Cygnet

Manual

Bachelorarbeit FS2013

Studenten: Stefan Rohner, Marco Tanner

Betreuer: Prof. Dr. Andreas Steffen, Tobias Brunner

Gegenleser Prof. Stefan Keller

Experte: TBA

Änderungsnachweis

Version	Änderung	Autor	Datum
1.0	Dokumentenentwurf	Marco Tanner	20.05.2013

Inhaltsverzeichnis

1 Einführung

Dieses Dokument beschreibt die Funktionsweise und Bedienmöglichkeiten von Cygnet. Es ist an den Enduser gerichtet.

1.1 Was ist Cygnet?

Cygnet ist eine Erweiterung für den StrongSwan VPN-Client und den dazugehörigen Server. Es ermöglicht die Definition und Durchsetzung von Richtlinien, die für alle VPN-Clients gelten und bei einem Verbindungsversuch erfüllt werden müssen.

StrongSwan-VPN-Clients (**Clients**) können in Cygnet in **Gruppen** eingeteilt werden, nach Betriebssystem, Unternehmensstruktur oder persönlicher Präferenz des Administrators. Es können Richtlinien (**Policies**) definiert werden, wie beispielsweise, dass alle verfügbaren Betriebssystemupdates auf dem Client installiert sind, oder dass gewisse Applikationen auf dem Client nicht installiert sein dürfen. Diese Richtlinien können dann auf die Gruppen angewandt/erzwungen (**Enforcements**) werden und werden von Cygnet bei einem Verbindungsversuch eines Clients geprüft.

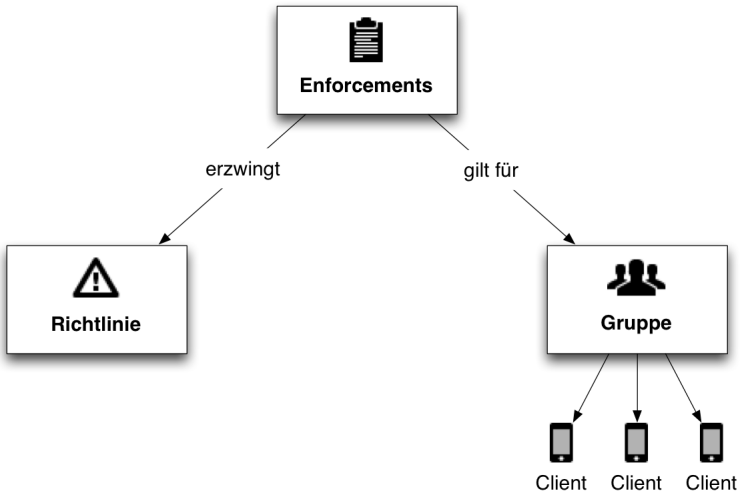

Abbildung 1.1: Übersicht

2 Schritt für Schritt Anleitung

In diesem Kapitel wird anhand eines Beispiel die Einrichtung einer VPN-Richtlinie für eine Unternehmung gezeigt.

2.1 Ausgangslage

Es wird davon ausgegangen, dass bereits eine StrongSwan-Installation mit Cygnet existiert. Siehe **??** Deployment.
Als Beispiel sei eine Hochschule, die einen VPN-Zugang für Studenten, Dozenten und Mitarbeiter anbietet. Jeder dieser Benutzer hat bereits einen Benutzernamen und ein Passwort erhalten, welche als Zugang für das VPN genügen. Grundsätzlich kann sich jeder Benutzer mit einem beliebigen (auch privaten) VPN-fähigen Gerät ins Hochschulnetz einwählen. Damit die Sicherheit des internen Hochschulnetzes nicht kompromittiert wird, wird mithilfe von Cygnet eine Sicherheitsrichtlinie definiert und durchgesetzt.

