Schweizerische
Fachschule
TEKO

Erarbeitung eines Client Verifizierung Modules für FortiClient Endpoint Management Server (EMS) 7.0.3

Diplomarbeit Samuel Leu

Dipl. Techniker HF Informatik 2022

Abgabedatum:	**16. Mai 2022**
Firmenbetreuer:	**Jens Müller, Abteilungsleiter Sicherheit & Linux**
Schulischer Betreuer:	**Fabian Hirter**

Inhaltsverzeichnis

1. Vorwort

1.1. Management Summary

In den letzten zwei Jahren markierte die Pandemie einen erzwungenen Wechsel der Gepflogenheiten aller. Spätestens nach der Einführung der HomeOffice-Pflicht suchten Firmen die im Dienstleistungssektor angesiedelt sind Lösungen, um ihren Mitarbeiter:innen die Arbeit von daheim zu ermöglichen.

Einer Firma mit rund 160 Angestellten erging es nicht anders. Die Geschäftsleitung fasste den strategischen Entschluss, alle Desktop Computer der Mitarbeiter:innen künftig mit tragbaren Geräten zu ersetzen. Dieser Austausch ist weiterhin im Gange und noch nicht alle Mitarbeiter:innen haben Laptops. Geräte können sich mittels installierter Software vom öffentlichen Netzwerk in das Firmennetz verbinden. Die Infrastruktur wurde so angepasst, dass von ausserhalb Verbindungen über SSL-VPN (Secure Socket Layer Virtual Private Network) möglich sind. Wer noch keinen Laptop erhalten hat, kann sich den Zugang mittels VPN-Client von Fortinet auf seinem privaten Rechner einrichten. Dass private Geräte auf das Firmeninterne Netzwerk zugreifen, widerspricht den internen Richtlinien. Die Verbindung mit privaten Geräten, die eine fehlerhafte Konfiguration aufweisen, ist derzeit noch möglich. Da sich keine andere Lösung fand, wurde dieses Risiko in Kauf genommen und akzeptiert.

Mit der Rückkehr der Arbeitnehmenden in die Geschäftsräumlichkeiten und der Aufhebung der HomeOffice-Pflicht, will die Firma die Richtlinien wieder erfüllen und sucht nach einer Lösung, wie die Verbindung via VPN nur noch von intern verwalteten Firmengeräten möglich ist. In einem ersten Schritt soll der Lifecycle Prozess abgeschlossen werden und firmenweit nur noch tragbare Geräte zum Einsatz kommen. Der Zugriff auf das Firmennetz soll nur noch über diese Notebooks erfolgen. Der Zugriff mit privaten Geräten soll nicht mehr funktionieren und unterbunden werden. Doch wie wird ein Firmengerät als solches auch erkannt? Wie kann verhindert werden, dass sich ein privater Rechner in das Netzwerk der Firma einloggt? Was geschieht mit einem Gerät, das die Verbindung ins Netzwerk aufgebaut hat, aber eigentlich nicht über die erforderlichen Berechtigungen verfügt? Diese Fragen gilt es zu klären, um die Sicherheit der Firma, ihrer Mitarbeiter:innen und der Kunden sicherzustellen und zu erhöhen.

Die Abhängigkeit von Fortinet innerhalb des Netzwerkes beschränkt die möglichen Optionen. Die ebenfalls von Fortinet vertriebene Software «FortiClient EMS» (FortiClient Endpoint Management Server) bietet aber eine Lösung für diese Situation. Mit EMS können die Clients der Firma eindeutig verifiziert werden. Regelbasierte Gruppen (sogenannte Tags) prüfen die Eigenschaften eines Notebooks und können ihm den Zugriff auf das Firmennetz bei Erfüllung der Regeln gewähren. Werden die Regeln nicht erfüllt, kann ein Gerät vom Netzwerk isoliert werden. Die Endpoints können über den EMS verwaltet werden. Geräte, welche nicht im EMS registriert sind, können sich nicht mit dem Firmennetz verbinden. Da der EMS, die FortiGate (Firewall) und der FortiClient (VPN Client auf Firmengeräten) allesamt vom gleichen Hersteller sind, sollte das Zusammenspiel gut funktionieren. Der Laptop mit dem VPN Client von Fortinet soll sich beim EMS melden und als Firmengerät markiert werden. Ist dies erfolgreich soll die Firewall dem Gerät den Zugriff auf das interne Netz und das Internet erlauben.

Während der Erarbeitung der Lösung tauchten allerdings grössere Probleme auf. Die von Fortinet vertriebenen Lösungen kommunizieren ungenügend miteinander. Features, die von Herstellerseite angepriesen werden, funktionieren nur bedingt oder nicht wie erwartet. Die Kommunikation zwischen dem Endpoint Management Server und der FortiGate Firewall ist instabil und unzuverlässig. So haben Clients, die mit dem VPN verbunden sind, keinen Internetzugriff. Durch die Testumgebung konnten diverse Fehler behoben oder identifiziert werden. Das Debugging gestaltete sich als Geduldsprobe mit vielen Lösungsansätzen, die meist nicht von Erfolg gekrönt wurden. Mithilfe des Herstellersupports klärten sich noch weitere Unstimmigkeiten bei den weiteren Features des EMS.

Aufgrund der oben genannten Probleme konnte die Lösung in der Firma nicht produktiv implementiert werden. Es bleibt aber die Hoffnung auf neue Versionen, die die vorhandenen Probleme entweder lösen oder einen Workaround bieten. Die Firma ist bestrebt, die Lösung so bald als möglich einzusetzen. Für den Diplomand geht die Arbeit weiter, sobald neue Versionen verfügbar werden.

1.2. Beruflicher Werdegang Samuel Leu

DV Bern AG, Bern **01.2022 – Heute**

System Administrator

- Support von internen und Firmenkunden
- Support per Telefon oder vor Ort
- Mitarbeit und operative Tätigkeiten in Projekten
- Ticketsystem der Firma bewirtschaften
- Second Level Support
- Verantwortlichkeit Lagerbestände intern

DV Bern AG, Bern **02.2021 – 12.2021**

IT-Supporter

- Support von internen und Firmenkunden
- Support per Telefon oder vor Ort
- Ticketsystem der Firma bewirtschaften
- Verantwortlichkeit Lagerbestände intern

ts mediamatik GmbH, Bern **09.2016 – 01.2021**

Verantwortlicher IT

- Betreuung Privat- und Firmenkunden
- Operative Leitung bei kleineren Projekten
- Verantwortlichkeit über Offerten, Rechnungen
- Funktionalität interner IT sicherstellen
- Support per Telefon oder vor Ort

Coop AG, Bern **01.2016 – 08.2016**

Mitarbeiter Kasse

Innosense GmbH, Tafers **10.2014 – 09.2014**

Mitarbeiter Laden

- Ladenbewirtschaftung
- Umsetzung von Aufträgen
- Zusammenbau/Installation von Computern
- Beratung und Support für Kunden im Laden

2. Projektinitialisierung und Planung

2.1. Ausgangslage

Eine Firma mit 160 Mitarbeiter:innen will den Zugriff auf das interne Netzwerk so beschränken, dass nur noch Firmengeräte den Zugriff erhalten. Die Firma führt aktuell einen Lifecycle durch, wodurch noch in diesem Jahr nur noch tragbare Geräte zum Einsatz kommen. Derzeit sind allerdings noch nicht alle Geräte ersetzt worden. Die Laptops werden professionell von der hauseigenen IT bereitgestellt. Es wird vermutet, dass einige Mitarbeiter aktuell mit ihren privaten Geräten auf die Firmeninfrastruktur zugreifen. Um dem entgegenzuhalten, sollen die Geräte der Firma auch von ausserhalb identifiziert werden können. Gleichzeitig soll der Zugriff von unbekannten Geräten unterbunden werden. So kann sichergestellt werden, dass nur Firmengeräte effektiv Zugriff auf sensible Daten erhalten. Die Multifaktor-Authentifizierung für eine VPN-Verbindung geschieht über den Microsoft Authenticator.

Die derzeit geltenden Richtlinien der Firma sollen so geändert werden, dass der Zugriff auf das interne Netzwerk nur noch über verwaltete Geräte der Firma geschieht. Die Firma ist nach ISO-27001 zertifiziert. Gemäss dieser Zertifizierung gelten Bestimmungen, die eingehalten werden müssen. Weiter ein zentraler Auszug aus dem internen Reglement «Umgang mit IT»:

- Punkt 2.2: Fahren Sie PC, Notebook, usw. bei Arbeitsschluss immer herunter, damit Strom gespart wird und Ihr Gerät beim Start die automatischen Softwareaktualisierungen ausführt.
- Punkt 2.2: Manipulationen an der IT-Hardware und Installationen von nicht freigegebenen Programmen sind verboten. Sollten Sie einen Bedarf an neuen Programmen oder Hardware haben, melden Sie diesen bei der Abteilung IT Services. Sie werden Ihre Anfrage prüfen und entsprechend bearbeiten
- Das Anschliessen fremder oder privater Geräte an die Firmen-Netzwerke (Ausnahme ist die Nutzung speziell dafür eingerichteter Gast Zugänge) ist verboten
- Punkt 3.3.2 Mit privaten Geräten sind mittels definierten Fernzugriffen (z.B. Citrix Zugang) der Zugriff auf die Infrastruktur der Firma erlaubt
- Punkt 3.3.2: Das direkte Verbinden von privaten Geräten mit dem Netzwerk der Firma X oder dessen Kunden (z.B. über Netzwerkkabel) ist untersagt

2.2. Aufgabenstellung

Der Auftraggeber will, dass die Richtlinien konsequent angewendet und überwacht werden. Zusammenfassend sollen folgende Punkte beachtet werden:

- Nicht autorisierte Geräte (zum Beispiel private Laptops) sollen via VPN keine Verbindung ins Firmennetz herstellen können
- Firmengeräte sollen die Möglichkeit haben, sich aus dem Internet via VPN mit der Firma zu verbinden
- Der Zugriff auf das Firmennetzwerk soll überwacht werden können
- Analyse eines Firmengeräts, welche Eigenschaften es hat um als Firmengerät zu gelten

Damit diese Richtlinien und deren Aufgaben erfüllt werden können, müssen die folgenden Fragen beantwortet werden:

- Wie kann erreicht werden, dass unbefugte Geräte nicht Zugriff auf das Netzwerk der Firma aus dem Internet erhalten?
- Wie kann ein Client der Firma als solchen identifiziert werden?
- Welche Voraussetzungen muss ein Client für die erfolgreiche Verbindung ins Firmennetz erfüllen?
- Was passiert mit einem Client, der nicht autorisiert ist?
- Wie kann die Lösung sinnvoll über alle Clients der Firma verteilt werden?

Zusammengefasst muss analysiert werden, was ein Firmengerät als solches erkennbar macht. Anhand dieser Analyse wird definiert, welche Voraussetzungen für ein erfolgreiches Verbinden via VPN erfüllt werden müssen und was mit einem Gerät geschieht, dass nicht für einen Zugriff autorisiert ist.

Ein grober Ablaufplan des Projekts soll einen Überblick über das Projekt bieten.

Was	**Datum**
Projektstart	01. April 2022
Initialisierung	04. April 2022
Testen der Umgebung	04. April 2022
Erarbeitung Definition von Firmengeräten	04. April 2022
Tests abgeschlossen	30. April 2022
Implementation in der Firma	03. Mai 2022
Abgabe der Arbeit	16. Mai 2022

Tabelle 1: Grober Ablauf des Projekts

2.3. Ist-Situation

Die Mitarbeiter:innen bekommen von der Firma Laptops, Virtual Desktop Instances (VDI) und teils PC's mit Windows, Linux oder MacOS als Betriebssystem. Diese Geräte gehören dem Unternehmen, sie dürfen die Geräte zu Firmenzwecken benützen. Die private Nutzung des Internetzugangs ist als Ausnahme zu betrachten und erfolgt immer nach den Grundsätzen der Verhältnismässigkeit. Softwareinstallationen sind gemäss Reglement untersagt und müssen von der Abteilung «IT-Services» geprüft und genehmigt werden. Die Möglichkeit aus dem HomeOffice zu arbeiten erfreut sich weiterhin grosser Beliebtheit unter den Mitarbeiter:innen.

In der Firma werden hauptsächlich Laptops mit Windows 10 eingesetzt. Diese Tabelle widerspiegelt die ungefähre Situation der im Einsatz stehenden Geräte der Firma.

Betriebssystem	Art	Anzahl Geräte	Prozentsatz
Alle	Laptop, VDI, Desktop	200	100%
Windows 10 Pro/Enterprise	Laptop, VDI, Desktop	176	88%
Linux	Laptop	20	10%
MacOS	Laptop	4	2%

Tabelle 2: Aufteilung der Firmengeräte

Derzeit stehen den Mitarbeiter:innen drei Möglichkeiten zur Auswahl, wie von daheim oder unterwegs auf das Firmennetz zugegriffen werden kann:

1. Via Virtual Private Network (VPN), mit dem FortiClient
2. Via Citrix Infrastruktur
3. Via Citrix Zugriff auf Virtual Desktop Instance und von dort mit Remotedesktop auf ihr Firmengerät

2.3.1. Verbindung ins Firmennetz mittels FortiClient:

Derzeit kann nicht geprüft werden, ob ein via VPN verbundenes Gerät der Firma gehört oder ob es ein Privatgerät eines/einer Angestellten ist. Aus Bequemlichkeit oder anderen trivialen Gründen werden die Firmengeräte meist in der Firma gelassen. Die Firma stellt ihren Mitarbeiter:innen eine detaillierte Anleitung zum Einrichten eines Zuganges via VPN zur Verfügung, damit sie im HomeOffice arbeiten können. Die Angestellten können mithilfe dieser Anleitung eine VPN-Verbindung auf ihrem privaten Computer einrichten und nutzen. Grundsätzlich kann davon ausgegangen werden, dass Mitarbeiter:innen der Firma gegenüber nicht mit bösen Absichten handeln.

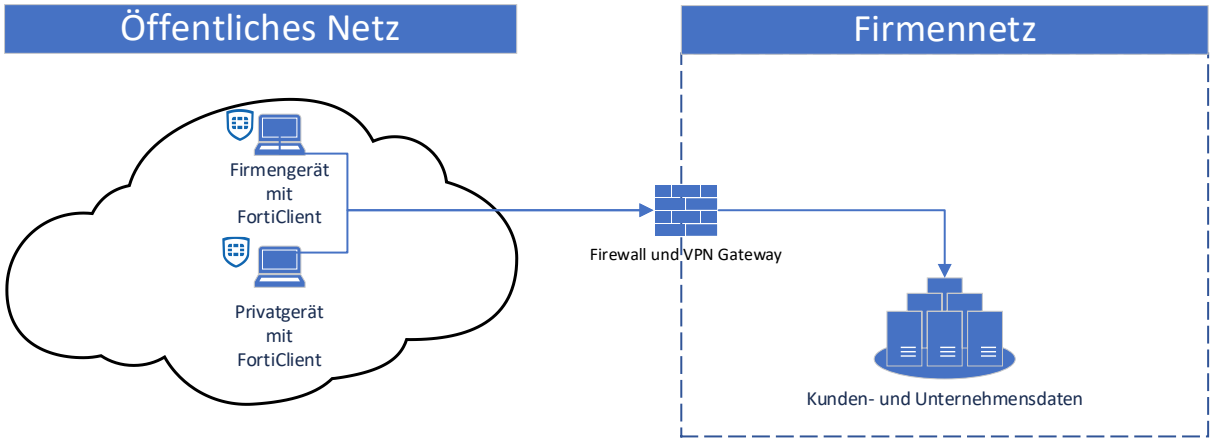


Abbildung 1: VPN-Verbindung via FortiClient

2.3.2. Verbindung ins Firmennetz via Citrix

Über die Citrix-Verbindung auf den Citrix Desktop der Firma wird den Mitarbeiter:innen erlaubt, auf das Firmennetz zuzugreifen. Mit dem Rollout der tragbaren Geräte und dem produktiven Einsatz von VPN, wird mittelfristig die Citrix-Umgebung der Firma Schritt für Schritt abgebaut. Die Geschäftsleitung hat entschieden, dass der Zugang auf Unternehmensdaten für Mitarbeiter:innen aus dem Internet in Zukunft nur noch über eine VPN-Verbindung funktionieren soll. Das Lifecycle Programm der Firma ist noch nicht vollständig abgeschlossen, weshalb weiterhin viele Angestellte mit dem Citrix Desktop von aussen auf das Firmennetz zugreifen. Durch den Abbau der internen Citrix Umgebung sollen zudem Kosten und Ressourcen gespart werden.

2.3.3. Verbindung ins Firmennetz via Citrix und Remote Desktop Protokoll (RDP)

Viele Mitarbeiter:innen (auch diese, die bereits ein Notebook von der Firma erhalten haben) lassen ihr Gerät in der Firma und schalten dieses nie aus. Wenn das Gerät läuft, können sie via Citrix und Remotedesktopverbindung auf das Firmengerät und damit auf sensible Daten zugreifen. Wird das Gerät nie ausgeschaltet werden auch keine wichtigen Updates installiert und das Gerät könnte eine Sicherheitslücke aufweisen.

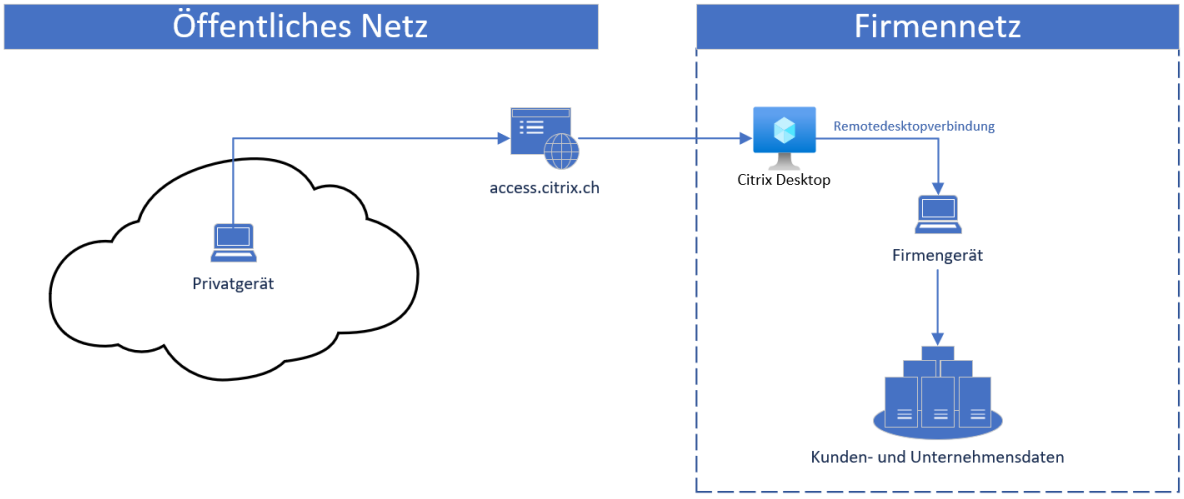


Abbildung 2: Verbindung ins interne Netzwerk via Citrix

2.4. Bestandteile des Systems

Die Lösung wird in einer Firma im Bereich «IT-Services» eingesetzt werden. Ist das Projekt erfolgreich durchgeführt, wird in einem nächsten Schritt die gesamte Firma mit dieser Lösung arbeiten. Der Bereich «IT-Services» soll umgesetzt werden.

Die produktiven Systeme müssen jederzeit erreichbar bleiben. Die Mitarbeiter:innen müssen sich aus dem HomeOffice weiterhin mit den oben genannten Varianten mit dem Firmennetz verbinden können. An den produktiven Systemen darf nicht getestet werden, weshalb eine Testumgebung bereitgestellt wird. Damit die Testumgebung als Referenz gültig ist, muss sie den produktiven Systemen wie Laptops oder Firewall nachempfunden sein. Im Optimalfall werden die gleichen Geräte in der Testumgebung verwendet wie in der produktiven Umgebung.

