-Pro hochladen zu können.

Erreichbarkeit der OPSWAT Oberfläche

Möchten Sie zusätzlich zur API auch die Weboberfläche von OPSWAT vom TightGate-Pro aus erreichen, so sind folgenden zusätzliche Einstellungen notwendig:

Als Administrator ***config***:

- Unter **Netzwerk > HTTP-Server** ist die IP-Adresse des OPSWAT-Servers einzutragen.
- Unter **Netzwerk > HTTP-Ports** ist der Port einzutragen, über den OPSWAT zu erreichen ist. Der Standard ist Port 8008.
- Sofern Sie einen Proxy im TightGate-Pro eingetragen haben, so ist der OPSWAT-Server als Proxy-Ausnahme einzutragen. Dies erfolgt über den Menüpunkt **Proxy > Proxy-Ausnahmen**. Dort ist der Name bzw. die IP-Adresse des OPSWAT-Servers einzutragen.
- Bitte das **Speichern** und **Anwenden** nicht vergessen.

Testen Sie die Einstellung, indem Sie nach dem **Anwenden** aller Einstellungen sich neu mit einem TightGate-Viewer anmelden und im Firefox den OPSWAT-Server ansurfen. So könnte der Aufruf aussehen:

https://opswat.m-privacy.local:8008