Wenn Sie Cygnet in einem Browser öffnen und Ihr Passwort eingeben, erscheint als erstes die Übersicht:

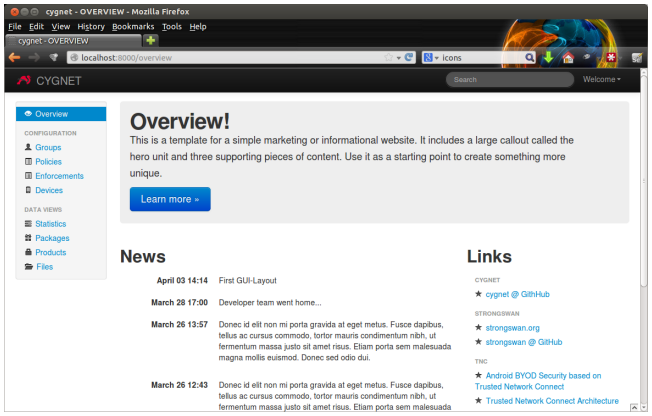

Abbildung 2.1: Cygnet: Übersicht

2.2 Gruppen

Über den ersten Navigationspunkt gelangen Sie auf die Gruppenübersicht. Anfangs sind noch keine Gruppen definiert. Neue Gruppen können mit dem “Hinzufügen”-Button (blaues Plus-Zeichen) erstellt werden.

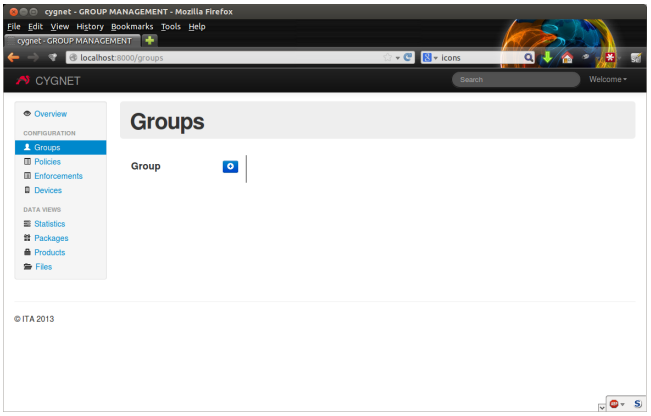

Abbildung 2.2: Cygnet: Gruppen

Eine Gruppe ist definiert über Ihren Namen und kann eine übergeordnete Gruppe haben. Ein Client, der Mitglied in einer Gruppe ist, ist automatisch auch Mitglied in allen übergeordneten Gruppen der Gruppe. Für das Beispiel werden einzelne Gruppen für Studenten, Dozenten und Mitarbeiter definiert, sowie passende Untergruppen. Wenn also ein Client Mitglied der Gruppe “Assistenten” ist, gelten für den Client automatisch auch alle Enforcements der Gruppe “Dozenten”.

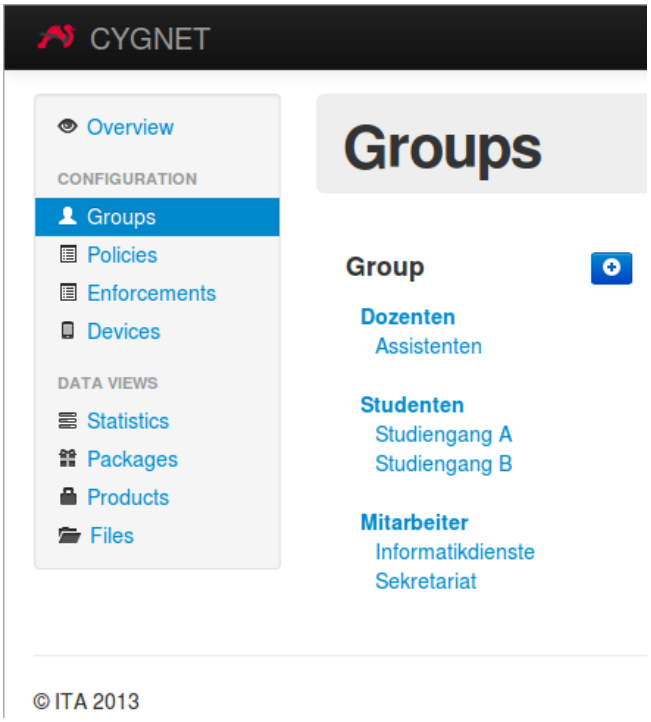

Abbildung 2.3: Cygnet: Beispielgruppen

2.3 Richtlinien (Policies)

Im nächsten Schritt sollen Richtlinien für die verschiedenen Gruppen erstellt werden. Dafür kann im Navigationspunkt “Policies” eine neue Richtlinie erstellt werden.