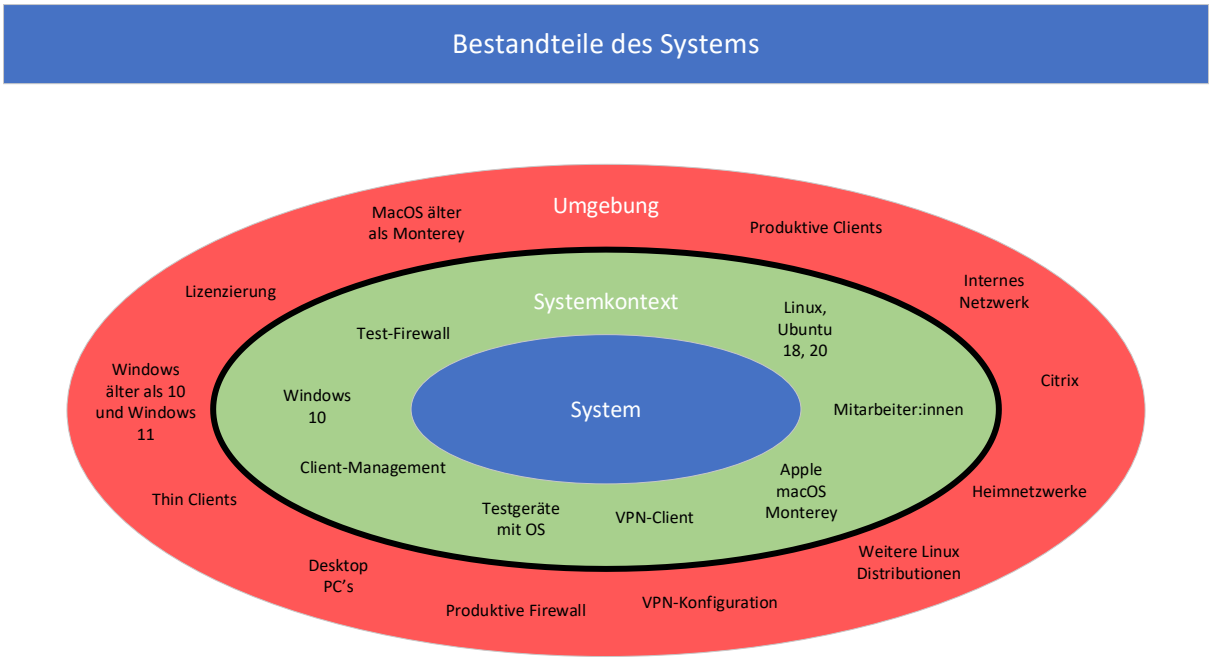


Abbildung 3: Bestandteile des Systems

Technische Bestandteile:

Die Lösung muss mit der Hardware der Firma kompatibel sein. Das Testsystem sollte darum mindestens folgende Hardwareanforderungen erfüllen:

- Fortinet Firewall
- Fortinet FortiClient VPN
- Windows 10 Notebook
- Linux Ubuntu 18 oder 20 Notebook
- MacBook mit Monterey 12.1

Personelle Bestandteile:

Im Sinne der Akteure sind nebst Auftraggeber und Product Owner auch das Client Management der Firma und die Mitarbeiter:innen betroffen.

Client Management:

Das Client Management ist ein Team aus mehreren Personen innerhalb des Bereichs «IT-Services». Diese sind bei der Erarbeitung der Lösung mit einzubeziehen. Die Lösung wird später mittels Client Management Software in der Firma ausgerollt und installiert.

Mitarbeiter:innen

Während die Lösung erarbeitet wird, sollen Mitarbeiter:innen mit einbezogen werden. Da sie zahlenmässig die grösste Anforderungsgruppe bilden, wird die Lösung mit einigen besprochen und Feedback eingeholt.

Umgebung

Die Umgebung zeigt auf, welche Systeme, Software oder Akteure während der Erarbeitung der Lösung zu vernachlässigen sind. Die Umgebung wird bei der Implementation der Lösung in der gesamten Firma eine wichtigere Rolle einnehmen. Die Testumgebung sollte deshalb der produktiven Umgebung möglichst ähnlich sein. Durch effektives Testing können so bereits Fehler gefunden und wenn möglich behoben werden.

2.5. Anforderungsanalyse

Personen, die von der eingesetzten Lösung betroffen sind, haben ihre eigenen Vorstellungen wie die Lösung auszusehen hat. Diese Bedürfnisse werden aus Sicht der Personen anhand Gesprächen und Eigeneinschätzung des Diplomanden analysiert und evaluiert. So wird definiert, wie die Lösung schlussendlich auszusehen hat, damit sie wirkungsvoll eingesetzt werden kann.

2.5.1. Anforderungsgruppen

2.5.1.1. Auftraggeber

Der Auftraggeber ist der Leiter des Bereichs IT-Services und Mitglied der Geschäftsleitung. Neben der Usability für die Nutzer:innen möchte er die allgemeine Sicherheit im Bereich der Remotezugänge erhöhen:

- «Als Leiter der IT-Sevices möchte ich, dass externe Zugriffe auf das Firmennetzwerk überwacht und aufgezeichnet werden.»
- «Mitarbeiter:innen sollen die Möglichkeit haben, sich vor der Anmeldung am Gerät mit dem internen Netzwerk zu verbinden. VPN vor Login»
- «Ich will, dass definiert werden kann was ein Firmengerät zu einem Firmengerät macht. Dafür möchte ich eine Analyse der aktuellen Geräte und welche Eigenschaften sie alle gemeinsam haben.»
- «Geräte, die nicht von der firmeneigenen IT ausgegeben werden, dürfen sich nicht aus dem Internet mit dem internen Netzwerk verbinden.»

2.5.1.2. Product Owner

Der Product Owner (PO) ist für den Entwicklungsprozess der Lösung zuständig. Die Anforderungen des Product Owners gehen in Richtung Funktionalität, Usability und Qualität der Lösung. Die Anforderungen des Product Owners variieren im Laufe des Projekts und können neu erstellt, geändert oder gelöscht werden.

- «Als Product Owner möchte ich eine Definition und Dokumentation darüber, was ein Firmengerät als solches erkennbar macht und wie es sich von externen Geräten unterscheidet.»
- «Ich will, dass Firmengeräte von Extern die Möglichkeit haben, sich mit dem Firmennetzwerk zu verbinden.»
- «Geräte, die nicht zum Zugriff auf das Firmennetz berechtigt sind, sollen blockiert werden.»
- «Anhand der verbunden Firmengeräte soll der zugehörige User ersichtlich sein.»

2.5.1.3. Client Management

Das Client Management ist ein Team aus mehreren Personen innerhalb des Bereichs «IT-Services». Es ist zuständig für die Verwaltung sämtlicher Clients, die in der Firma im Einsatz sind.

- «Als Teamleiter des Client Managements möchte ich, dass die Lösung über unser Client Management System verwaltbar ist.»
- «Die Software wird laufend aktualisiert und Updates werden uns zur Verfügung gestellt, damit diese auf die produktiven Clients ausgerollt werden kann.»
- «Sämtliche Änderungen und Updates werden mit meinem Team und mir besprochen. Dazu möchte ich vorgängig Wartungsfenster definieren und die Belegschaft informieren.»

2.5.1.4. Sicherheitsbeauftragter der Firma

Aus Sicht des Sicherheitsbeauftragten einer Firma mit über 160 Angestellten wird jede Lösung Schwächen haben. Die Anforderungen richten sich an den Schutz der Daten von Kunden, der Firma und der Benutzer:innen und die Sicherheit im Netzwerk gegen Angriffe.

- «Als Sicherheitsbeauftragter der Firma will ich, dass eine Analyse durchgeführt wird, was ein Firmengerät zu einem solchen macht. Ich möchte, dass eine Definition für Firmengeräte erstellt wird, die für die gesamte Firma gültig ist.»
- «Ich möchte, dass sich nur Firmengeräte aus dem Internet mit dem firmeninternen Netzwerk verbinden können.»
- «Erfüllt ein Firmengerät die Anforderungen nicht oder nicht mehr, soll dieses als externes Gerät betrachtet werden und der Zugriff via VPN blockiert werden.»
- «Sämtliche externen Geräte, die nicht zum Zugriff autorisiert sind, sollen sich nicht per VPN mit der Firma verbinden können.»

2.5.1.5. Mitarbeiter:innen

Die grösste Anforderungsgruppe sind mit über 160 Personen die Mitarbeiter:innen. Technisch hat diese Gruppe keine hohen Anforderungen. Für sie steht die Usability, das Aussehen und die Verfügbarkeit der Lösung im Zentrum.

- «Wir wollen, dass die Lösung jederzeit und von überall verfügbar ist.»
- «Während der Arbeit sollen keine Unterbrüche in der Verbindung ins Firmennetz auftreten.»
- «Das Herstellen der Verbindung soll möglichst einfach und verständlich sein.»
- «Vorhandene Desktopverknüpfungen sollen nach der Umstellung wieder am gleichen Platz vorhanden sein.»
- «Während der Arbeit im Firmennetz von Extern, sollen alle Ressourcen zugänglich sein und keine wichtigen Arbeitssysteme blockiert werden.»

2.5.1.6. Geschäftsleitung

Für den Auftraggeber und die anderen Mitglieder der Geschäftsleitung stehen die finanziell benötigten Mittel im Zentrum. Die Lösung muss mehr Nutzen bringen als sie Kosten verursacht. Eine Kosten/Nutzen-Analyse wird in einem weiteren Schritt erstellt.

- «Wir möchten, dass die investierten Gelder genutzt werden, um die Firma, ihre Mitarbeiter:innen, Partner und Kunden besser gegen Bedrohungen aus dem Internet zu schützen.»

2.5.2. Funktionale Anforderungen

Die funktionalen Anforderungen bestimmen, was in der Lösung enthalten sein muss. Beispielsweise soll die VPN-Verbindung vor dem Windows-Login möglich sein. Eine nicht funktionale Anforderung wäre beispielsweise, dass die Lösung in den Unternehmensfarben gestaltet wird. Die Eigenschaften der VPN-Verbindung an sich sind in den nicht-funktionalen Anforderungen, da sie bereits vorhanden sind und nicht bearbeitet werden.

In der folgenden Tabelle wird die Abkürzung «Req.» für Requirement benutzt.

Req. Nr.	Anforderung	Anforderungsgruppe
Req1	Definieren, was ein Firmengerät zu einem Firmengerät macht	Product Owner, Auftraggeber, Sicherheitsbeauftragter
Req2	Definition von Anforderungen an Clients, die es zu erfüllen gilt	Sicherheitsbeauftragter, Product Owner
Req3	Überwachung der Zugriffe auf das interne Netzwerk	Auftraggeber, Sicherheitsbeauftragter
Req4	Zugriff über VPN nur von Firmengeräten erlauben	Sicherheitsbeauftragter, Mitarbeiter:innen, Product Owner, Auftraggeber
Req5	Isolieren von Geräten, die nicht von der Firma stammen und sich via VPN zu verbinden versuchen	Sicherheitsbeauftragter, Product Owner, Auftraggeber
Req6	Erkennen von Firmengeräten, die sich via VPN verbinden	Sicherheitsbeauftragter, Product Owner, Auftraggeber
Req7	Isolation von Firmengeräten, die die definierten Anforderungen nicht vollständig erfüllen	Sicherheitsbeauftragter, Auftraggeber, Product Owner
Req8	VPN vor Login bei Windows Geräten einrichten	Auftraggeber, Mitarbeiter:innen

Tabelle 3:Funktionale Anforderungen

2.5.3. Nicht-funktionale Anforderungen

Req. Nr.	Anforderung	Anfoderungsgruppe
Req9	Hohe Stabilität der VPN-Verbindung, keine Timeouts	Mitarbeiter:innen
Req10	VPN-Verfügbarkeit jederzeit und von überall möglich	Mitarbeiter:innen, Auftraggeber
Req11	Keine Einschränkungen der Zugriffe während der VPN-Verbindung	Mitarbeiter:innen
Req12	Möglichst identischer Ablauf zum Herstellen einer Verbindung	Mitarbeiter:innen
Req13	Verknüpfungen auf Desktop und Icons der Lösung sollen gleich sein	Mitarbeiter:innen
Req14	Der Mehrwert für die Firma übersteigt die Kosten der Lösung	Geschäftsleitung
Req15	Die Lösung ist durch das Client Management der Firma verwaltbar	Client Management
Req16	Die Lösung wird laufend aktualisiert	Client Management, Sicherheitsverantwortlicher

Tabelle 4: Nicht-funktionale Anforderungen

2.5.4. Anforderungsbewertung

Die Anforderungen zusätzlich nach ihrer Priorität bewertet. Je nach Anforderungsgruppe können diese stark unterscheiden. Die Skala wird von 1 = unwichtig bis 5 = kritisch unterschieden. Aus der Summe ergibt sich die Wertung der verschiedenen Anforderungen.

Nr.	Product Owner	Mitarbeiter:innen	Sicherheitsverantwortlicher	Geschäftsleitung	Auftraggeber	Client Management	Summe
Req1	4	1	5	1	5	2	**18**
Req2	4	1	5	1	3	3	**17**
Req3	5	1	5	1	5	1	**18**
Req4	5	5	5	3	4	2	**24**
Req5	5	1	5	3	4	1	**19**
Req6	4	1	5	1	4	1	**16**
Req7	4	1	5	1	4	1	**16**
Req8	1	4	1	1	4	1	**12**
Req9	3	4	2	1	2	1	**13**
Req10	2	4	2	1	3	1	**13**
Req11	2	4	2	1	2	1	**12**
Req12	1	4	1	1	1	1	**9**
Req13	1	4	1	1	1	1	**9**
Req14	1	1	1	5	4	1	**13**
Req15	1	1	2	1	1	4	**10**
Req16	2	1	3	1	3	4	**14**

Tabelle 5: Bewertung der Anforderungen

Anhand der Summe wird mittels Punktesystem bestimmt, welche Anforderungen am wichtigsten sind. Das Punktesystem unterscheidet zwischen 4 Stufen. Die Maximale Anzahl an Punkten beträgt 30.

Punktesystem:

6– 11 Punkte	Unwichtig, zu vernachlässigen
12 – 17 Punkte	Wichtig
18 – 23 Punkte	Sehr Wichtig
24 – 30 Punkte	Kritisch

Wichtigkeit	Anforderungen	Anzahl
Unwichtig, zu vernachlässigen	Req12, Req13, Req15	3
Wichtig	Req2, Req6, Req7, Req8, Req9, Req10, Req11, Req14, Req16	9
Sehr wichtig	Req1, Req3, Req5	3
Kritisch	Req4	1

Tabelle 6: Übersicht Punktesystem der Anforderungen

Das Ergebnis zeigt auf, dass die meisten Anforderungen nicht von allen Anforderungsgruppen gleich gewichtet werden. Umso wichtiger sind die Anforderungen, die über alle Gruppen hinweg als relevant dienen. Die Anforderungsgruppen wurden mithilfe dieser Tabelle befragt. Die relevanten Anforderungen werden nun noch genauer erläutert.

Unwichtig, zu vernachlässigen

Req12: Möglichst identischer Ablauf zum Herstellen einer Verbindung

- Wird von den Benutzer:innen gewünscht, aufgrund bisherigem Verfahren. Gewohnheiten werden möglichst beachtet, sind aber bei der Implementation zu vernachlässigen

Req13: Verknüpfungen auf Desktop und Icons der Lösung sollen gleich sein

- Mitarbeiter:innen sind sich gewohnt, wie die Verbindung ins VPN abläuft. Diese Gewohnheiten sind zu vernachlässigen, nach Möglichkeit wird aber Rücksicht auf das bisherige Verfahren genommen.

Req15: Die Lösung ist durch das Client Management der Firma verwaltbar

- Die Lösung im eigenen «Software-Kiosk» zu verwalten erhöht die Wartbarkeit auf den Endgeräten. Verfügt die Lösung über eine eigene Möglichkeit die Software zu verwalten, muss nicht zwingend das Client Management Tool der Firma verwendet werden.

Sehr wichtig:

Req1: Definieren, was ein Firmengerät zu einem Firmengerät macht

- Diese Definition wird über die gesamte Firma zum Einsatz kommen. Anhand dieser wird bestimmt, was ein Firmengerät ausmacht.

Req3: Überwachung der Zugriffe auf das interne Netzwerk

- Zur Nachverfolgung von Ereignissen wie Malware Befall, unautorisiertem Zugang oder das beheben von Zugriffsproblemen.

Req5: Isolieren von Geräten, die nicht von der Firma stammen und sich via VPN zu verbinden versuchen

- Sicherheitstechnisch die höchste Anforderung, damit sich unautorisierte Geräte nicht mit dem Firmennetz verbinden können.

Kritisch

Req4 – Zugriff über VPN nur von Firmengeräten erlauben

- Diese Anforderung ist zwingend notwendig. Der Zugriff auf das Firmennetzwerk ist von zentraler Bedeutung.

2.6. Projektplanung

Die Anforderungen an die Lösung können sich im Verlauf des Projekts ändern. Ein klassisches Wasserfallmodell mit linearen Phasen, die aufeinander aufbauen, wird nicht umsetzbar sein. Der PO kann die Anforderungen in Absprache mit den Anforderungsgruppen während des Projekts an das Produkt anpassen und verändern. Eine agile Projektmethode wie SCRUM oder Kanban können besser eingesetzt werden. In der Firma wird SCRUM benutzt, weshalb diese Methode durchaus Sinn ergibt. Damit SCRUM allerdings nutzbar wird, müssen diverse Anpassungen vorgenommen werden. Eine generelle Übersicht von SCRUM ist im Anhang A1, SCRUM Grundlagen ersichtlich.

2.6.1. Eingesetzte SCRUM-Methode

Zusammen mit dem Product Owner (PO) ist die Definition of Done (DoD) spezifiziert und Scrum auf die Bedürfnisse und Anforderungen des Projektes angepasst. Einige Aspekte von Scrum fallen ganz weg.

Definition of Done (DoD)

«Die Aufgabe ist im Sinne der Aufgabe durchgeführt und durch den Product Owner begleitet worden. Dokumentation über mögliche Einstellungen und "Defaults" muss erstellt und peer-reviewed sein. Alle funktionalen Tests müssen erfolgreich durchgeführt worden sein.»

Team

Das Team besteht aus dem Diplomanden, einem IT-Service Architekten und punktuell Spezialisten aus angrenzenden Bereichen.

Scrum Master

Auf den Einsatz eines Scrum-Masters wird aufgrund der geringen Grösse des Teams verzichtet. Die Meetings werden durch den PO geführt.

Sprint Planning

Das Sprint Planning findet am Montagmorgen mit dem Team und dem Product Owner statt. Der Product Owner definiert die zu erledigenden Tasks.

Daily Scrums

Aufgrund der Grösse der Teams werden keine Daily Scrums geführt. Sollten grössere Probleme auftreten nimmt der Diplomand direkt mit dem PO Kontakt auf und informiert ihn über die Unstimmigkeiten.

Sprint Review

Das Sprint Review wird jeweils mit dem PO am Freitagnachmittag innerhalb eines Sprints gehalten.

Sprint Retrospektive

Die Retrospektive wird jeweils am Montag nach Abschluss eines Sprints und vor dem Beginn des Sprint Plannings gehalten.

Projektdauer

Das Projekt dauert insgesamt 6 Wochen. Start ist der 1. April 2022 und Abgabe ist am 16. Mai 2022.

Sprints

Die Sprints sind in Absprache zwischen dem Diplomanden und dem PO definiert. Es werden 4 Sprints durchgeführt, während zwei Wochen für die Dokumentation benötigt werden. Ein Sprint dauert eine Woche. Ein Sprint beginnt und endet jeweils an Montagen.

StoryPoints

Den Tasks werden Gewichtungen in Form von StoryPoints vergeben. Zur Planung wird durch das Team festgelegt, dass ein StoryPoint = 4 Stunden Arbeitsaufwand bedeutet. Die StoryPoints können auch in Brüchen (z.B.: 1/2 StoryPoint = 2 Stunden) angewandt werden.

Zusammenfassung

Der Projektstart ist am 1. April 2022 und dauert 6 Wochen. Abgabetermin ist der 16. Mai 2022. Insgesamt sollen 4 Sprints stattfinden. Der erste Sprint beginnt am 4. April 2022. Die Sprints dauern jeweils eine Woche und werden mit dem PO im Rahmen des Sprint Planning besprochen. Der PO bearbeitet das Product Backlog und entscheidet jeweils am Ende des Sprints während des Sprint Reviews über das weitere Vorgehen.

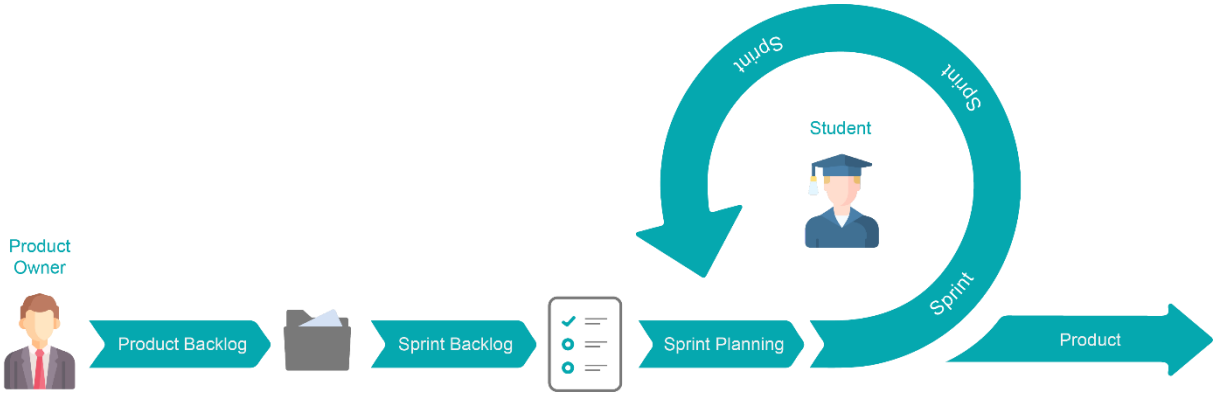


Abbildung 4: Geänderte Scrum Methode

2.7. Ziele

Die Anforderungen aller beteiligten Personen, die Projektmethode und die Bestandteile des Systems sind definiert und geklärt. Als nächster Schritt werden die Ziele für den Projekterfolg erörtert. Die Ziele werden anhand der Anforderungen abgeleitet und als Ziele umformuliert. Die Ziele werden dem Auftraggeber vorgelegt und von ihm abgesegnet.

Req. Nr.	Anforderung
Req1	Definieren, was ein Firmengerät zu einem Firmengerät macht
Req2	Definition von Anforderungen an Clients, die es zu erfüllen gilt
Req3	Überwachung der Zugriffe auf das interne Netzwerk
Req4	Zugriff über VPN nur von Firmengeräten erlauben
Req5	Isolieren von Geräten, die nicht von der Firma stammen und sich via VPN zu verbinden versuchen
Req6	Erkennen von Firmengeräten, die sich via VPN verbinden
Req7	Isolation von Firmengeräten, die die definierten Anforderungen nicht vollständig erfüllen
Req8	VPN vor Login bei Windows Geräten einrichten
Req9	Hohe Stabilität der VPN-Verbindung, keine Timeouts
Req10	VPN-Verfügbarkeit jederzeit und von überall möglich
Req11	Keine Einschränkungen der Zugriffe während der VPN-Verbindung
Req12	Möglichst identischer Ablauf zum Herstellen einer Verbindung
Req13	Verknüpfungen auf Desktop und Icons der Lösung sollen gleich sein
Req14	Der Mehrwert für die Firma übersteigt die Kosten der Lösung
Req15	Die Lösung ist durch das Client Management der Firma verwaltbar
Req16	Die Lösung wird laufend aktualisiert

Tabelle 7: Übersicht Anforderungen

2.7.1. Zieldefinition und Priorisierung

Die Ziele werden anhand der «smart»-Methode erstellt. Mithilfe dieser Methode werden die Ziele so formuliert, dass sie spezifisch, messbar und terminiert sind.

2.7.1.1. Spezifisch

Es gilt zu spezifizieren, was verbessert werden muss und wie diese Verbesserung erreicht werden kann.

2.7.1.2. Messbar

Damit ein Ziel messbar wird, sollen Zahlen genannt werden. Vage Formulierungen wie «Anrufe müssen vermehrt angenommen werden» sind zu vermeiden. Messbar bedeutet in diesem Beispiel: «Anrufe müssen zu 95% angenommen werden».

2.7.1.3. Akzeptieren

Mitarbeiter:innen die von den Zielen betroffen sind, müssen mit diesen Zielen einverstanden sein.

2.7.1.4. Realistisch

Sind die Ziele utopisch gestaltet und unrealistisch zu erreichen, sollten daraus Teilziele entstehen die realistischer sind. Wird ein Ziel unrealistisch formuliert, wirkt sich dies demotivierend auf die Mitarbeiter:innen aus.

2.7.1.5. Terminiert

Ein Ziel muss ordentlich terminiert werden. Es empfiehlt sich, für das Erreichen des Ziels einen exakten Zeitpunkt zu nennen.

2.7.2. Zielbewertung

Die zu definierenden Ziele werden mit dem Auftraggeber in verschiedene Kategorien unterteilt. Es wird zwischen den folgenden Priorisierungen unterschieden:

2.7.2.1. MUSS-Ziel:

Diese Ziele müssen erreicht werden und dürfen sich während der Erarbeitung des Projekts nicht verändern. Werden diese nicht erreicht ist das Projekt ganz (oder teilweise) gescheitert.

2.7.2.2. SOLL-Ziel:

SOLL-Ziele werden vom Auftraggeber explizit gewünscht. Anders als die MUSS-Ziele können sie während dem Projekt in Absprache mit dem Auftraggeber geändert oder gelöscht werden.

2.7.2.3. KANN-Ziel:

Die KANN-Ziele sind in der Priorität zuunterst anzutreffen. Meist sind es Ziele, die kosmetischer Natur oder «nice-to-have» sind. KANN-Ziele sind für den Erfolg des Projektes nicht relevant und können laufend geändert oder gelöscht werden.

Die Ziele sind «smart» gestaltet und aus den Anforderungen abgeleitet. Die Ziele sind zusammen mit dem Auftraggeber vereinbart und priorisiert. Folgende Ziele sind definiert:

Nr.	Ziel	Req. Nr.	Priorität
1	Ein Windows-Firmengerät kann von einem «Standard-Gerät» unterschieden werden	1, 2, 4, 5	MUSS
2	Die Lösung erkennt ein Firmengerät anhand definierter Eigenschaften	1, 2, 4, 6, 7	MUSS
3	Die Lösung erkennt innerhalb von 1 Minute, wenn ein Firmengerät nicht mehr den Anforderungen entspricht	3, 5, 7	MUSS
4	Ist ein Firmengerät nicht mehr unternehmenskonform wird das Gerät innert 10 Sekunden nach Erkennung vom Netzwerk isoliert	3, 5, 7	MUSS
5	Ist ein Gerät nicht autorisiert wird eine entsprechende Meldung ausgegeben	5	KANN
6	Die Lösung kann anhand des Firmengerätes bestimmen welches Operating System (OS) auf dem Gerät läuft und kann dies kennzeichnen	6	KANN
7	Die Testumgebung ist am 4. April einsatzbereit	-	MUSS
8	Das Windows-Testgerät entspricht dem Standard-Setup der Firma und ist aktualisiert	6	SOLL
9	Das Linux-Testgerät entspricht dem Standard-Setup der Firma und ist aktualisiert	6	SOLL
10	Das macOS-Testgerät läuft unter der aktuellen macOS Version 12, Monterey	6	SOLL
11	Das Testen ist bis am 30 April vollumfänglich abgeschlossen und Fehler sind bekannt und in Bearbeitung oder behoben	-	MUSS
12	Der Einsatz der Lösung soll bis am 16. Mai erfolgen	-	SOLL
13	Ein nicht konformes Gerät hat zu keinem Zeitpunkt Zugriff auf sensible Daten, wenn es per VPN verbunden ist	3, 5, 7	MUSS
14	VPN-Verbindung wird innert 20 Sekunden erfolgreich aufgebaut	6, 8, 9, 10, 12	MUSS
15	Windows-Benutzer:innen können sich mit VPN vor Login anmelden	8, 10, 12	SOLL
16	Die Kosten für das Projekt belaufen sich jährlich unter 5'000 CHF	14	SOLL
17	Bei einer Verbindung mit VPN hat ein konformes Gerät immer Zugriff auf entsprechende Ressourcen	11	SOLL

Tabelle 8: Zieldefinition und Priorisierung

Die MUSS-Ziele sind teilweise nicht von vielen Anforderungsgruppen gefordert. Allerdings haben sicherheitskritische Ziele für den Product Owner, den Auftraggeber und den Sicherheitsverantwortlichen höchste Priorität.

MUSS-Ziele:

Ziel 1: Ein Windows-Firmengerät kann von einem «Standard-Gerät» unterschieden werden

- Um einem Firmengerät den Zugriff auf das interne Netzwerk zu gewähren, muss dieses zwingend als solches erkannt werden und sich von der breiten Masse unterscheiden

Ziel 2: Die Lösung erkennt ein Firmengerät anhand definierter Eigenschaften

- Damit ein Firmengerät von einem anderen Gerät unterschieden werden kann, müssen die Eigenschaften der Firmengeräte bekannt sein

Ziel 3: Die Lösung erkennt innerhalb von 1 Minute, wenn ein Firmengerät nicht mehr den Anforderungen entspricht

- Sollten auf dem Gerät Eigenschaften verloren gehen, die es als Firmengerät kennzeichnen muss die Lösung dies erkennen und entsprechend handeln

Ziel 4: Ist ein Firmengerät nicht mehr unternehmenskonform wird das Gerät innert 10 Sekunden nach Erkennung vom Netzwerk isoliert

- Wird ein Firmengerät als solches aberkannt, soll das Gerät isoliert und analysiert werden

Ziel 7: Die Testumgebung ist am 4. April einsatzbereit

- Damit erfolgreich und effektiv getestet werden kann, muss die Testumgebung bereitstehen

Ziel 11: Das Testen ist bis am 30 April vollumfänglich abgeschlossen und Fehler sind bekannt und in Bearbeitung oder behoben

- Bis zu diesem Datum müssen allfällige Bugs, Fehler und Probleme diagnostiziert, dokumentiert und Massnahmen getroffen sein.

Ziel 13: Ein nicht konformes Gerät hat zu keinem Zeitpunkt Zugriff auf sensible Daten, wenn es per VPN verbunden ist

- Stellt ein nicht Gerät eine Verbindung ins interne Netzwerk der Firma her, darf dieses zu keinem Zeitpunkt Zugriff auf sensible Daten haben

Ziel 14: VPN-Verbindung wird innert 20 Sekunden erfolgreich aufgebaut

- Um Timeouts und lange Wartezeiten zu vermeiden, muss die VPN-Verbindung innerhalb dieser Zeit aufgebaut werden

MUSS Ziele

Ziel Nr.	Ziel
1	Ein Windows-Firmengerät kann von einem «Standard-Gerät» unterschieden werden
2	Die Lösung erkennt ein Firmengerät anhand definierter Eigenschaften
3	Die Lösung erkennt innerhalb von 1 Minute, wenn ein Firmengerät nicht mehr den Anforderungen entspricht
4	Ist ein Firmengerät nicht mehr unternehmenskonform wird das Gerät innert 10 Sekunden nach Erkennung vom Netzwerk isoliert
7	Ein Windows-Firmengerät kann von einem «Standard-Gerät» unterschieden werden
11	Die Lösung erkennt ein Firmengerät anhand definierter Eigenschaften
13	Die Lösung erkennt innerhalb von 1 Minute, wenn ein Firmengerät nicht mehr den Anforderungen entspricht
14	Ist ein Firmengerät nicht mehr unternehmenskonform wird das Gerät innert 10 Sekunden nach Erkennung vom Netzwerk isoliert

Tabelle 9: Übersicht MUSS Ziele

SOLL-Ziele

Ziel Nr.	Ziel
8	Das Windows-Testgerät entspricht dem Standard-Setup der Firma und ist aktualisiert
9	Das Linux-Testgerät entspricht dem Standard-Setup der Firma und ist aktualisiert
10	Das macOS-Testgerät läuft unter der aktuellen macOS Version 12, Monterey
12	Der Einsatz der Lösung soll bis am 16. Mai erfolgen
15	Windows-Benutzer:innen können sich mit VPN vor Login anmelden
16	Die Kosten für das Projekt belaufen sich jährlich unter 5'000 CHF
17	Bei einer Verbindung mit VPN hat ein konformes Gerät immer Zugriff auf entsprechende Ressourcen

Tabelle 10: Übersicht SOLL-Ziele

KANN-Ziele

Ziel Nr.	Ziel
5	Ist ein Gerät nicht autorisiert wird eine entsprechende Meldung ausgegeben
6	Die Lösung kann anhand des Firmengerätes bestimmen welches Operating System (OS) auf dem Gerät läuft und kann dies kennzeichnen

Tabelle 11: Übersicht KANN-Ziele

Mit der Definition der Ziele und deren Priorisierung folgt der nächste Schritt. Es soll eine Lösung gefunden werden, die diese Anforderungen und Ziele erfüllen kann.

3. Realisierung

3.1. Einführung in FortiClient EMS

Um das Verständnis für den FortiClient EMS in den weiteren Kapiteln zu gewährleisten, wird ein kurzer Überblick über die wichtigsten Funktionen des EMS gewährt. Die detaillierte Beschreibung von EMS erfolgt in den jeweiligen Sprints.

3.1.1. Dashboard

Im Dashboard des EMS befinden sich wichtige Informationen zum EMS selber, wie Seriennummer oder Hostname der Instanz. Es gibt ebenfalls Auskunft über den Status der verbunden Endpoints.

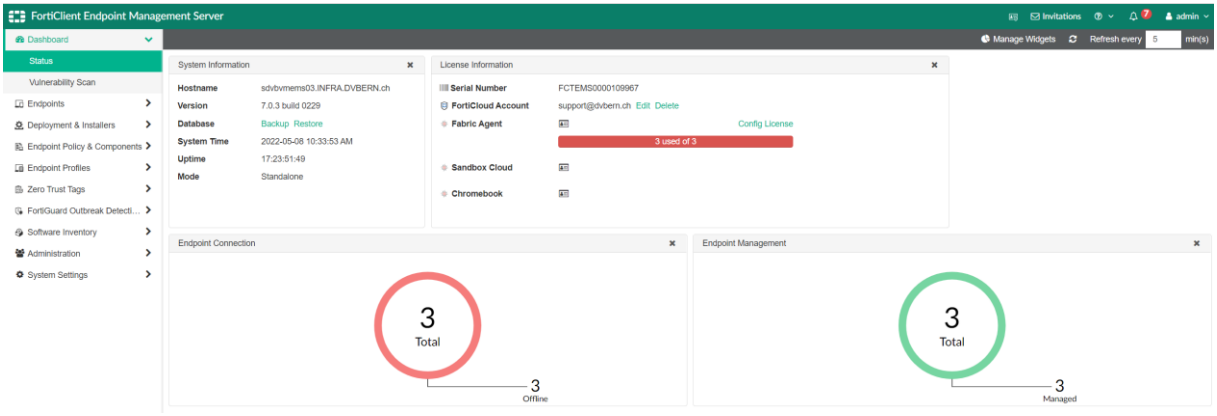


Abbildung 5: Graphical User Interface des EMS

3.1.2. Endpoints

Dient zur Verbindung mit einem Active Directory Server, um Endpoints in den EMS zu laden. Die Endpoints lassen sich nach bestimmten Kriterien filtern und anzeigen. Damit ein Endpoints als «managed» gilt, muss der FortiClient auf dem Gerät installiert sein. Zusätzlich muss das Gerät mittels Telemetry Key mit dem EMS verbunden werden. Dieser Key wird im EMS definiert und wird später am FortiClient des zu verbindenden Endpoints eingegeben, um die Verbindung zum EMS herzustellen und zu verwalten. Ist ein Endpoint mit EMS verbunden, meldet er sich jede Minute beim EMS, ob Updates oder Aktualisierungen verfügbar sind.

3.1.3. Deployment und Installers

Windows und macOS-Installers für FortiClient können mit gewissen Einschränkungen im EMS erstellt werden. So kann einem Installer der Telemetry Key zur Verbindung mit EMS mit der Installation mitgegeben werden. Der Endpoint sollte sich nach der Installation direkt mit dem EMS verbinden.

3.1.4. Endpoint Policy & Components

Die definierten Endpoint Profiles lassen sich in den Policies auf die Endpoints anwenden.

3.1.5. Endpoint Profiles

Einstellungen zu Remote Access, Webfilter und weiteren Einstellungen, die durch den Endpoint Management Server verwaltet und auf die Endpoints angewendet werden.

3.1.6. Zero Trust Tags

Endpoints können anhand ihres Betriebssystems, Registry Keys und weiteren Indikatoren mit einem Tag markiert werden. Anhang dieser Tags lassen sich die Endpoints weiter gruppieren. Die Tags können auf die Firewall synchronisiert werden und dort in den Firewall Policies genutzt werden, um Firmengeräte den Zugriff auf das Netzwerk zu erlauben und unbekannte Geräte auszuschliessen.

3.1.7. Administration

Verwalten von Benutzer und Administratoren. Über dieses Menü wird auch die Verbindung zur FortiGate Firewall mittels «Fabric Devices» hergestellt.

3.1.8. System Settings

Generelle Einstellungen zum Endpoints Management Server wie die Konfiguration von Logfiles, Hostname und welche Features genutzt werden.

3.2. Lösungsfindung und Variantenvergleich

Durch die technische Infrastruktur der Firma und die dadurch entstehende Abhängigkeit von Fortinet sind bereits einige Komponenten vorgegeben. So muss die Implementation innerhalb der bestehenden Lösungen erfolgen.

Dazu gehören:

- « FortiClient Endpoint Management Server (EMS) »
    - Serversoftware des Herstellers Fortinet, die Endpoints (Laptops, Computer) verwaltet
- « FortiGate Firewall (VPN) »
    - Eine Firewall des Herstellers Fortinet

Durch die Einschränkungen der Komponenten, die benutzt werden können, ergeben sich drei Lösungsvarianten. Diese Varianten werden untereinander verglichen und bewertet. Anhand der definierten Ziele werden Bewertungskriterien erstellt und auf die Varianten angewendet und verglichen.

3.2.1. Lösungsvariante 1: Hardware-Adressen basierte Liste auf der Firewall pflegen

Die Hardware-Adresse (auch als MAC-Adresse bekannt) kann jedem Gerät in einem Netzwerk eindeutig zugeordnet werden. Jedes netzwerkfähige Gerät verfügt über eine MAC-Adresse, damit dieses eindeutig identifiziert werden kann. Mithilfe dieser physikalischen Adresse kann auf der Firewall der Firma eine Liste mit Geräten erstellt werden, die auf das interne Netzwerk zugreifen dürfen.

3.2.2. Lösungsvariante 2: ZTNA-Tags im Endpoint Management Server (EMS)

Im EMS können Geräte, die mit einem FortiClient VPN Client ausgestattet sind, verwaltet werden. Die Firma nutzt bereits den FortiClient um eine VPN Verbindung in das Firmennetz aufzubauen. Die Endpoints können mit dem EMS verbunden und mit ZTNA-Tags (Zero Trust Network Access) bestückt werden. Durch die Definition der Tags kann eine Zutrittskontrolle erstellt werden. Endpoints, die einen bestimmten Tag besitzen, können ein- oder ausgeschlossen werden. Dabei kann eine variable Anzahl an Tags definiert werden. Geräte, die nicht mit dem EMS verbunden sind, können sich nicht am VPN anmelden.

3.2.3. Lösungsvariante 3: Client-Identifizierung mittels Zertifikats

Zur Identifikation und Verifikation von Endpoints können Zertifikate benutzt werden. Clients, die im Besitz dieses Zertifikats sind, werden zum Zugriff auf das interne Netzwerk autorisiert. Geräte ausserhalb der Firma oder Firmengeräte, die das Zertifikat nicht installiert haben, wird der Zugriff verweigert.

3.2.4. Nutzwertanalyse

Zur Bewertung der Lösungsvarianten werden aus den definierten Zielen Kriterien abgeleitet. Diese Kriterien gilt es zu gewichten, da gewisse Kriterien wichtiger sind als andere. Die Gewichtung wird in Punkten angegeben. Für die Gewichtung werden insgesamt 100 Punkte auf die verschiedenen Kriterien verteilt. Der Bewertungsmassstab gibt an, wie gut ein Kriterium erfüllt wird.

Diese Ziele sind definiert:

Nr.	Ziel	Priorität
1	Ein Windows-Firmengerät kann von einem «Standard-Gerät» unterschieden werden	MUSS
2	Die Lösung erkennt ein Firmengerät anhand definierter Eigenschaften	MUSS
3	Die Lösung erkennt innerhalb von 1 Minute, wenn ein Firmengerät nicht mehr den Anforderungen entspricht	MUSS
4	Ist ein Firmengerät nicht mehr unternehmenskonform wird das Gerät innert 10 Sekunden nach Erkennung vom Netzwerk isoliert	MUSS
5	Ist ein Gerät nicht autorisiert wird eine entsprechende Meldung ausgegeben	KANN
6	Die Lösung kann anhand des Firmengerätes bestimmen welches Operating System (OS) auf dem Gerät läuft und kann dies kennzeichnen	KANN
7	Die Testumgebung ist am 4. April einsatzbereit	MUSS
8	Das Windows-Testgerät entspricht dem Standard-Setup der Firma und ist aktualisiert	SOLL
9	Das Linux-Testgerät entspricht dem Standard-Setup der Firma und ist aktualisiert	SOLL
10	Das macOS-Testgerät läuft unter der aktuellen macOS Version 12, Monterey	SOLL
11	Das Testen ist bis am 30 April vollumfänglich abgeschlossen und Fehler sind bekannt und in Bearbeitung oder behoben	MUSS
12	Der Einsatz der Lösung soll bis am 16. Mai erfolgen	SOLL
13	Ein nicht konformes Gerät hat zu keinem Zeitpunkt Zugriff auf sensible Daten, wenn es per VPN verbunden ist	MUSS
14	VPN-Verbindung wird innert 20 Sekunden erfolgreich aufgebaut	MUSS
15	Windows-Benutzer:innen können sich mit VPN vor Login anmelden	SOLL
16	Die Kosten für das Projekt belaufen sich jährlich unter 5'000 CHF	SOLL
17	Bei einer Verbindung mit VPN hat ein konformes Gerät immer Zugriff auf entsprechende Ressourcen	SOLL

Tabelle 12: Übersicht der Ziele für Kriterien

Anhand der Ziele werden die Kriterien gewonnen und gewichtet. Das stärkste Kriterium ist die Sicherheit. Dies geht aus den Anforderungen der Stakeholder in der Analysephase hervor. Weitere Kriterien an die Lösungen sind:

- Wartbarkeit und Support
- Personeller Aufwand
- Wirtschaftlichkeit
- Usability

Sicherheitskriterien	**MUSS Ziel**	**SOLL-Ziel**	**KANN-Ziel**	**Gewichtung**
Firmengerät von Standardgerät unterscheiden	1, 2,	6, 8, 9	5	**10**
Kein Zugriff auf Firmendaten für unbekannte Geräte	1, 2, 3, 4, 13			**15**
Das verbundene Gerät kann vom Netzwerk isoliert werden	1, 2, 3, 4, 13		5	**10**
Kein Zugriff auf Firmennetzwerk für kompromittierte Geräte	1, 2, 3, 4, 13			**15**
Überwachen der Zugriffe auf das interne Netzwerk	1, 2, 3, 4, 13, 17			**10**
Wartbarkeit und Support Kriterien	**MUSS Ziel**	**SOLL-Ziel**	**KANN-Ziel**	**Gewichtung**
Eingesetzte Firmengeräte sind aktuell	1	8, 9, 10		**5**
Lösung ist einfach aktuell zu halten	11	16		**5**
Arbeitsaufwand für Wartung ist niedrig	11	16		**5**
Personeller Aufwand	**MUSS Ziel**	**SOLL-Ziel**	**KANN-Ziel**	**Gewichtung**
Der personelle Aufwand zur Einrichtung der Lösung ist gering		16		**10**
Kriterien für Kosten	**MUSS Ziel**	**SOLL-Ziel**	**KANN-Ziel**	**Gewichtung**
Die laufenden Kosten übersteigen das Kostendach von jährlich 5000 CHF nicht	12	16		**10**
Usability Kriterien	**MUSS Ziel**	**SOLL-Ziel**	**KANN-Ziel**	**Gewichtung**
VPN vor Login mit FortiClient	7	15		**5**

Tabelle 13: Kriterien aus Zielen formulieren

Die Kriterien sind somit definiert und gewichtet. Nun müssen die drei Lösungsvarianten anhand dieser Kriterien miteinander verglichen werden. Dazu werden die jeweiligen Kriterien mithilfe eines Masstabes auf deren Erfüllungsgrad geprüft.