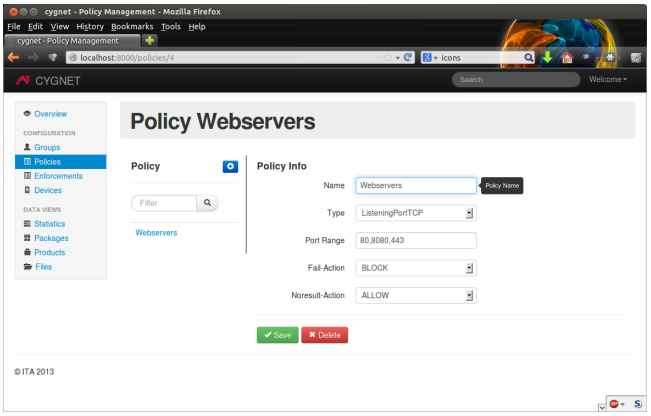

Abbildung 2.4: Cygnet: Neue Policy

Eine Policy besteht aus folgenden Eigenschaften:

Eigenschaft	Beschreibung
Name	Name der Policy
Typ	Typ der Policy (siehe 2.3.1 für mehr Informationen)
Argument	Hängt vom Typ ab. Siehe 2.3.1
Fail-Aktion	Legt fest, wie das System reagiert, wenn die Richtlinie vom Client nicht erfüllt wird.
Noresult-Aktion	Legt fest, wie das System reagiert, wenn eine Messung auf einem Client nicht durchgeführt werden kann.

Beide dieser Aktions-Felder haben vier Auswahlmöglichkeiten. Wenn die Bedingungen der Richtlinie erfüllt werden, ist die Empfehlung immer “ALLOW”.

Aktion	Bedeutung
NONE	Keine Empfehlung
ALLOW	Erlauben
ISOLATE	Isolieren, in ein Spezialnetz verbinden
BLOCK	Blockieren, Verbindung verweigern

Wenn mehrere Richtlinien mit unterschiedlichen Ergebnissen auf einen Client angewandt werden, zählt immer das “schlechtere” Ergebnis, also BLOCK vor ISOLATE vor ALLOW.

2.3.1 Policy-Typen

Die folgenden Policy-Typen werden zurzeit von Cygnet unterstützt.

File Hash

Diese Policy prüft, ob der Hash einer Datei auf dem Client mit dem entsprechenden Referenzwert in der Datenbank übereinstimmt. Die Datei kann aus einer Auswahlliste ausgewählt werden. Der passende Referenzwert wird anhand des Betriebssystems des Clients bestimmt.

Dir Hash

Wie File Hash, aber prüft sämtliche bekannten Dateien in einem Verzeichnis.

Listening Port TCP/UDP

Die Policy prüft, ob auf den angegebenen Ports Listening Sockets eröffnet wurden. Die Port-Range kann beispielsweise folgendermassen aussehen:
`21, 22, 80, 443, 1000-1500, 2048, 6000-40000`

File Exist

Die Policy prüft, ob eine bestimmte Datei auf dem Client exisiert. Sie schlägt fehl, wenn die Datei nicht existiert.

File Not Exist

Wie File Exist, aber prüft, ob die Datei NICHT existiert und schlägt fehl, wenn die Datei existiert.

Missing Update

Prüft, ob alle installierten Softwarepakete (etwa aus dem Google Play Store) auf dem aktuellsten Stand sind. Schlägt fehl, wenn ein Update fehlt.

Missing Security Update

Wie Missing Update, prüft aber nur auf sicherheitsrelevante Updates. Nicht sicherheitsrelevante Updates dürfen fehlen und die Policy ist trotzdem erfolgreich.