In dieser Nutzwertanalyse gilt der Massstab von:

- 1 = nicht erfüllt
- 2 = ungenügend erfüllt
- 3 = erfüllt
- 4 = gut erfüllt
- 5 = sehr gut erfüllt.

Die Berechnung des Teilnutzens ergibt sich aus dem Produkt zwischen Gewichtung und Bewertung. Für die Berechnung des Gesamtnutzens werden die Teilnutzen addiert. Die höchstmögliche Punktzahl ist demnach 5*100 = 500 Punkte.

Bewertungssystem des Gesamtnutzen:

400 - 500 Punkte = sehr gut

300 – 399 Punkte = gut

200 – 299 Punkte = genügend

Unter 200 Punkte = ungenügend

3.2.4.1. Nutzwertanalyse Variante 1: Hardware-Adressen Liste in der Firewall

Sicherheitskriterien	**Gewichtung**	**Bewertung (1-5)**	**Teilnutzen**
Firmengerät von Standardgerät unterscheiden	10	3	**30**
Kein Zugriff auf Firmendaten für unbekannte Geräte	15	4	**60**
Das verbundene Gerät kann vom Netzwerk isoliert werden	10	4	**40**
Kein Zugriff auf Firmennetzwerk für kompromittierte Geräte	15	1	**15**
Überwachen der Zugriffe auf das interne Netzwerk	10	3	**30**
Wartbarkeit und Support Kriterien	**Gewichtung**	**Bewertung (1-5)**	**Teilnutzen**
Eingesetzte Firmengeräte sind aktuell	5	2	**10**
Lösung ist einfach aktuell zu halten	5	2	**10**
Arbeitsaufwand für Wartung ist niedrig	5	2	**10**
Personeller Aufwand	**Gewichtung**	**Bewertung (1-5)**	**Teilnutzen**
Der personelle Aufwand zur Einrichtung der Lösung ist gering	10	2	**20**
Kriterien für Kosten	**Gewichtung**	**Bewertung (1-5)**	**Teilnutzen**
Die laufenden Kosten übersteigen das Kostendach von jährlich 5000 CHF nicht	10	3	**30**
Usability Kriterien	**Gewichtung**	**Bewertung (1-5)**	**Teilnutzen**
VPN vor Login mit FortiClient	5	4	**20**

Tabelle 14: Nutzwertanalyse der MAC-Adressen Liste

Bei einer Gewichtung von 100 Punkten und der Bewertung zwischen 1 und 5 wird deren Produkt berechnet. Die Summe der Teilnutzen ergibt den Gesamtnutzen. Für die Lösungsvariante heisst dies:

Erreichte Punktzahl: 275 von möglichen 500 Punkten

Fazit:

Die Sicherheitskriterien sind umsetzbar, es wird allerdings nur ein Indikator geprüft: Die Hardware-Adresse. Die MAC-Adresse kann mit wenig technischem Wissen geändert werden. Die Rede hier ist von MAC-Spoofing (Verschleierung). MAC-Spoofing kann auf einem beliebigen Rechner innert weniger Minuten umgesetzt werden. Dabei wird die MAC-Adresse des eigenen Rechners so geändert, dass sie der Adresse eines anderen Gerätes gleichkommt. Besteht Kenntnis einer MAC-Adresse eines Firmengeräts, kann dies für unautorisierten Zugriff auf das interne Netzwerk genutzt werden.

3.2.4.2. Nutzwertanalyse Variante 2: ZTNA-Tags im Endpoint Management Server

Sicherheitskriterien	**Gewichtung**	**Bewertung (1-5)**	**Teilnutzen**
Firmengerät von Standardgerät unterscheiden	10	5	**50**
Kein Zugriff auf Firmendaten für unbekannte Geräte	15	5	**75**
Das verbundene Gerät kann vom Netzwerk isoliert werden	10	4	**40**
Kein Zugriff auf Firmennetzwerk für kompromittierte Geräte	15	4	**60**
Überwachen der Zugriffe auf das interne Netzwerk	10	4	**40**
Wartbarkeit und Support Kriterien	**Gewichtung**	**Bewertung (1-5)**	**Teilnutzen**
Eingesetzte Firmengeräte sind aktuell	5	5	**25**
Lösung ist einfach aktuell zu halten	5	4	**20**
Arbeitsaufwand für Wartung ist niedrig	5	4	**20**
Personeller Aufwand	**Gewichtung**	**Bewertung (1-5)**	**Teilnutzen**
Der personelle Aufwand zur Einrichtung der Lösung ist gering	10	3	**20**
Kriterien für Kosten	**Gewichtung**	**Bewertung (1-5)**	**Teilnutzen**
Die laufenden Kosten übersteigen das Kostendach von jährlich 5000 CHF nicht	10	3	**30**
Usability Kriterien	**Gewichtung**	**Bewertung (1-5)**	**Teilnutzen**
VPN vor Login mit FortiClient	5	4	**20**

Tabelle 15: Nutzwertanalyse der ZTNA-Tags im EMS

Bei einer Gewichtung von 100 Punkten und der Bewertung zwischen 1 und 5 wird deren Produkt berechnet. Die Summe der Teilnutzen ergibt den Gesamtnutzen. Für die Lösungsvariante 2 heisst dies:

Erreichte Punktzahl: 400 von möglichen 500 Punkten

Fazit:

Die ZTNA-Tags des Endpoint Management Servers von Fortinet erfüllt alle Kriterien. Die Sicherheitsaspekte werden allesamt mit «gut» oder «sehr gut» erfüllt. Bei der Auswahl der Indikatoren für ein Firmengerät kann aus einem breiten Spektrum an Eigenschaften gewählt werden. Erhält ein Gerät den benötigten Tag nicht, wird der Netzwerkzugriff nicht gestattet.

3.2.4.3. Nutzwertanalyse Variante 3: Client Identifizierung mittels Zertifikats

Sicherheitskriterien	**Gewichtung**	**Bewertung (1-5)**	**Teilnutzen**
Firmengerät von Standardgerät unterscheiden	10	3	**30**
Kein Zugriff auf Firmendaten für unbekannte Geräte	15	5	**75**
Das verbundene Gerät kann vom Netzwerk isoliert werden	10	4	**40**
Kein Zugriff auf Firmennetzwerk für kompromittierte Geräte	15	2	**30**
Überwachen der Zugriffe auf das interne Netzwerk	10	4	**40**
Wartbarkeit und Support Kriterien	**Gewichtung**	**Bewertung (1-5)**	**Teilnutzen**
Eingesetzte Firmengeräte sind aktuell	5	4	**20**
Lösung ist einfach aktuell zu halten	5	4	**20**
Arbeitsaufwand für Wartung ist niedrig	5	4	**20**
Personeller Aufwand	**Gewichtung**	**Bewertung (1-5)**	**Teilnutzen**
Der personelle Aufwand zur Einrichtung der Lösung ist gering	10	1	**10**
Kriterien für Kosten	**Gewichtung**	**Bewertung (1-5)**	**Teilnutzen**
Die laufenden Kosten übersteigen das Kostendach von jährlich 5000 CHF nicht	10	1	**10**
Usability Kriterien	**Gewichtung**	**Bewertung (1-5)**	**Teilnutzen**
VPN vor Login mit FortiClient	5	4	**20**

Tabelle 16: Nutzwertanalyse der Client Identifizierung mittels Zertifikats

Bei einer Gewichtung von 100 Punkten und der Bewertung zwischen 1 und 5 wird deren Produkt berechnet. Die Summe der Teilnutzen ergibt den Gesamtnutzen. Für die Lösungsvariante 2 heisst dies:

Erreichte Punktzahl: 315 von möglichen 500 Punkten

Fazit:

Zertifikate für das Verifizieren eines Firmengeräts können genutzt werden. Der Zugriff für kompromittierte Geräte lässt sich über das Zertifikat nicht regeln. Es gibt nur einen Indikator für die Erkennung eines Firmengeräts. Das Zertifikat könnte von einem Firmengerät entwendet werden und so in falsche Hände gelangen, die der Firma Schaden zufügen wollen.

3.2.5. Variantenentscheid

Die zusammenfassende Gegenüberstellung der drei verglichenen Lösungsvarianten ergibt folgendes Bild:

Variante	Gesamtnutzen	Maximale Punktzahl	Differenz
Hardware-Adressen basierte Liste auf der Firewall	275	500	225
ZTNA-Tags im Endpoint Management Server	400	500	100
Client-Identifizierung mittels Zertifikats	315	500	185

Tabelle 17: Variantenentscheid

Mit 400 Punkten von möglichen 500, ist die Variante 2: ZTNA-Tags im Endpoint Management Server die beste Lösung.

Variante 1 erfüllt die Anforderungen genügend, besteht jedoch nur aus einem Indikator für die Unterscheidung zwischen Firmengerät und einem beliebigen Gerät. MAC-Spoofing kann von einem Laien durchgeführt werden, wenn die Hardwareadresse eines Firmengeräts bekannt ist. Eine Liste von über 160 MAC-Adressen auf der Firewall zu pflegen und aktuell zu halten bedingt einen hohen personell Aufwand. Gibt es Mutationen bei Mitarbeiter:innen, wie Eintritte oder Austritte, muss die Liste jeweils aktualisiert werden. Bei einem fehlerhaften Gerät muss dieses aus der Liste gestrichen werden und ein neues aufgenommen werden.

Variante 2 erfüllt die Anforderungen sehr gut. Der Endpoint Management Server kommt vom gleichen Hersteller wie die Firewall und der FortiClient. Die ZTNA-Tags im EMS bieten ein breites Spektrum an unterschiedlichen Indikatoren zur Erkennung von Firmengeräten. Das Management von Geräten ist schnell und unkompliziert. Der FortiClient bildet das Bindeglied zum EMS. Wird ein Gerät ersetzt oder ein neues Gerät eingerichtet muss lediglich die Verbindung zum EMS getrennt oder hergestellt werden. EMS ist skalierbar und erlaubt das zentralisierte Verwalten von Endpoints.

Variante 3 erfüllt die Anforderungen teilweise sehr gut. Der Verlust oder die Entwendung des Zertifikats sind allerdings eine reale Gefahr. Ein einziger Indikator reicht nicht aus. Um diese Lösung durchzuführen, wird viel Wissen mit Zertifikaten vorausgesetzt. Der Diplomand besitzt das nötige «Know-How» nicht, um eine solche Lösung anzustreben. Der Aufbau des benötigten Wissens würde den Zeithorizont des Projekts sprengen und hohe Kosten verursachen. Aus diesen Gründen wird diese Lösung nicht weiter verfolgt.

Somit wird die Variante 2: «ZTNA-Tags im Endpoint Management Server» gewählt. Die Voraussetzungen für das Umsetzen der Lösung müssen nun erarbeitet werden.

3.3. Voraussetzungen und benötigte Ressourcen

Zur Umsetzung der Lösung müssen gewisse Rahmenbedingungen erfüllt und Ressourcen vorhanden sein. Die Testumgebung ist bereits einige Male erwähnt, aber noch nicht spezifiziert worden. Diese Spezifikation der Ressourcen soll in diesem Kapitel erstellt werden.

3.3.1. Produktbezogene Rahmenbedingungen

Um den Endpoint Management Server von Fortinet zu betreiben, muss diverse Hard- und Software vorhanden sein:

Lizenzen für Endpoint Management Server

- Die Lizenzen für den produktiven EMS sind bereits vorhanden. Der EMS wird zusammen mit dem FortiClient, der in der Firma standardmässig als VPN-Client benutzt wird, lizenziert.

Windows-Server 2022 Standard für die Nutzung von EMS

- EMS wird auf einem lizenzierten Windows-Server installiert und betrieben. Die Beschaffung eines Servers ist notwendig.

Firewall ist mit dem EMS verbunden

- Die eingesetzte FortiGate ist mit dem EMS verbunden

3.3.2. Prozessbezogene Rahmenbedingungen

Damit der Endpoint Management Server mit den ZTNA Tags im Zeithorizont des Projekts getestet werden kann, müssen einige Bedingungen erfüllt sein:

Der Windows-Test-Server ist einsatzbereit

- Der Windows-Server für den Betrieb von EMS ist betriebsbereit

Die Testumgebung mit benötigter Hard- und Software ist einsatzbereit

- Eine FortiGate Firewall mit FortiOS muss verfügbar und für Testzwecke konfiguriert sein

Lizenzierung für Testumgebung

- Am produktiven System kann nicht getestet werden, eine Trial-Lizenz für FortiClient inkl. EMS muss vorhanden sein

VPN konfiguriert und funktional

- Die VPN-Verbindung ist konfiguriert und kann genutzt werden

3.3.3. Projektkosten

3.3.3.1. Personalaufwand

Für die ungefähre Berechnung der Kosten der Projektmitarbeiter:innen wird ein pauschaler Stundenansatz von 100 CHF / Stunde angenommen und wird über das gesamte Projekt berechnet.

Person	**Arbeit**	**Geschätzter Aufwand**	**Kosten**
IT-Architekt	Beratung bei Sicherheitstechnischen Aspekten	ca. 8 Stunden	800 CHF
Diplomand	Projektplanung, Initialisierung, Analysen, Testing, Durchführung, Dokumentation	ca. 180 Stunden	18'000 CHF
Product Owner	Bearbeitung Product Backlog, Erstellung Sprint Backlog. Teilnahme an Sprintreviews und Sprint Plannings	ca. 25 Stunden	2500 CHF
Fachbereichsleiter Client Management	Absprache zum Rollout von FortiClient	ca. 5 Stunden	500 CHF
Auftraggeber	Erteilung des Auftrags, Anwesenheit Sprint Reviews	ca. 10 Stunden	1000 CHF

Tabelle 18: Personalaufwand zur Umsetzung EMS

3.3.3.2. Kosten produktive Umgebung

3.3.3.2.1. Lizenzkosten

Bei den Lizenzkosten für den FortiClient ist die Lizenz für den On-Prem (Installation auf Windows Server der Firma) FortiClient EMS inkludiert. Es werden Lizenzen für die gesamte Firma bestellt. In der Firma arbeiten rund 160 Personen und die Lizenzen sind in 25er Schritten beim Verkaufspartner bestellbar. Die nächste Stufe der Lizenzierung sind 500 Lizenzen. Bei den Lizenzen sind sowohl der FortiClient auf den Endpoints, sowie auch der FortiClient EMS inbegriffen.

Abbildung 6: FortiClient Lizenz für 1 Jahr, 25 Endpoints

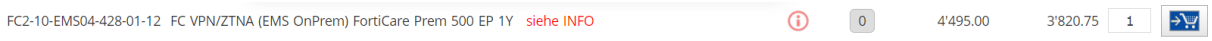


Abbildung 7: FortiClient Lizenz für 1 Jahr, 500 Endpoints

Es wird mit 175 Lizenzen für Endgeräte gerechnet. Ein Block mit 25 Lizenzen inkl. EMS Server kostet die Firma 471.75 CHF im Jahr, während die Lizenz für 500 Geräte jährlich 7475.75 CHF kostet.

Lizenz	Anzahl Lizenzen	Endpoints inkludiert	Dauer	Kosten
FortiClient EMS mit 25 Endpoints	1	25 Endpoints	1 Jahr	241.40 CHF
FortiClient EMS mit 25 Endpoints	7	175 Endpoints	1 Jahr	1689.80 CHF
FortiClient EMS mit 25 Endpoints	16	400 Endpoints	1 Jahr	3862.40 CHF
FortClient EMS mit 500 Endpoints	1	500 Endpoints	1 Jahr	3820.75 CHF

Tabelle 19: Kosten der FortiClient EMS Lizenzen

Die Lizenz mit 500 Endgeräten wird erst mit über 400 Geräten rentabel. Die Lizenzen sind jährlich anpassbar, sollte sich die Anzahl an Mitarbeiter:innen stark erhöhen.

3.3.3.2.2. Hardwarekosten

Die Kosten für den Betrieb einer Virtuellen Maschine wird monatlich abgerechnet. Die Firma bezahlt für den Betrieb eines virtuellen Windows Servers:

Gerät	Anzahl	Dauer	Kosten
VMware Virtual Machine, Windows Server 2019	1	1 Monat	270.00 CHF
VMware Virtual Machine, Windows Server 2019	1	1 Jahr	3240.00 CHF

Tabelle 20: Kosten für produktive Hardware

Als Microsoft-Partner erhält die Firma Serverlizenzen zum internen Gebrauch, die nicht verrechnet werden. Die Server-Lizenz für den Windows-Server mit EMS wird so abgerechnet. Die Lizenz wird folglich nicht weiterverrechnet.

3.3.3.3. Kosten Testumgebung

Die Netzwerkumgebung in der Firma ist komplex aufgebaut. Sämtliche Hardware und Serverlizenzen für die Testumgebung sind in der Firma oder beim Diplomanden vorhanden und müssen nicht zusätzlich erworben werden. Die Kosten für die Betreibung der Hardware und die Benutzung einer weiteren Internetverbindung sind intern und werden somit nicht weiter verrechnet. Die Lizenzierung der Produkte erfolgt über eine «Trial-Lizenz». Somit werden keine Lizenzierungskosten verursacht. Damit der EMS effektiv getestet werden kann, benötigt es folgende Geräte:

- FortiGate Firewall
- Windows Server für den Betrieb des Endpoint Management Servers
- 3 verschiedene Laptops mit den Betriebssystemen Windows, Linux und macOS
- Ethernet-Switch

Diese Hardware steht zum Erarbeiten der Lösung zur Verfügung:

Notebooks

Hostname	OS	Modell	Staging	Diverses
NBFIRMA-EMS-TEST	Windows 10 Pro	HP EliteBook 840 G5	Standard Services	Älteres Modell mit Lüfterproblemen
MacBook_Pro_von_lesa	macOS 12.3.1 Monterey	MacBook Pro, 2016	Standard MacBook Setup	Privatgerät
NBFIRMA157	Ubuntu 20	Dell XPS 15 9510	Firmenstandard	Aktuelles Entwicklergerät

Tabelle 21: Notebooks in Testumgebung

Firewall Cluster

Hostname	Hersteller	Model	Firmware	Diverses
Fwemstest01	Fortinet	FortiGate 500E	V6.4.7 build1911	
Fwemstest02 (Primary)	Fortinet	FortiGate 500E	V6.4.7 build1911	

Tabelle 22: Firewall in Testumgebung

Windows Server für EMS

Hostname	OS	IP	Gateway	Diverses
SFIRMAVMEMS03	Windows Server 2022 Standard	10.40.1.30	10.40.1.1	

Tabelle 23: Windows Server in Testumgebung

Endpoint Management Server

Hostname	FQDN	IP	Gateway	Diverses
SVMEMS03.INFRA.FIRMA.ch	Ems-test.firma.ch	10.40.1.30	10.40.1.1	Trial-Lizenz mit 3 FortiClients inkludiert

Tabelle 24: Endpoint Management Server in Testumgebung

3.3.4. Verwendete Software

Zur Erreichung der Ziele wird ein breites Spektrum an Software benötigt. Nebst der Software von FortiClient wird auch Software zur Erstellung von Abläufen, Bildern und Illustrationen benötigt. Diese Liste soll einen Überblick über die genutzte Software liefern.

Hersteller	Name	Nutzen	Version(en)
Fortinet	FortiClient	VPN Client	6.4.7+
Fortinet	FortiClient EMS	Endpoint Management	6.4.7+
Fortinet	FortiOS	Firewall Operating System	6.4.7+
HighSystems	HighSystem Client Management Tool	Client Management der Firma	9.8.003
Microsoft	Office 365 Apps for Enterprise	Dokumentationen schreiben	2203
Microsoft	Visio Plan 2	Abläufe beschreiben	2203
Adobe	InDesign	Illustrationen erstellen	17.2.1
ESET	ESET Endpoint Security	Antivirus	9.0.2046.0

Tabelle 25: Verwendete Software

3.3.5. Verwendung Erzeugnisse Dritter

Die Nachfolgenden Erzeugnisse können im laufenden Betrieb übernommen werden:

- Grundkonfiguration der Testumgebung mit Konfiguration Windows Server, Firewall, Netzwerk und EMS wird firmenintern zur Verfügung gestellt
- FortiClient, EMS und FortiOS Versionen, zur Verfügung gestellt von Fortinet
- Fortinet Dokumentationen zu EMS, FortiClient, FortiOS (Verschiedene Versionen)
- Release Notes zu EMS, FortiClient, FortiOS (verschiedene Versionen)
- New Features Guide zu EMS, FortiClient, FortiOS (verschiedene Versionen)

3.4. Risikoanalyse

Basierend auf den durchgeführten Analysen und der Definition der Lösung, wird zusätzlich eine Risikoanalyse durchgeführt. Diese soll mögliche Gefahren, deren Eintrittswahrscheinlichkeit und auch Chancen aufzeigen, die die Firma betreffen könnten. Die gemachten Überlegungen im Risikomanagement können auch Feuerwehrübungen vermeiden, die den Projekterfolg in Gefahr bringen. Die Risikoanalyse wird in einem schmalen Rahmen in den folgenden drei Schritten durchgeführt:

1. Risiken identifizieren
2. Risiken bewerten
3. Massnahmen festlegen

3.4.1. Risiken identifizieren

Damit Risiken gezielt angegangen werden können, wird zwischen folgenden Risiken unterschieden:

1. Externe Risiken: Risiken, die nicht durch das Projektteam steuerbar sind
2. Interne Risiken: Direkt durch das Projektteam steuerbar

In untenstehender Tabelle werden die Risiken mit Risk#X abgekürzt.

Risikonr.	Art des Risikos	Risikobeschreibung
Risk#1	Extern	Bugs im Endpoint Management Server
Risk#2	Extern	Bugs im FortiClient
Risk#3	Extern	Höhere Gewalt die das Projekt gefährden (Umwelt, Krieg)
Risk#4	Intern	Testumgebung unvollständig und nicht einsatzbereit
Risk#5	Intern	Testhardware defekt
Risk#6	Intern	Ausfall Teammitglieder durch Krankheit/Unfall
Risk#7	Intern	Zeitverzug aufgrund von mangelhafter Planung
Risk#8	Intern	Testumgebung nicht gemäss den Anforderungen umgesetzt
Risk#9	Intern	Lizenzen nicht rechtzeitig einsatzbereit

Tabelle 26: Risiken identifizieren

3.4.2. Risiken bewerten

Die genannten Risiken haben jeweils eine höhere oder tiefere Eintrittswahrscheinlichkeit. Die Risikobewertung setzt sich aus Eintrittswahrscheinlichkeit und Tragweite zusammen.

Die Tragweite wird in die folgenden Stufen unterteilt:

1. Zu vernachlässigen
2. Nicht kritisch
3. Auf Teilbereiche kritisch (leichte, negative Auswirkungen auf Teile des Projekts)
4. Kritisch (starke, negative Auswirkungen auf das Projekt)
5. Sehr Kritisch (Projektgefährdend)

Die Eintrittswahrscheinlichkeit in der Tabelle wird in Prozent angegeben. Es werden Prozentstufen in 10er Schritten unterschieden von 1 bis 100% Eintrittswahrscheinlichkeit.

Risikonr.	Risikobeschreibung	Eintritt in %	Tragweite
Risk#1	Bugs im Endpoint Management Server	30%	3
Risk#2	Bugs im FortiClient	20%	3
Risk#3	Höhere Gewalt die das Projekt gefährden	1%	5
Risk#4	Testumgebung unvollständig und nicht einsatzbereit	20%	4
Risk#5	Testhardware defekt	10%	4
Risk#6	Ausfall Teammitglieder durch Krankheit/Unfall	30%	3
Risk#7	Zeitverzug aufgrund von mangelhafter Planung	40%	2
Risk#8	Testumgebung nicht gemäss den Anforderungen umgesetzt	20%	3
Risk#9	Lizenzen nicht rechtzeitig einsatzbereit	10%	2

Tabelle 27: Risikobewertung und Risk Score

Anhand der Heatmap können Risiken zur besseren Übersicht grafisch dargestellt werden.

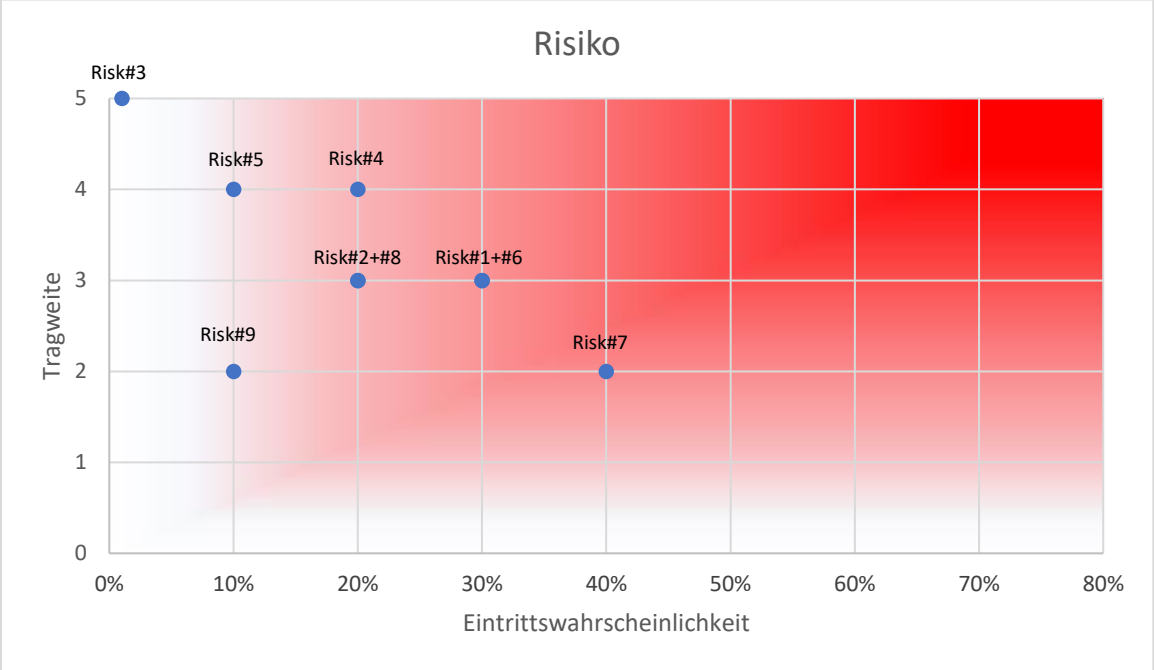


Tabelle 28: Risikobewertung

Risk Score

Aus dem Produkt der Eintrittswahrscheinlich und der Tragweite wird der Risk Score gewonnen. Ab einem bestimmten Risk Score werden im nächsten Schritt Massnahmen definiert, im Falle eines Eintritts des Risikos.

Der tiefste Wert für den Risk Score beträgt 0.01. Der theoretisch höchste Wert ist 5, wobei eine Eintrittswahrscheinlichkeit von 100% und eine Tragweite von 5 katastrophal wäre.

Risikonr.	Risikobeschreibung	Eintritt in %	Tragweite	Risk Score
Risk#1	Bugs im Endpoint Management Server	30%	3	**0.9**
Risk#2	Bugs im FortiClient	20%	3	**0.6**
Risk#3	Höhere Gewalt die das Projekt gefährden	1%	5	**0.05**
Risk#4	Testumgebung unvollständig und nicht einsatzbereit	20%	4	**0.8**
Risk#5	Testhardware defekt	10%	4	**0.4**
Risk#6	Ausfall Teammitglieder durch Krankheit/Unfall	30%	3	**0.9**
Risk#7	Zeitverzug aufgrund von mangelhafter Planung	40%	2	**0.8**
Risk#8	Testumgebung nicht gemäss den Anforderungen umgesetzt	20%	3	**0.6**
Risk#9	Lizenzen nicht rechtzeitig einsatzbereit	10%	2	**0.2**

Tabelle 29: Risk Score

3.4.3. Massnahmen festlegen

Für jedes Risiko können Massnahmen ergriffen werden, damit es nicht eintrifft. Bei Risiken mit einem Risk Score unter 0.5 sind Massnahmen nicht empfehlenswert, da ein Eintritt entweder äusserst unwahrscheinlich oder zu vernachlässigen ist. Massnahmen zur Vorbeugung sollen wenn möglich getroffen werden. Falls es zu einem Eintritt eines Risikos kommt, müssen Gegenmassnahmen vorbereitet sein.

Massnahmen und Gegenmassnahmen

Risikonr.	Risikobeschreibung	Massnahme	Gegenmassnahmen
Risk#1	Bugs im Endpoint Management Server	Administration Guide, Known Issues und Fixed Issues lesen	Supportticket bei Hersteller erstellen, Fehleranalyse durchführen
Risk#2	Bugs im FortiClient	Administration Guide, Known Issues und Fixed Issues lesen	Supportticket bei Hersteller erstellen, Fehleranalyse durchführen
Risk#3	Instanzen von höherer Gewalt, die das Projekt gefährden	Massnahmen anhand des Vorkommnisses	Gegenmassnahmen anhand des Vorkomnisses
Risk#4	Testumgebung unvollständig und nicht einsatzbereit	Spezifikation und Definition der benötigten Testhardware verifizieren	Gespräch suchen, Lösungen finden
Risk#5	Testhardware defekt	Hardware testen	Ersatzhardware bereithalten
Risk#6	Ausfall Teammitglieder durch Krankheit/Unfall	Öffentliche Verkehrsmittel meiden	HomeOffice, Stellvertretung
Risk#7	Zeitverzug aufgrund ungeplanter Ereignisse	Planung im Vorfeld bestätigen lassen, Zeitreserven einbauen	Zeitreserven nutzen, Eskalation an Product Owner
Risk#8	Testumgebung nicht gemäss den Anforderungen umgesetzt	Definition und Spezifikation der benötigten Testumgebung vorgängig bestimmen und verifizieren	Gespräch suchen, Lösungen finden
Risk#9	Lizenzen nicht rechtzeitig einsatzbereit	Abklärungen treffen mit Einkaufsabteilung	Hersteller kontaktieren

Tabelle 30: Massnahmenkatalog für Risiken

4. Product Backlog, Epic «Installation und Konfiguration EMS 7.0»

Basierend auf den Anforderungen der einzelnen Gruppen hat der Product Owner folgendes Product Backlog erstellt. Das Product Backlog besteht nur aus dem Epic «Installation und Konfiguration EMS 7.0». Das Team hat beim ersten SCRUM-Meeting die Einheit eines StoryPoints festgelegt (1 StoryPoint = 4 Stunden Arbeitszeit) und den Aufwand der einzelnen Tasks in StoryPoints geschätzt.

Das Product Backlog wird laufend durch den Product Owner bearbeitet. Das untenstehende Backlog ist das komplette Backlog mit allen Tasks, die während der Sprints dazugekommen sind. Der Status der jeweiligen Tasks wird hier nicht angegeben, damit die Nachverfolgung gegeben ist.

Task Nr.	Beschrieb	StoryPoints
759	EMS Testinstallation von Version 6.4.7 auf 7.0.3 aktualisieren	1
760	Testen des Updates von FortiClient 6.4.7 auf Version 7.0.3 unter Windows 10	1
761	Testen des Updates von FortiClient 6.4.7 auf Version 7.0.3 unter Linux Ubuntu 20	2
762	Testen des Updates von FortiClient 6.4.7 auf Version 7.0.3 unter macOS 12.3.1 Monterey	1
763	ZTNA Tags auf ihre Funktionalität hin überprüfen	3
764	VPN Verbindungsparameter für Firma festlegen	1
765	Client-Rollout: Ablauf mit Client Management besprechen	1
766	Mögliche ZTNA Tags definieren	1
767	Evaluation ZTNA Tags Feature	2
768	Evaluation Endpoint Profiles	2
769	Endpoint Profiles für Clients definieren	1
770	EMS AD Anbindung	1
771	Firewall Policies mit ZTNA Tags	3
772	VPN vor Login unter Windows / Linux / Mac einrichten und testen	2
773	FortiClient Installer für Endpoint Profile zur Verfügung stellen (ITS, DEV und Office)	4
774	FortiGate Update auf 7.0.5	4
775	Konfiguration EMS Produktion abschliessen	6
776	Dokumentation für Präsentation am Show and Tell	8
777	Testen des Installers FortiClient 7.0.3 mit Firmensettings für Update	2
778	"compliant" Tag mit unverschlüsseltem USB-Stick behalten	1
779	Support-Case bei Fortinet erstellen/bearbeiten	2
784	Endpoint Policies in EMS 7.0.3 erstellen und testen	2

Tabelle 31: Product Backlog "Installation und Konfiguration EMS 7.0"

Mit der Erstellung des Product Backlogs beginnen die Sprints. Es werden 4 Sprints zu je einer Woche durchgeführt. Die 4 Sprints sind:

Name	Dauer
Sprint 2022/W15	vom 4. April bis zum 08. April 2022
Sprint 2022/W16	vom 11. April bis zum 14. April 2022 (15 April ist Karfreitag)
Sprint 2022/W17	vom 19. April bis zum 22. April 2022 (18. April ist Ostermontag)
Sprint 2022/W18	vom 25. April bis zum 29. April 2022

Tabelle 32: Bezeichnungen Sprints in Epic

Ablauf eines Sprints

Der Product Owner gibt am jeweiligen Sprint Meeting des bevorstehenden Sprints die Tasks an, die erledigt werden sollen. Dabei müssen nicht alle Tasks vollständig erledigt werden, da meist unerwartete Zwischenfälle einen Task verzögern können. Ziel der Tasks sind das Erfüllen der gestellten Ziele und das Erfüllen der Anforderungen. Wie die Tasks gehandhabt werden, ob neue hinzugefügt werden oder gelöscht werden, entscheidet der Product Owner. Innerhalb des Sprints entscheidet der Diplomand, welche Tasks er in welcher Reihenfolge bearbeiten will.

Um die Leserlichkeit des Dokuments zu erhöhen, werden die einzelnen Tasks pro Sprint in den Anhang verschoben. Die Tasks werden im Sprint Review jeweils kurz zusammengefasst und auf den ausführlichen Arbeitsablauf im Anhang verwiesen.

4.1. Sprint 2022/W15

Der erste Sprint beginnt am 4. April 2022 und endet am 08. April 2022. Gemäss der Definition der StoryPoints können für diese 5 Tage 10 StoryPoints bearbeitet werden. Die Gesamtzahl an StoryPoints für den ersten Sprint liegt bei 11 StoryPoints.

Der Product Owner verlangt für den ersten Sprint folgende Tasks:

Name	Beschreibung	Startdatum	StoryPoints	Enddatum
Task-759	EMS Testinstallation von Version 6.4.7 auf 7.0.3 aktualisieren	04.04.2022	1	04.04.2022
Task-760	Testen des Updates von FortiClient 6.4.7 auf Version 7.0.3 unter Windows 10	04.04.2022	1	04.04.2022
Task-762	Testen des Updates von FortiClient 6.4.7 auf Version 7.0.3 unter Mac 12.3.1 Monterey	04.04.2022	1	04.04.2022
Task-767	Evaluation ZTNA-Tags	05.04.2022	2	06.04.2022
Task-766	Mögliche ZTNA Tags definieren	05.04.2022	1	07.04.2022
Task-761	Testen des Updates von FortiClient 6.4.7 auf Version 7.0.3 unter Windows 10	05.04.2022	2	04.04.2022
Task-763	ZTNA Tags auf ihre Funktionalität hin überprüfen	06.04.2022	3	08.04.2022

Tabelle 33: Übersicht Sprint W2022/15

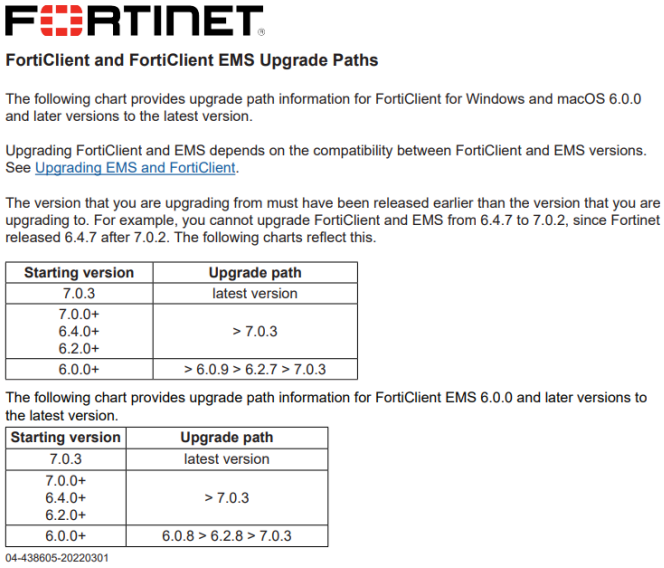
4.1.1. Task 759: EMS Testinstallation von Version 6.4.7 auf 7.0.3 aktualisieren

Damit die Lösung möglichst aktuell ist, wird als erstes der Endpoint Management Server auf die neuste Version 7.0.3 aktualisiert.

4.1.1.1. Upgrade Path

Fortinet stellt einen Upgrade Pfad für die gesamte Konfiguration zur Verfügung, an die man sich zu halten hat. So können Bugs oder Fehler umgangen werden. Die Testumgebung ist derzeit unter FortiOS 6.4.7, FortiClient 6.4.7 und FortiClient EMS 6.4.7 betriebsbereit.

Gemäss nachfolgender Grafik wird zuerst der EMS-Server auf die aktuelle Version und danach der FortiClient auf den Endpoints aktualisiert. Die gewünschte Version ist der FortiClient EMS 7.0.3, respektive der FortiClient 7.0.3. Das Upgrade ist gemäss Upgrade Path von Fortinet so durchzuführen. Als letztes Update folgt das FortiOS der FortiGate Firewall auf 7.0.3.



FortiClient and FortiClient EMS Upgrade Paths

The following chart provides upgrade path information for FortiClient for Windows and macOS 6.0.0 and later versions to the latest version.

Upgrading FortiClient and EMS depends on the compatibility between FortiClient and EMS versions. See Upgrading EMS and FortiClient.

The version that you are upgrading from must have been released earlier than the version that you are upgrading to. For example, you cannot upgrade FortiClient and EMS from 6.4.7 to 7.0.2, since Fortinet released 6.4.7 after 7.0.2. The following charts reflect this.

Starting version	Upgrade path
7.0.3	latest version
7.0.0+ 6.4.0+ 6.2.0+	> 7.0.3
6.0.0+	> 6.0.9 > 6.2.7 > 7.0.3

The following chart provides upgrade path information for FortiClient EMS 6.0.0 and later versions to the latest version.

Starting version	Upgrade path
7.0.3	latest version
7.0.0+ 6.4.0+ 6.2.0+	> 7.0.3
6.0.0+	6.0.8 > 6.2.8 > 7.0.3

04-438605-20220301

Abbildung 8: Fortinet Upgrade Pfad

Vor dem Update des EMS, konsultiert der Diplomand allerdings einen von Fortinet zur Verfügung gestellten «Compatibility Chart». Sollten die Versionen zwischen FortiOS, FortiClient und FortiClient EMS nicht kompatibel sein, muss ein anderer Weg gewählt werden.

FortiClient EMS
Compatibility Chart
This chart summarizes FortiClient EMS support for other Fortinet products.

FortiClient EMS	FortiClient		FortiOS	FortiAnalyzer[1]	FortiManager	FortiSandbox[2]
	Windows, macOS, and Linux	iOS and Android				
6.2.0+	6.0.0+ 6.2.0+[3]	6.0.0+ 6.2.0+[2] 6.4.0+[2]	6.0.0+ 6.2.0+	6.0.0+[4] 6.2.0+	6.0.0+[3] 6.2.0+	2.5.0+ 3.0.0+ 3.1.0+ 3.2.0+
6.4.0-6.4.3	6.2.0+[2] 6.4.0+[2]	6.2.0+[2] 6.4.0+[2] 7.0.0+[2]	6.2.0+ 6.4.0+	6.4.0+	6.4.0+	2.5.0+ 3.0.0+ 3.1.0+ 3.2.0+
6.4.4 6.4.7[5]				6.4.0+ 7.0.0+		3.1.0+ 3.2.0+ 4.0.0+
6.4.7[5]	6.4.7					
7.0.0	6.4.0+[2] 7.0.0+[2]		6.4.0+ 7.0.0+		EMS can import Web Filter profiles from all versions of FortiManager. EMS and FortiClient cannot receive new product installers from any version of FortiManager.	2.5.0+ 3.0.0+ 3.1.0+ 3.2.0+
7.0.1-7.0.3[6]						3.1.0+ 3.2.0+ 4.0.0+
7.0.3[6]	7.0.2+					

Abbildung 9: Kompatibilität FortiClient EMS

Gemäss der Grafik ist der geplante Upgrade Pfad des Product Owners untereinander kompatibel.

4.1.1.2. Unterschiede zu den Versionen

Ab EMS 7.0.3 wird für die Verbindung zwischen EMS und FortiOS ein Websocket geöffnet. Ein Websocket bietet gegenüber der bisherigen Methode diverse Vorteile, die im Kapitel «Firewall Policies mit ZTNA Tags auf FortiOS 6.4.7» genauer erläutert werden.

Die Vorteile lassen sich allerdings erst nutzen, wenn auch das FortiOS auf der FortiGate auf einer Version 7.0+ ist. Die aktuelle Version 6.4.7 des FortiOS unterstützt keine Websocket-Verbindung.