Blacklisted Package

Prüft, ob ein Softwarepaket installiert wurde, das vom Administrator auf die Blacklist gesetzt wurde.

OSSettings

Der IMV kontrolliert, ob gewisse Betriebssystemoptionen korrekt gesetzt sind. Ist von der StrongSwan-Implementation abhängig.

Deny

Diese Policy prüft nichts. Sie schlägt per Definition fehl und dient hauptsächlich zum definieren einer Geräte-Blacklist.

2.4 Enforcements

Als dritter und letzter Schritt müssen die erstellen Gruppen und Policies einander zugeordnet werden. Dies kann im Navigationspunkt “Enforcements” gemacht werden. Ein Enforcement setzt eine Policy auf einer Gruppe um.
Zusätzlich kann ein Zeitintervall in Tagen angegeben werden, das angibt, wie oft die Policy getestet werden soll. Ein Wert von 3 bedeutet, dass die Policy, wenn die letzte Prüfung erfolgreich war, nur alle 3 Tage geprüft wird. Ein Wert von 0 bedeuetet, dass die Policy jedes Mal geprüft wird.
Bei einem Enforcement könnnen die “Fail-Action” und “Noresult-Action” überschrieben werden, falls gewünscht. Standardmässig werden die Aktionen von der gewählten Policy geerbt.
Wenn ein Client in zwei Gruppen eingeteilt ist auf denen dieselbe Policie angewandt wurde, so wird die Policy nur einmal getestet. Wenn sich die konfigurierten Aktionen oder das Zeitintervall unterscheiden so wird die drastischere Aktion (BLOCK vor ISOLATE vor ALLOW), resp. das kürzere Zeitintervall angewandt.

2.5 Geräte / Clients

In diesem Bereich werden allen bekannten Clients aufgelistet. Die Liste wird automatisch um neue Clients ergänzt. Ein Client kann hier Gruppen zugeordnet werden, auf denen allenfalls weitere Policies angewandt wurden. Es kann ein Beschreibungstext zum Gerät zugeordnet werden, um die Wiedererkennbarkeit zu vereinfachen.
Zusätzlich kann hier der “Device-Report” eingesehen werden. In dieser Ansicht werden die letzten Mess-Ergnisse eines Geräts angezeigt, in welchen Gruppen das Gerät eingeteilt ist und welche Enforcements auf das Gerät wirken. Dies kann nützlich sein, um herauszufinden warum ein Gerät blockiert oder isoliert wurde.

2.6 Dateien / Files

In diesem Abschnitt werden die bekannten Dateihashes gespeichert. Sie dienen als Referenzwerte für File Hash und Dir Hash Richtlinien. Dateien und Hashes sind read-only. Sie können nur gelöscht, aber nicht bearbeitet oder neu erfasst werden. Die zurzeit bekannten und unterstützten Hash-Algorithmen sind:

- SHA-1
- SHA-1-IMA
- SHA-256
- SHA-384

2.7 Pakete / Packages

Auf dieser Seite werden alle bekannten Software-Pakete und deren Versionen aufgelistet. Hier kann definiert werden, welche Pakete auf der Blacklist stehen und für die “Blacklisted Package”-Policy (Seite 7) getestet werden.
Ein Paket kann entweder global blockiert werden oder nur einzelne Versionen davon. Wenn die Einstellung global für das Paket verändert wird, werden die allenfalls gemachten konfigurationen der einzelnen Versionen überschrieben.

2.8 Produkte / Products

Die hier aufgelisteten Produkte sind alle Client-Betriebssysteme die bisher bei Clients installiert waren. Die Liste wird automatisch ergänzt wenn Clients mit einem anderen Betriebssystem auftauchen. In diesem Bereich können Standard-Gruppen zu Betriebssystemen zugeordnet werden. Das bedeutet, dass wenn ein neuer Client mit einem bestimmten Betriebssystem zum ersten Mal eine Verbindung aufbaut, werden ihm automatisch die Standard-Gruppen des Produkts zugeordnet. So kann eine Default-Policy für unterschiedliche Betriebssysteme konfiguriert werden.