Im EMS 7.0.3 wurden die Profile und die Endpoint Policies verbessert. Die erstellten Endpoint Profiles können nun in den Policies ausgewählt und angewandt werden. So lässt sich eine Policy einfach und zeitsparend mit den vorhandenen Profilen erstellen. Der Policy können nun die gewünschten Profile zugeordnet und angewendet werden.

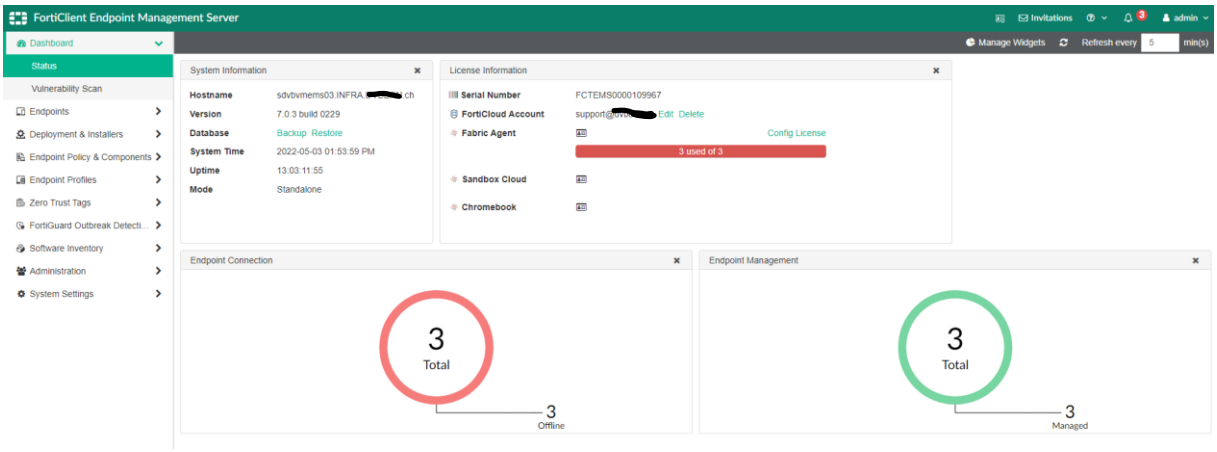


Abbildung 10: Dashboard von EMS 7.0.3

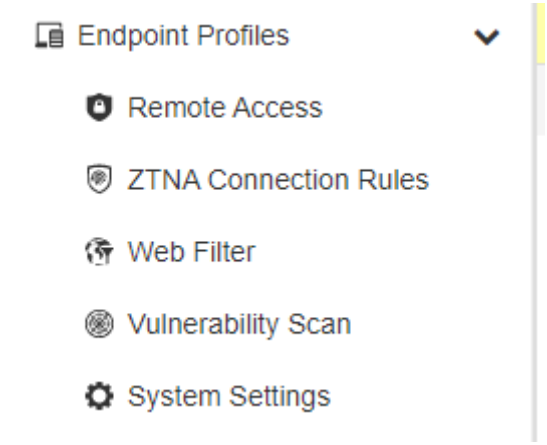


Abbildung 11: Ansicht Endpoint Profiles unter EMS 7.0.3

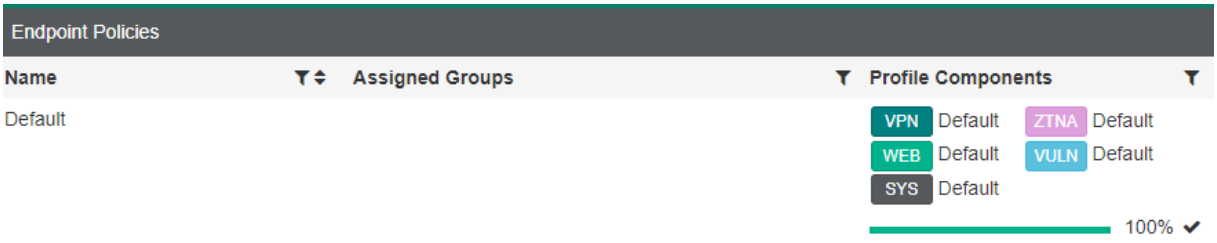


Abbildung 12: Ansicht Endpoint Policies unter EMS 7.0.3

4.1.1.3. Auswertung

Das Update von EMS 7.0.3 kann erfolgreich heruntergeladen und installiert werden. Das Update an sich läuft problemlos durch und die Clients verlieren die Verbindung zum EMS nicht. Der Telemetry Key, der im EMS definiert wird, um Endpoints mit dem EMS zu verbinden bleibt ebenfalls bestehen. Es gibt keine unerwarteten Probleme oder Bugs.

4.1.2. Task 760: Testen des Updates von FortiClient 6.4.7 auf Version 7.0.3 unter Windows 10

Auf dem Windows Testgerät «NBFIRMA-EMS-Test» ist der FortiClient 6.4.7 installiert und die Verbindung zu EMS und zum VPN funktionieren problemlos. Die Desinstallation unter Windows erfolgt über das Client-Management Tool der Firma (HighSystem). Nach der Deinstallation von FortiClient startet sich das Gerät ohne Ankündigung neu. Die Installationsdatei für den FortiClient 7.0.3 stammt von aus dem Support-Repository von Fortinet.

4.1.2.1. Testfall Update auf 7.0.3

Der Product Owner will wissen ob es möglich ist, den FortiClient 6.4.7 auf 7.0.3 zu aktualisieren, ohne den alten Client zu deinstallieren und den unangekündigten Neustart zu umgehen

Update auf 7.0.3: Neustart soll gemacht werden, kann aber verneint werden. Der FortiClient lässt sich ohne Neustart nutzen aber:

- Langsamer Startup
- Keine Verbindung zum EMS
- Unlizenzierte Version von FortiClient bei Test
- Verbindung VPN nicht möglich. Das Nutzen des Endpoints ist weiterhin möglich, auf Kosten der VPN Verbindung.

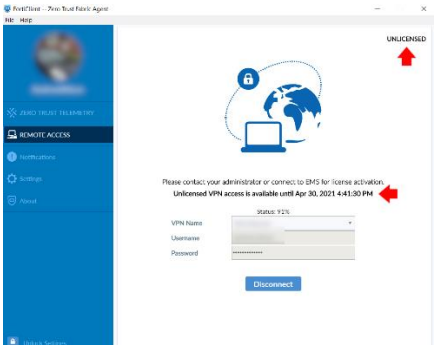


Abbildung 13: FortiClient unlizenziert nach Update auf 7.0.3

Der Neustart des Clients sollte deshalb unbedingt durchgeführt werden. Durch die Ankündigung können Mitarbeiter:innen ihre aktuellen Arbeitsdossiers noch speichern und es kommt zu keinem Datenverlust.

4.1.2.2. Auswertung

Das Update ist erfolgreich, die Test-VPN Verbindung kann erfolgreich hergestellt werden. Die Installation von Version 7.0.3 von der Downloadseite von Fortinet funktioniert ohne weitere Zwischenfälle.

Wichtig: Wird der FortiClient via HighSystem deinstalliert, wird das Gerät einen ungefragten Neustart durchführen. User sind also zwingend zu benachrichtigen, dass sämtliche ungespeicherte Arbeiten verloren gehen, falls dies so umgesetzt wird. Die elegantere Lösung ist, den FortiClient zu aktualisieren und den User das Gerät selber neu starten zu lassen.

4.1.3. Task 762: Testen des Updates von FortiClient 6.4.7 auf Version 7.0.3 unter MacOS 12.3.1 Monterey

Endpoints mit dem Betriebssystem macOS sind in der Firma derzeit noch rar. Derzeit sind zwei Geräte produktiv im Einsatz und noch keine weiteren Geräte an Lager, die als Testgerät fungieren können. Aus diesem Grund wird das private MacBook Pro des Diplomanden verwendet. Somit kann das MacBook «MacBook_Pro_von_lesa» als Testgerät mit MacOS 12.3.1 Monterey genutzt werden. Es gilt, die Version 6.4.7 zu testen und das Update auf die Version 7.0.3 zu vollführen.

4.1.3.1. Auswertung

Die Installation der FortiClient Version 6.4.7 und das anschliessende Update auf Version 7.0.3 verläuft ohne Zwischenfälle. Vorteile gegenüber der Windows-Version:

- Kein Neustart erforderlich
- Kein unangekündigter Neustart
- VPN Verbindung nach Update weiterhin vorhanden
- FortiClient bleibt mit EMS verbunden und ist lizenziert

4.1.4. Task 761: Testen des Updates von FortiClient 6.4.7 auf Version 7.0.3 unter Linux Ubuntu 20

NBFIRMA157 mit Linux Ubuntu 20 kann als Testgerät verwendet werden. Das Gerät muss erst mit FortiClient 6.4.7 ausgestattet und getestet werden, bevor das Update auf 7.0.3 erfolgt. Unter Linux muss der FortiClient mittels folgender Befehle manuell installiert werden:

 # Alte FortiClient Version löschen (-r, --remove package)

dpkg -r forticlient

 # Neue FortiClient Version installieren (-i, --install package-file)

dpkg -i <forticlient.deb>

 # In den FortiClient Installationspfad wechseln

cd /opt/forticlient

 # Löschen des History-Files (/home/<user>/.bash_history) damit der Telemetry Key nicht in der History ersichtlich ist

unset HISTFILE

 # Verbindung mit EMS herstellen, anschliessende Abfrage nach Telemetry Key

./epctrl -r ems.firma.ch

4.1.4.1. Auswertung

Installation von FortiClient 6.4.7 kann ohne Mühe abgeschlossen werden. Die Verbindung zu EMS und das VPN funktionieren einwandfrei. Das Update auf FortiClient 7.0.3 stellt keine Probleme dar. Die VPN Verbindung kann auch nach dem Update hergestellt werden und die Verbindung zu EMS bleibt bestehen. Ein Neustart des Geräts ist nicht nötig.

4.1.5. Task 767: Evaluation ZTNA Tags Feature

Das Feature Zero Trust Tags wird dazu benutzt, Endpoints anhand ihres Betriebssystems, Domänenzugehörigkeit und vielem mehr zu unterscheiden und zu gruppieren. Dank Forti OS können diese dynamischen Endpunktgruppen später anhand der Tags durch Policies verschieden behandelt werden.

Die Tags können auf Windows, macOS und Linux Geräte angewandt werden.

4.1.5.1. Funktionalität der ZTNA-Tags

Der EMS versendet die Tag-Rules mittels Telemetry-Kommunikation an die Endpoints. Der installierte FortiClient prüft die erhaltenen Tags und sendet die Antwort zurück an den EMS, ob der Client zum Teil Tags erfüllt. Der EMS setzt dem Client danach den Tag.

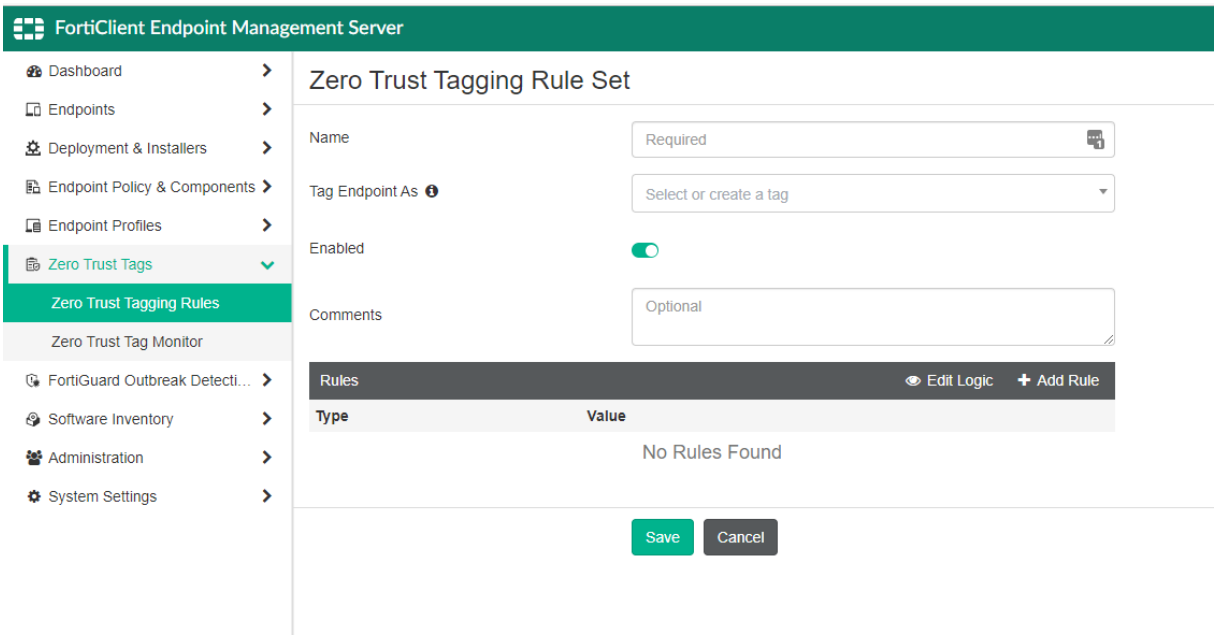


Abbildung 14: Übersicht Zero Trust Tags

Ein wesentlicher Bestandteil des Projekts ist es, die ZTNA-Tags so zu formulieren, dass ein Client der Firma eindeutig zugeordnet werden kann. Dazu muss aber erst anhand der vorhandenen Möglichkeiten der Tags entschieden werden, was einen Client der Firma als solchen kennzeichnet. Es soll ein Mittelweg zwischen Usability und Security gewählt werden, damit nicht die User Experience darunter leidet.

Bevor die möglichen Tags genauer analysiert werden, hat sich der Diplomand selbst Gedanken darüber gemacht, wie er ein Firmengerät als solches definieren könnte. Ein Auszug aus seinen Notizen zur Definition eines Gerätes der Firma:

- Hostname (könnte gefälscht sein, plus anlegen von evt. Datenbank für ems?)
- Gibt es das Gerät im AD? (was ist, wenn keine Verbindung zum Server besteht?)
- Macadresse - müsste ein Register mit Mac Adressen geführt werden, welches EMS abrufen und prüfen kann. Achtung, Mac Spoofing.
- Softwareaktualisierungen in den letzten 5 Tagen?
- Keine Kritische Sicherheitslücke von Rootkit oder Vulnerability-Scan des FortiClients
- Ist in der Domain firma.ch (könnten viele Geräte sein)
- OS Version: mindestens Windows 10 (sehr schwammig, kann fast jedes Gerät sein.)
- User-basierend ausschliessen? User kann sich ja von überall einloggen wenn er das möchte.
- Irgend ein Key in der Registry?
- Ein File im Dateisystem der Clients, das nicht ersichtlich ist?
- HighSystem Agent installiert und aktiv (Version?)
- Sonstiges Inventar an Software, was typisch für die Firma ist?
- Seriennummer des Geräts, bsp. 5CD1405GQP?
- MacAdresse des Gateway?

Einige dieser Einfälle würden die Usability stark einschränken, da zu viele Kennzeichen geprüft werden müssen. Teilweise können einige der Ideen wahrscheinlich nicht umgesetzt werden.

4.1.5.2. ZTNA Tags in EMS 7.0.3

EMS bietet einige der gemachten Überlegungen auch als Möglichkeit an, wie ein Gerät analysiert werden kann. Folgende Regeln kann der EMS via FortiClient auf Windows-Endpoints prüfen:

Regeln	**Prüfung**
Active Directory Groups (AD Groups)	Mitglied der Gruppe X im Active Directory?
Anti-Virus Software	Anti-Virus installiert und in Betrieb?
Certificate	Bestimmtes Zertifikat vorhanden?
EMS Management	Verbindung zum EMS Server hergestellt?
File	Bestimmtes File auf dem Endpoint vorhanden?
Logged in Domain	Mitglied der Domäne firma.ch?
Registry Key	Definierter Registry Key vorhanden?
Running Process	Bestimmte Prozesse aktiv?
OS Version	Betriebssystem «X» installiert?
Sandbox Detection	Malwarebefall in den letzten 7 Tagen? (Benötigt zusätzliche Lizenzen)
User Identity	Bestimmter Benutzer auf dem Endpoint?
Vulnerable Devices	Hat das Gerät einen definierten Schweregrad an Verletzlichkeit?
Windows Securtiy	Sind gewisse Windows Features aktiviert?
Internet Protocol(IP)-Range	Befindet sich das Gerät in der definierten IP-Range?
On-Fabric Status	Befindet sich das Gerät innerhalb der Firma?

Tabelle 34: Mögliche ZTNA Tags in EMS 7.0.3

Um Stärken, Schwächen und Einsatzmöglichkeiten zu testen, werden die Regeln analysiert und mittels Pro und Contra miteinander verglichen. Es können mehrere Regeln für einen einzigen Tag definiert werden, eine Kombination aus mehreren Regeln zur Bestimmung eines Firmengeräts liegt demnach nahe.

AD Group Pro	**AD Group Contra**
Einfach zu implementieren mit Verbindung zum AD	Actice Directory Server könnte offline sein, nicht geprüft werden
Schliesst alle Geräte ausserhalb der Domäne bereits aus	User im AD gesperrt
	Zu viele Gruppen in der Firma
	Könnte sein, dass Gruppen hinzugefügt werden und so vergessen gehen
AntiVirus Pro	**AntiVirus Contra**
Einfach zu überprüfen, da einheitlicher AV in der Firma installiert ist	Wird nicht geprüft, welcher Anti-Virus installiert ist
Muss zwingend aktiv sein	
Certificate Pro	**Certificate Contra**
Kann einfach mitgeliefert werden	Kann ablaufen
Schwierig zu fälschen, stehlen	Muss lokal auf dem Client installiert sein
	Könnte exportiert werden
	Könnte gelöscht werden
EMS Management Pro	**EMS Management Contra**
Telemetry Key muss für Verbindung vorhanden sein	Verfügbarkeit EMS ausserhalb des internen Netzwerks
Telemetry Key ist nur wenigen bekannt	Ist der Schlüssel bekannt, ist die Verbindung zu EMS einfach herzustellen
Telemetry Key wird mit der Installation des erstellten Installers verteilt	
File Pro	**File Contra**
Einfache Variante zur Verifizierung	Könnte unabsichtlich gelöscht werden
Kann gut im System versteckt werden	Unsicher bei bekanntwerden
Schnell und leicht zu erstellen	Könnte von Anti-Virus in Quarantäne verschoben werden
Loggen in Domain Pro	**Logged in Domain Contra**
Benutzer müsste Domain Admin Passwort kennen, um das Gerät in die Domäne aufzunehmen	Könnte auch ein altes Gerät sein
Schliesst bereits sehr viele Geräte aus	Zugriff auf User und Passwort des Domain Administrators der Firma ist für interne problemlos möglich
Registry Key Pro	**Registry Key Contra**
Schwer zu finden	Bei Diebstahl könnte der Key ausgelesen werden
Softwarespezifischer Key verwenden	
Running Process Pro	**Running Process Contra**
Typische Software wie Anti-Virus oder Agent des Client Management Tools (HighSystem)	Kann vorkommen, dass der Prozess beendet wird
	Prozess könnte nicht gestartet sein
Sandbox Detection Pro	**Sandbox Detection Contra**
Gerät würde als sicher eingestuft werden	zusätzliche Kosten für Lizenzen

OS Version Pro	**OS Version Contra**
Alte und zu neue Geräte können effektiv ausgefiltert werden	Aktuelle Windows Version ist sehr verbreitet
	Schliesst nur sehr alte Geräte aus
User Identity Pro	**User Identity Contra**
Man wüsste genau, welcher User sich anmeldet	Anmeldedaten können abgegriffen werden
Vulnerable Device Pro	**Vulnerable Device Contra**
Gefährdete Geräte können effektiv aussortiert werden	Schwierig, was EMS als «High» einstuft und was nicht
Windows Security Pro	**Windows Security Contra**
BitLocker ist aktiv, was er gem. Richtlinien der Firma auch sein muss	-
IP-Range Pro	**IP-Range Contra**
Sehr spezifisch	Hohe Fehlerquote
	HomeOffice nicht möglich bei dieser Anzahl an Mitarbeiter:innen
	IP-Range kann einfach nachgestellt werden

Tabelle 35: Analyse Pro und Contra der ZTNA Tags

4.1.5.3. Auswertung

Es gibt in EMS 7.0 sehr viele Tags die gesetzt werden können. Die Analyse der ZTNA-Tags bringt viel Licht in das Verständnis von EMS. Durch die Tags können via Policy auf der FortiGate verschiedene Szenarien eingestellt werden, wie die angehängten Clients gehandhabt werden sollen.

4.1.6. Task 766: Mögliche ZTNA Tags definieren

Die kennengelernten Tags sollen nun definieren, wie ein Firmengerät aussieht. Im EMS wird dafür der ZTNA Tag «compliant» erstellt. Werden die Regeln erfüllt, erhält der Laptop den Tag und gilt als Firmengerät. Der Aufwand, um alle definierten Regeln im Tag zu umgehen oder zu fälschen ist beträchtlich. Die Regeln werden am Ende des Sprints mit dem Product Owner angeschaut. Das Verhalten von EMS, wenn ein Client diesen Tag nicht hat, wird später geprüft.

Es werden zusätzliche Tags für die generelle Unterscheidung der Geräte zwischen Windows, macOS und Linux erstellt.

4.1.6.1. Regeln für ZTNA Tag «windows»

1. OS Version: Windows 10
2. EMS Management: FortiClient installed and Telemetry connected to EMS

4.1.6.2. Regeln für ZTNA Tag «linux»

1. OS Version: Ubuntu 18.04 or Ubuntu 20
2. EMS Management: FortiClient installed and Telemetry connected to EMS
3. File: /etc/.csum

4.1.6.3. Regeln für ZTNA Tag «mac»

1. MacOS
2. EMS Management: FortiClient installed and Telemetry connected to EMS
3. FileVault Disk Encryption is enabled
4. Anti-Viren (AV) Software is installed and running

4.1.6.4. Regeln für ZTNA Tag «compliant»

Basierend auf der Evaluation der ZTNA Tags bleiben 13 Regeln übrig, welche einen Client der Firma als solchen beschreiben. Diese Regeln für Windows 10, MacOs und Linux Laptops der Firma sind:

Windows:

1. Anti-Virus Software is installed and running
2. Logged in Domain firma.ch
3. Running Process, ekrn.exe (ESET), ERAAgent.exe (ESET) und hdnClSvc.NET.exe (HighSystem)
4. OS Version: Windows 10
5. EMS Management: FortiClient installed and Telemetry connected to EMS
6. Registry Key: HKEY_LOCAL_MACHINE\SOFTWARE\highsystem.NET\Client\Parameters\WebGatewayUrl
7. Windows Security, Bitlocker Disk Encryption is enabled

Linux:

1. OS Version: Ubuntu 18.04 or Ubuntu 20
2. EMS Management: FortiClient installed and Telemetry connected to EMS
3. File: /etc/.csum

MacOS:

1. OS Version: Monterey
2. Security: AV Software is installed and running
3. EMS Management: FortiClient installed and Telemetry connected to EMS

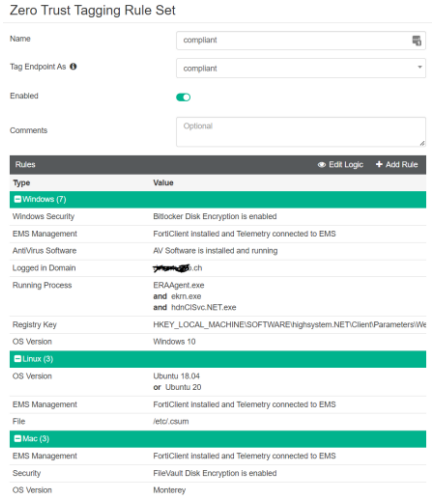


Abbildung 15: ZTNA Tag "compliant"

4.1.6.5. Auswertung

Die Definition zur Unterscheidung zwischen den jeweiligen Betriebssystemen wird bei einer hohen Anzahl von Geräten sicherlich sinnvoll sein. Dem Product Owner werden die definierten Tags als Vorschlag zur Identifikation eines Firmengerätes unterbreitet. Bei der Prüfung der Funktionalität im nächsten Schritt, können noch Anpassungen vorgenommen werden.

4.1.7. Task 763: ZTNA-Tags auf ihre Funktionalität hin überprüfen

Nun geht es darum, die definierten Tags mit den zur Verfügung stehenden Geräten zu testen und die Funktionalität der Tags zu prüfen. Dazu werden die in Task 766 definierten Tags gesetzt. Es wird an den jeweiligen Endgeräten geprüft, ob die Clients die definierten Tags erhalten. Mögliche Probleme oder Bugs sollen so frühzeitig erkannt werden.

4.1.7.1. ZTNA Tags am NBFIRMA-EMS-Test:

Folgende Tags sollen dem Testgerät mit Windows 10 zugeordnet und getestet werden:

ZTNA Tag	Rules	Value	Tag OK?
windows	OS Version	Windows 10	OK

Tabelle 36: ZTNA Tag "windows"

ZTNA Tag	Rules	Value	Tag OK?
compliant	OS Version	Windows 10	
compliant	EMS-Management	FortiClient installed and Telemetry connected to EMS	
compliant	AntiVirus Software	AntiVirus Software is installed and running	
compliant	Windows Security	Bitlocker Disk Encryption is enabled	
compliant	Registry Key	..WebGatewayUrl	
compliant	Running Process	Ekrn.exe, ERAAgent.exe und hdnClSvc.exe	
compliant	Logged in Domain	Firma.ch	
			OK

Tabelle 37: ZTNA Tag "compliant" unter Windows

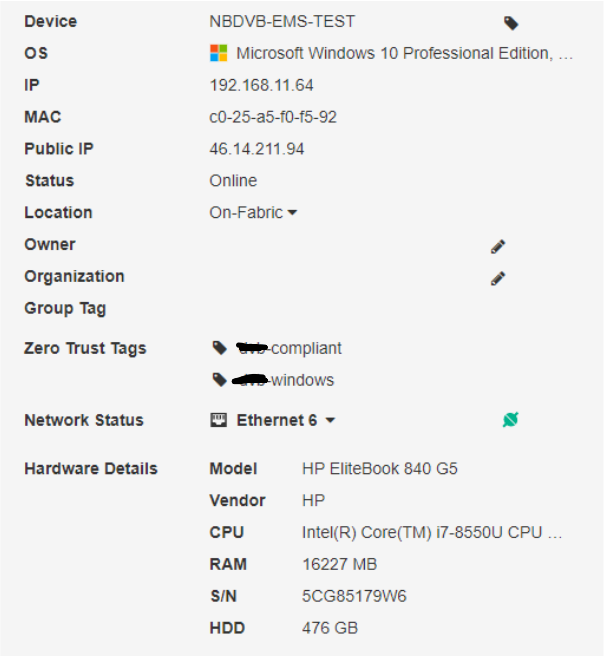


Abbildung 16: Endpoint mit Tag "windows" und "compliant"

Der FortiClient hat die Informationen vom EMS erhalten und das Hostsystem geprüft. Die Antwort meldet er EMS und erhält die ZTNA Tags. Nun werden weiterführende Tests am Gerät durchgeführt, um die Stabilität der Tags zu prüfen. Dazu werden die definierten Regeln zum Erhalt des Tags gebrochen.

Rule	Massnahme	Tag OK?
Running Process	Ekrn.exe manuell beendet	Tag NOK
Running Process	Ekrn.exe manuell gestartet	Tag OK

Tabelle 38: Testing Regel "Running Process"

Rule	Massnahme	Tag OK?
Windows Security (Bitlocker)	Verschlüsselung der Disk aufgehoben	Tag NOK
Windows Security (Bitlocker)	Verschlüsselung wieder aktiviert	Tag OK
Windows Security (Bitlocker)	USB-Stick angehängt	Tag NOK
Windows Security (Bitlocker)	USB-Stick ausgeworfen	Tag OK

Tabelle 39: Testing Regel "Windows Security"

Rule	Massnahme	Tag OK?
Registry Key	Key entfernt	Tag NOK
Registry Key	Key wieder hinzugefügt	Tag OK

Tabelle 40: Testing Regel "Running Process"

Rule	Massnahme	Tag OK?
Logged in Domain	Testgerät aus Domäne entfernt	Tag NOK
Logged in Domain	Testgerät der Domäne hinzugefügt	Tag OK

Tabelle 41: Testing Regel "Logged in Domain"

4.1.7.1.1. Auswertung der Tests

Testing der Rule «Windows Security»:

Wird ein USB-Stick oder eine Festplatte angeschlossen, die nicht mit Bitlocker verschlüsselt ist, verliert das Gerät seinen Tag.

Testing der Rule «Windows Security»

Besitzt ein Client eine zweite interne Festplatte und ist diese nicht verschlüsselt, verliert ein Gerät den «compliant» Tag. Dieser Fall betrifft User mit älteren Geräten in der Firma, die sowohl eine Solid State Drive (SSD) und eine Harddisk eingebaut haben. Bei der Verschlüsselung mit Bitlocker muss also darauf geachtet werden, dass sämtliche Disks verschlüsselt.

4.1.7.2. ZTNA Tags am MacBook Pro:

Folgende Tags sollen dem MacBook Pro mit macOS Monterey zugeordnet und getestet werden:

ZTNA Tag	Rules	Value	Tag OK?
mac	OS Version	Monterey	OK

Tabelle 42: ZTNA Tag "mac"

ZTNA Tag	Rules	Value	Tag OK?
compliant	EMS-Management	FortiClient installed and Telemetry connected to EMS	
compliant	AntiVirus Software	AntiVirus Software is installed and running	
compliant	Security	FileVault Disk Encryption is enabled	
			NOK

Tabelle 43: ZTNA Tag "compliant" unter macOS

Der «compliant» Tag kann nicht vergeben werden. Die Einzelnen Rules werden wiederum auf ihre Funktionalität getestet.

4.1.7.2.1. Auswertung der Tests

Testing der Regel «AntiVirus Software»:

FortiClient erkennt die installierte Antivirus-Software nicht. In diesem Fall den ESET Endpoint Security, der in der gesamten Firma im Einsatz ist

Testing der Regel: «Security»:

FortiClient erkennt die die Verschlüsselung der Festplatte durch FileVault nicht. Möglicherweise könnte das Problem ein ähnliches sein wie beim Windows Client. Es wird lediglich die «Macintosh HD»-Partition verschlüsselt. Der Container disk1 und die Apple SSD selber sind als «nicht verschlüsselt» deklariert. Ein erneutes Aus- und wieder Einschalten gibt die gleiche Situation wider.

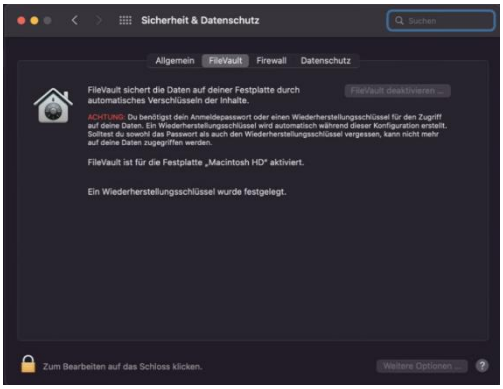


Abbildung 18: FileVault unter macOS

Abbildung 17: Eigenschaften der Apple SSD

Somit muss das MacBook nur noch eine Voraussetzung erfüllen, damit es den Tag «compliant» erhält.

ZTNA Tag	Rules	Value	Tag OK?
compliant	EMS-Management	FortiClient installed and Telemetry connected to EMS	OK

Tabelle 44: Effektiver ZTNA Tag "compliant" unter macOS

4.1.7.3. ZTNA Tags am Dell XPS 15 9510 (Linux Ubuntu 20)

Folgende Tags sollen dem Dell XPS mit Linux Ubuntu 20 zugeordnet und getestet werden:

ZTNA Tag	Rules	Value	Tag OK?
linux	OS Version	Ubuntu 18.04 or Ubuntu 20	OK

Tabelle 45: ZTNA Tag "linux"

ZTNA Tag	Rules	Value	Tag OK?
compliant	EMS-Management	FortiClient installed and Telemetry connected to EMS	
compliant	AntiVirus Software	AntiVirus Software is installed and running	
compliant	File	/etc/.csum	
compliant	OS Version	Ubuntu 18.04 or Ubuntu 20	
			NOK

Tabelle 46: ZTNA Tag "compliant" unter Linux Ubuntu 20

Unter Linux können die definierten Regeln ebenfalls nicht alle erfolgreich geprüft werden. Die definierten Regeln werden auf ihre Funktionalität geprüft.

4.1.7.3.1. Auswertung der Tests

Testing der Regel «AntiVirus Software»:

FortiClient erkennt die installierte AntiVirus-Software unter Linux Ubuntu 20 nicht.

Aus den Tests ergeben sich für den Tag folgende Regeln:

ZTNA Tag	Rules	Value	Tag OK?
compliant	EMS-Management	FortiClient installed and Telemetry connected to EMS	
compliant	File	/etc/.csum	
compliant	OS Version	Ubuntu 18.04 or Ubuntu 20	
			OK

Tabelle 47: ZTNA Tag "compliant" unter Linux Ubuntu 20

4.1.7.3.2. Auswertung der Funktionalität

Die Tags für die Unterscheidung der Operating Systems können erfolgreich eingeführt und getestet werden. Damit die Geräte den «compliant» Tag erhalten, müssen einige Anpassungen gemacht werden. Die Bearbeitung der möglichen Bugs wird in einem späteren Schritt durchgeführt. Für das weiterführende Testing wird mit den definierten «compliant» Tag gearbeitet.

4.2. Review Sprint 2022/W15

Das Sprint Review bezeichnet das Ende eines Sprints. Der Product Owner wird über den Fortschritt informiert und die Arbeit im Sprint zusammengefasst. Das Produkt wird dem PO vorgeführt und es wird entschieden, wie weiter vorgegangen wird. Abgeschlossen wird der Sprint kurz vor dem Sprintmeeting am 11. April 2022 für den Sprint 2022/W16.

Name	Beschreibung	Erledigt	Grund
Task 759	EMS Testinstallation von Version 6.4.7 auf 7.0.3 aktualisieren	Ja	-
Task 760	Testen des Updates von FortiClient 6.4.7 auf Version 7.0.3 unter Windows 10	Ja	-
Task 762	Testen des Updates von FortiClient 6.4.7 auf Version 7.0.3 unter Mac 12.3.1 Monterey	Ja	-
Task 767	Evaluation ZTNA-Tags	Ja	-
Task 766	Mögliche ZTNA Tags definieren	Ja	-
Task 761	Testen von EMS 7.0 auf Linux Ubuntu 20	Ja	-
Task 763	ZTNA Tags auf Funktionalität prüfen	Ja	-

Tabelle 48: Sprint Review 2022/W15

Gespräch mit Product Owner am Freitag, 08. April 2022:

Alle Tasks sind abgeschlossen. Während der Demonstration des EMS behalten die Notebooks ihre Tags. Der Product Owner zeigt sich zufrieden mit der Arbeitsweise und dem erfolgreichen Abschliessen der Tests. Die Demonstration stimmt ihn und den Auftraggeber zuversichtlich für die nächsten Schritte. Die Tags werden innerhalb von ca. 30 Sekunden den Geräten zugewiesen oder entfernt. Die Tags bleiben bestehen und die Verbindung via VPN funktioniert ohne Einschränkungen.

Task 759: EMS Testinstallation von Version 6.4.7 auf 7.0.3 aktualisieren

Das Update von EMS 7.0.3 kann erfolgreich heruntergeladen und installiert werden. Das Update an sich läuft problemlos durch und die Clients verlieren die Verbindung zum EMS nicht. Der Telemetry Key, der im EMS definiert wird, um Endpoints mit dem EMS zu verbinden bleibt ebenfalls bestehen. Es gibt keine unerwarteten Probleme oder Bugs.

Task 760: Testen des Updates von FortiClient 6.4.7 auf Version 7.0.3 unter Windows 10

Das Update ist erfolgreich, die Test-VPN Verbindung kann erfolgreich hergestellt werden. Die Installation von Version 7.0.3 von der Downloadseite von Fortinet funktioniert ohne weitere Zwischenfälle.

Wird der FortiClient via Client Management Tool (HighSystem) deinstalliert, wird das Gerät einen ungefragten Neustart durchführen. User sind also zwingend zu benachrichtigen, dass sämtliche ungespeicherte Arbeiten verloren gehen, falls dies in der produktiven Umgebung genutzt wird. Die elegantere Lösung ist, den FortiClient zu aktualisieren und den User das Gerät selber neu starten zu lassen.

Task 762: Testen des Updates von FortiClient 6.4.7 auf Version 7.0.3 unter Mac 12.3.1 Monterey

Die Installation der FortiClient Version 6.4.7 und das anschliessende Update auf Version 7.0.3 verläuft ohne Zwischenfälle. Vorteile gegenüber der Windows-Version:

- Kein Neustart erforderlich
- Kein unangekündigter Neustart
- VPN Verbindung nach Update weiterhin vorhanden
- FortiClient bleibt mit EMS verbunden und ist lizenziert

Task 761: Testen von EMS 7.0 auf Linux Ubuntu 20

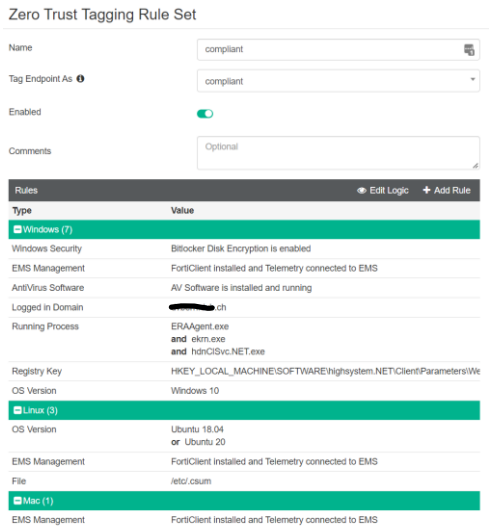
Installation von FortiClient 6.4.7 kann ohne Mühe abgeschlossen werden. Die Verbindung zu EMS und das VPN funktionieren einwandfrei. Das Update auf FortiClient 7.0.3 stellt keine Probleme dar. Die VPN Verbindung kann auch nach dem Update hergestellt werden und die Verbindung zu EMS bleibt bestehen. Ein Neustart des Geräts ist nicht nötig.

Task 767: Evaluation ZTNA-Tags

Es gibt in EMS 7.0 sehr viele Tags, die gesetzt werden können. Die Analyse der ZTNA-Tags bringt viel Licht in das Verständnis des EMS. Durch die Tags können via Policy auf der FortiGate verschiedene Szenarien eingestellt werden, wie die verbundenen Clients gehandhabt werden sollen. Die Tags können via FortiClient diverse Eigenschaften wie «Bitlocker enabled», «Running Process» oder «Registry Key» prüfen. Erfüllt ein Endpoint die Regeln erhält er den entsprechenden Tag. Es können mehrere Regeln für einen Tag erstellt werden.

Task 766: Mögliche ZTNA Tags definieren

Die Definition zur Unterscheidung zwischen den jeweiligen Betriebssystemen ist bei einer hohen Anzahl von Geräten sinnvoll. Dem Product Owner werden die definierten Tags als Vorschlag zur Identifikation eines Firmengerätes unterbreitet. Bei der Prüfung der Funktionalität im nächsten Schritt, können noch Anpassungen vorgenommen werden.


Zero Trust Tagging Rule Set

Name: compliant

Tag Endpoint As: compliant

Enabled

Comments: Optional

Rules — Edit Logic — Add Rule

Type	Value
Windows (7)	
Windows Security	Bitlocker Disk Encryption is enabled
EMS Management	FortiClient installed and Telemetry connected to EMS
AntiVirus Software	AV Software is installed and running
Logged in Domain	[redacted].ch
Running Process	ERAAgent.exe **and** ekrn.exe **and** hdnCISvc.NET.exe
Registry Key	HKEY_LOCAL_MACHINE\SOFTWARE\highsystem.NET\Client\Parameters\We
OS Version	Windows 10
Linux (3)	
OS Version	Ubuntu 18.04 **or** Ubuntu 20
EMS Management	FortiClient installed and Telemetry connected to EMS
File	/etc/.csum
Mac (1)	
EMS Management	FortiClient installed and Telemetry connected to EMS

Abbildung 19: Aktiver Tag "compliant" nach Sprint 2022/W15

Task 763: ZTNA Tags auf Funktionalität prüfen

Die Tags für die Unterscheidung der Operating Systems können erfolgreich eingeführt und getestet werden. Damit die Geräte den «compliant» Tag erhalten, müssen einige Anpassungen gemacht werden. Die Bearbeitung der möglichen Bugs wird in einem späteren Schritt durchgeführt. Für das weiterführende Testing wird mit dem definierten «compliant» Tag gearbeitet.

Feststellungen des Diplomanden:

Beim Testen der Regeln sind diverse Unstimmigkeiten aufgetaucht. Diese werden dem PO kurz zusammengefasst und erläutert.

Unter Windows:

- Bitlocker Recovery is enabled: Wird ein unverschlüsselter USB-Stick oder eine externe Festplatte angeschlossen, prüft der FortiClient diese ebenfalls auf die Bitlocker Verschlüsselung. Sind diese nicht verschlüsselt, geht der Tag «compliant» verloren. Das gleiche Verhalten wird bei Endpoints mit mehreren internen Festplatten beobachtet.

Linux:

- Anti Virus Software wird nicht erkannt

MacOS:

- FileVault Verschlüsselung unter macOS wird nicht erkannt
- Anti Virus Software wird nicht erkannt

Anforderungen Product Owner

Der Product Owner gibt neue Tasks für den Epic «Installation und Konfiguration EMS 7.0» vor:

- Task 778 - "compliant" Tag mit unverschlüsseltem USB-Stick behalten
- Task 777 - Testen des Installers FortiClient 7.0.3 mit Firmeneinstellungen für Update

Aktuell genutzte Versionen auf der Testumgebung:

Software	Version
FortiClient auf Windows Testgerät	7.0.3
FortiClient auf Linux Testgerät	7.0.3
FortiClient auf macOS Testgerät	7.0.3
FortiOS auf Testfirewall FortiGate 500E	6.4.7
FortiClient EMS	7.0.3

Tabelle 49: Aktuell genutzte Versionen nach Sprint 2022/W15

4.3. Sprint 2022/W16

Im Sprintmeeting des zweiten Sprints definiert der PO weitere Tasks. In dieser Woche sind nur 8 StoryPoints zu vergeben, da am 15.04.2022 der Karfreitag ist. Diese Woche ist also kürzer und die Anzahl an Tasks etwas zu hoch angesetzt. Der Product Owner verlangt für den Sprint folgende Tasks:

Name	Beschreibung	Startdatum	StoryPoints	Enddatum
Task 771	Firewall Policies mit ZTNA Tags	08.04.2022	3	
Task 768	Evaluation Endpoint Profiles	11.04.2022	2	-
Task 769	Endpoint Profiles für Clients definieren	11.04.2022	1	-
Task 778	"compliant" Tag mit unverschlüsseltem USB-Stick behalten	11.04.2022	1	-
Task 764	VPN Verbindungsparameter für die Firma festlegen	nicht begonnen	1	-
Task 770	EMS AD Anbindung	nicht begonnen	1	-

Tabelle 50: Übersicht Sprint 2022/W16

4.3.1. Task 771: Firewall Policies mit ZTNA Tags

Mit den im letzten Sprint gestalteten Tags sollen nun auf der FortiGate Policies erstellt oder ergänzt werden, damit Endpoints anhand der Tags Zugriff auf das Netzwerk erhalten oder davon ausgeschlossen werden. Um die Firewall Konfiguration zu verstehen, wird diese zuerst analysiert.

4.3.1.1. Konfiguration der FortiGate 500E:

Da die Firewall hinter der root-Firewall der Firma läuft, wird dessen Konfiguration ausser Acht gelassen. In diesem Bereich wird vor allem auf das VPN und die Policies der Testfirewall eingegangen.

4.3.1.1.1. Netzwerk Interfaces:

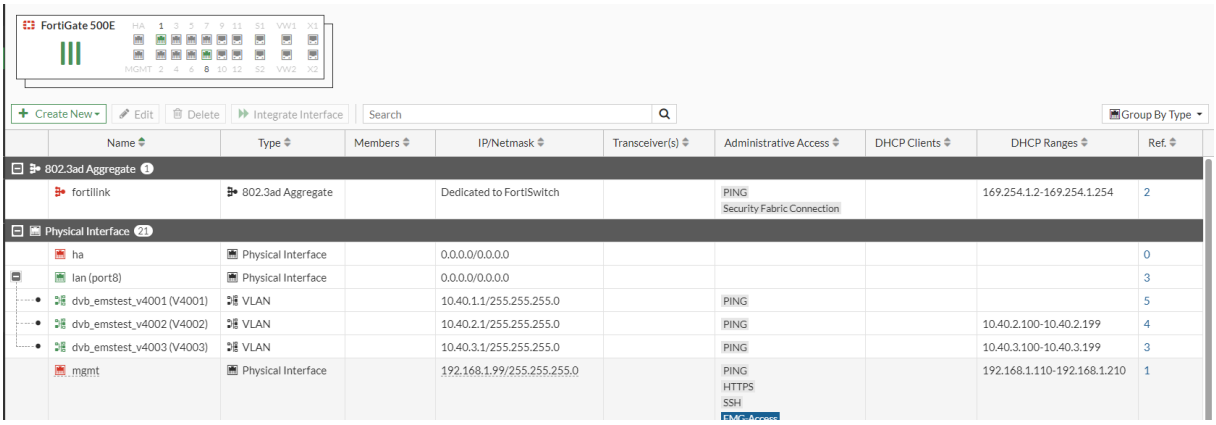


Abbildung 20: Übersicht Network Interfaces FortiGate

Der WAN-Anschluss ist auf Port 1 der Firewall eingerichtet. Auf Port 8 läuft das Local Area Network (LAN) mit drei weiteren Virtual-LANs.

4.3.1.1.2. Virtual Private Network (VPN)

Als Test-VPN wurde das Portal «torteloni-inc» eingerichtet. Als Source IP-Pool wurde das «vpn3» eingerichtet mit einem Pool von Adressen. Das Split Tunneling wurde bewusst ausgeschaltet, da der gesamte Verkehrt während dem VPN über den Tunnel laufen soll.

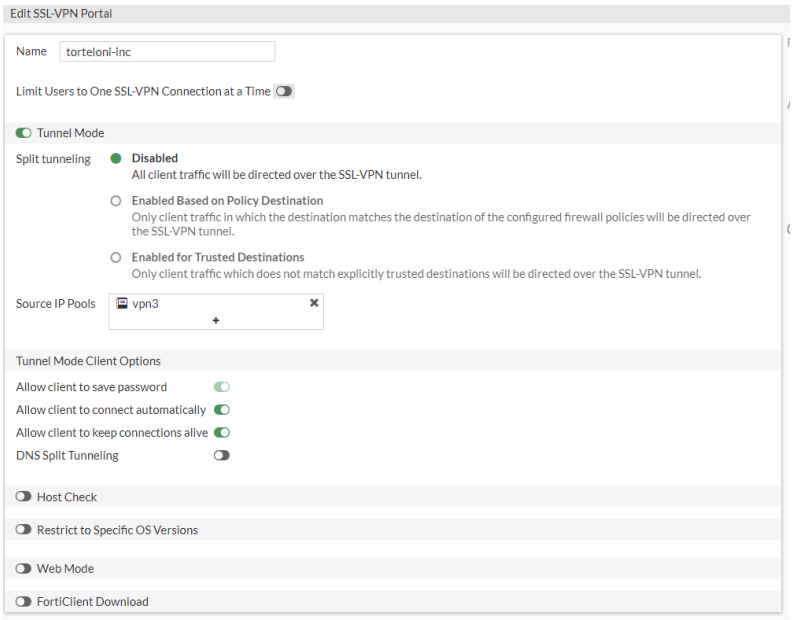


Abbildung 21: Einstellungen des Virtual Private Network

Die Adressen, die nach der erfolgreichen Verbindung des Tunnels vergeben werden, sind gemäss diesem Screenshot definiert:

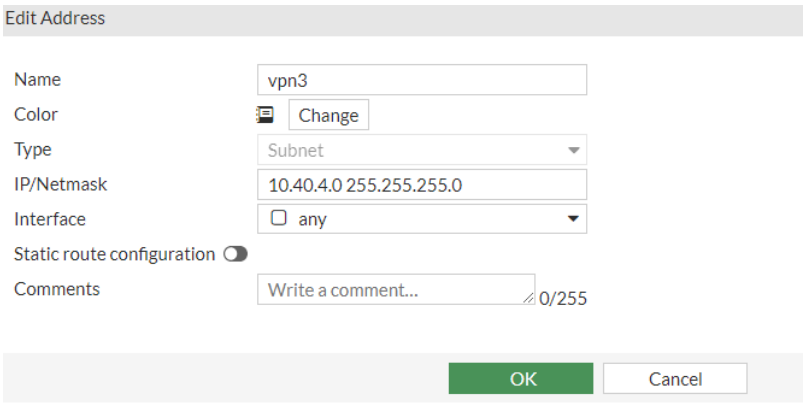


Abbildung 22: Konfiguration IP-Pool "vpn3"

In den generellen VPN-Einstellungen werden die DNS-Server von Google gewählt. Zur Authentifizierung mit dem VPN wird ein User «testiloni» erstellt, welcher sich via VPN verbinden kann.

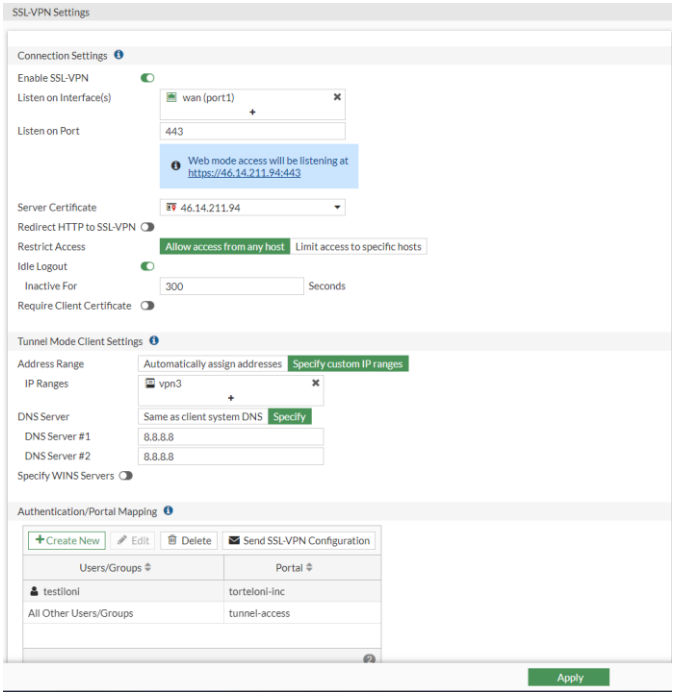


Abbildung 23: Einstellungen SSL-VPN

4.3.1.1.3. Firewall Policy

Die Firewall Policy bestimmt, wer von welchem Netz (internes LAN, wie auch extern über WAN) auf welche Ressourcen Zugriff haben soll. Der einfacheren Übersicht werden die Regeln in einer Tabelle kurz zusammengefasst und erklärt.

ID	Name	From	To	Source	ZTNA Tag	Enforce ZTNA	Destination	Schedule	Service
4	EMS Access	wan (port1)	dvb_emstest_v4001 (V4001)	185.125.165.125		Disabled	Clone of to ems and beyond	always	HTTPS RDP EMS Telemetry
3	Internet Access	dvb_emstest_v4002 (V4002) dvb_emstest_v4003 (V4003) dvb_emstest_v4001 (V4001)	wan (port1)	dvb_emstest_v4002 dvb_emstest_v4003 dvb_emstest_v4001		Disabled	all	always	PING Web Access NTP
5	Fortinet, Fortiguard Access	dvb_emstest_v4002 (V4002) dvb_emstest_v4003 (V4003) dvb_emstest_v4001 (V4001)	wan (port1)	dvb_emstest_v4002 dvb_emstest_v4003 dvb_emstest_v4001		Disabled	Fortinet-FortiGuard	always	Internet Service
8	EMS-Zugriff aus VPN	SSL-VPN tunnel interface (ssl.root)	dvb_emstest_v4001 (V4001)	testiloni vpn3		Disabled	Clone of to ems and beyond	always	EMS Telemetry HTTPS RDP FortiOS Connector
9	DNS-Access	SSL-VPN tunnel interface (ssl.root)	wan (port1)	testiloni vpn3		Disabled	dns.google.com	always	DNS
11	test drop	SSL-VPN tunnel interface (ssl.root)	wan (port1)	testiloni vpn3		Disabled	all	always	ALL
10		SSL-VPN tunnel interface (ssl.root)	wan (port1)	all		Disabled	all	always	ALL
6	Internetzugriff aus VPN	SSL-VPN tunnel interface (ssl.root)	wan (port1)	testiloni vpn3		Enabled	all	always	ALL
0	Implicit Deny	any	any	all			all	always	ALL

Abbildung 24: Übersicht der Firewall Policies auf FortiGate 500E

4.3.1.1.4. Policy #1: Zugriff auf den EMS Server aus Public Range

ID	Name	From	To	Source	Destination	Service	NAT
4	EMS Access	Wan (port 1)	VLAN 4001	185.125.165.125	Static NAT 10.40.1.30	EMS Telemetry, FortiOS Connector, HTTPS, RDP	Disabled

Tabelle 51: Firewall Policy 1: Zugriff auf EMS aus Public Range

Diese Regel erlaubt den Zugriff aus der Public Range (185.125.165.0/24) auf den EMS-Server mit den eingetragenen Services. Der Windows Server, der EMS betreibt, hat die IP 10.40.1.30.

4.3.1.1.5. Policy #2: Vom internen LAN ins Internet

ID	Name	From	To	Source	Destination	Service	NAT
3	Internet Access	VLAN4001, 4002, 4003	Wan (port 1)	Vlan4001, 4002, 4003	All	Ping, WebAccess, NTP	Enabled

Tabelle 52: Firewall Policy 2: Zugriff LAN auf WAN

4.3.1.1.6. Policy #3: Zugriff von intern auf benötigte Dienste von Fortinet

ID	Name	From	To	Source	Destination	Service	NAT
5	Fortinet FortiGuard Access	VLAN4001, 4002, 4003	Wan (port 1)	Vlan4001, 4002, 4003	Fortinet-FortiGuard	Internet Service	Enabled

Tabelle 53: Firewall Policy 3: Zugriff auf Dienste von Fortinet

4.3.1.1.7. Policy #4: Zugriff von VPN auf EMS

ID	Name	From	To	Source	Destination	Service	NAT
8	EMS-Zugriff aus VPN	SSL-VPN	VLAN4001	testiloni(User), vpn3	Static NAT 10.40.1.30	EMS Telemetry, FortiOS Connector, HTTPS, RDP	Disabled

Tabelle 54: Firewall Policy 4: Zugriff von VPN auf EMS

Der Zugriff auf den EMS-Server soll während aktiver VPN-Verbindung weiterhin möglich sein.

4.3.1.1.8. Policy #5: Zugriff aus VPN auf DNS

ID	Name	From	To	Source	Destination	Service	NAT
9	DNS Access	SSL-VPN	Wan (port1)	testiloni(User), vpn3	Dns.google.com	DNS	Enabled

Tabelle 55: Firewall Policy 5: Zugriff aus VPN auf DNS

Unabhängig davon, ob ein Client Zugriff auf das Firmennetzwerk hat, muss er einen Domain Name System Server (DNS-Server) erreichen.

4.3.1.1.9. Policy #6: Zugriff VPN auf Internet

ID	Name	From	To	Source	ZTNA TAG	Destination	Service	NAT
6	Internetzugriff aus VPN	SSL-VPN	Wan (port1)	testiloni(User), vpn3	«compliant»	All	All	Enabled

Diese Policy ist für Funktionalität der ZTNA Tags relevant. Werden hier ZTNA Tags gesetzt, sollen nur Geräte, die ebendiesen Tag besitzen, Zugriff auf das Internet haben. Mittels der Tags können auch andere Ressourcen stark eingeschränkt werden. Diese Policy ist in diesem Sinne dynamisch, da je nach Tagging mehr oder weniger Geräte den Zugriff auf bestimmte Ressourcen erhalten oder nicht. Der ZTNA Tag «compliant» ist in der Policy eingetragen. Somit müssten alle Endpoints, die den Tag im EMS erhalten haben, Zugriff via VPN ins Internet und interne Netz haben.

4.3.1.1.10. Policy #7: Implicit Deny

ID	Name	From	To	Source	ZTNA TAG	Destination	Service	Action
0	Implicit Deny	Any	Any	All		All	All	Deny

4.3.2. Firewall Policies mit ZTNA Tags auf FortiOS 6.4.7

Die Verbindung zwischen EMS und FortiOS ist instabil. Die Informationen die im EMS vorhanden sind, werden nicht vollständig in die FortiGate geladen. Es dauert mehrere Minuten, bis ein Client mit dem «compliant» Tag in der FortiGate ersichtlich wird. Die Verbindung des Endpoints auf das VPN und das Internet funktioniert, sobald dieser in die FortiGate geladen ist.

Die Kommunikation zwischen FortiGate und dem FortiClient EMS basiert auf dem Representational State Transfer (REST). Diese Verbindung wird geöffnet und geschlossen, weshalb die Tags und Endpoints nicht innerhalb weniger Sekunden in der FortiGate erscheinen.

In Tests mit dem Windows-Testgerät kann festgestellt werden, dass die Verbindung ins VPN via Hotspot an einem Smarthphone bis zu 45 Sekunden dauern kann. Die Dauer bis zur erfolgreichen Verbindung kann ebenfalls der Verbindung zwischen FortiOS und dem EMS zugewiesen werden.

Der Product Owner will, dass die FortiOS Version auf 7.0.3 aktualisiert wird. Ab der Version 7+ unterstützt sowohl der FortiClient EMS als auch FortiOS eine Websocket Verbindung. Ein Websocket zwischen FortiClient EMS und FortiGate sollte die Performance merklich erhöhen.

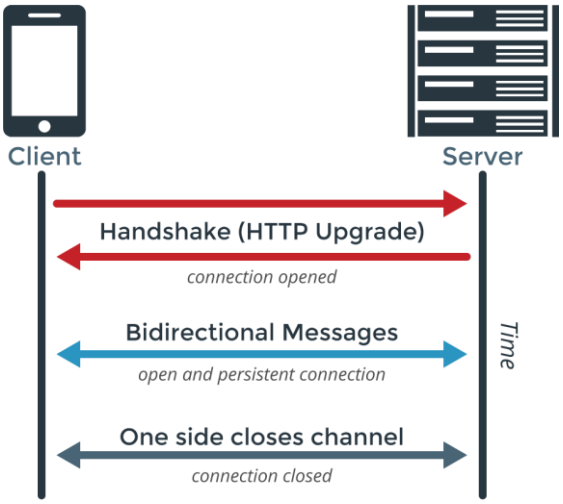


Abbildung 25: Websocket Verbindungsaufbau

Ähnlich wie bei einer Verbindung über Hypertext Transfer Protocol (http) wird zu Beginn ein Handshake durchgeführt. Ist dieser abgeschlossen fordert der Client ein Upgrade auf das Websocket Protokoll. Anders als bei http bleibt diese Verbindung offen und der Server kann die Verbindung aktiv nutzen, um neue Informationen an den Client weiterzugeben, ohne dass dieser eine neue Anfrage starten muss.

4.3.3. Firewall Policies mit ZTNA Tags auf FortiOS 7.0.3

Das Firewall Update auf FortiOS 7.0.3 funktioniert ohne unerwartete Zwischenfälle. Die Verbindung zwischen EMS und FortiOS ist dank dem Websocket nun und schneller. Die ZTNA Tags sind in etwa 10 Sekunden auf der Firewall zu sehen. Das Problem ist, dass die Websocket-Verbindung zusammenbricht und die Verbindung zum EMS neugestartet werden muss.

4.3.3.1. Verbindungsprobleme im VPN

Die Verbindung ins VPN mit allen 3 Testgeräten funktioniert. Die Policy, für den Zugriff auf das interne Netz und das Internet innerhalb des VPNs, wird allerdings nicht richtig appliziert. Die Endpoints verlieren die Internetverbindung, sobald das VPN verbunden wird. Beim Trennen des VPN ist der Internetzugriff wieder vorhanden.

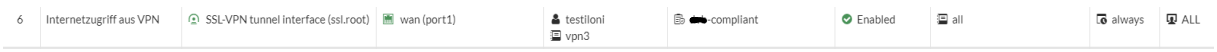


Abbildung 26: Gesetzter ZTNA Tag "compliant" in Policy 6

4.3.3.2. Debugging der Kommunikation zwischen EMS, FortiClient und FortiGate

Im nachfolgenden werden entsprechenden Debug-Methoden, die daraus folgenden Schlüsse und die Unterschiede zu den Versionen angeschaut. Es werden nicht alle Kombinationen genauer beschrieben, da viele die gleichen Bugs/Probleme haben.

Debugging zwischen FortiOS 7.0.3, EMS 7.0.3 und FortiClient 7.0.3

Nach erfolgreicher Verbindung mit dem VPN, verliert der Client den Internetzugriff, obwohl der Client den notwendigen ZTNA-Tag besitzen würde. Auf der FortiGate kann sehr gut nachverfolgt werden, was bei der Synchronisation vom FortClient auf dem Endpoint und der FortiGate passiert und warum das Gerät keine Internetverbindung hat.

Zur Vervollständigung der Meldungen werden die nützlichen Informationen des Debuggens eingeschaltet.

Folgende Befehle wurden auf der FortiGate in der CLI ausgeführt:

```
fwemstest02 # diagnose debug application fcnacd -1
Debug messages will be on for 30 minutes.
```

Abbildung 27: Debugging NAC Daemon auf Firewall

Dieser Befehl erlaubt Realtime Debugging des Network Access Control (NAC) Daemons. Via NAC werden Verbindungen von FortiClients und EMS abgehandelt.

```
fwemstest02 # diagnose debug enable
```

Abbildung 28: Debugging auf Firewall einschalten

Nun wird sämtlicher Verkehr des NAC Daemons angezeigt.

Auf dem Windows Testgerät mit dem Tag «compliant» wird eine VPN Verbindung hergestellt. Das Debug Log zeigt nach etwa 0.5 Sekunden diese Information:

```
[ec_rec_set_sslvpn_conn:972] called (FTCL UID 9AFC6F68EF6141A9917C2E276CD2166C).

[ec_rec_add:1007] called (FTCL UID 9AFC6F68EF6141A9917C2E276CD2166C).

[fcems_call_vpn_client_gateway_call:1134] VPN act connect (UID: 9AFC6F68EF6141A9917C2E276CD2166C, Interface: port1, IP: 10.40.4.1, VDom: root, FortiGate-SN: FG5H0E5818
900027) added to EMS testiems03(FCTEMS0000109967)
[ec_ems_context_submit_work:410] Call submitted successfully.
    obj-id: 6, desc: REST API to send updated regarding VPN updates., entry: api/v1/fgt/gateway_details/vpn.
```

Abbildung 29: Verbindungsanfrage eines Clients für VPN

Die Anfrage für die Verbindung ins VPN kommt vom FortiClient auf dem Endpoint und wird beinahe Realtime vom NAC Daemon erkannt, die IP 10.40.4.1 wird vergeben und das Update wird zum EMS Server gesendet. Der EMS aktualisiert dies innert einiger Sekunden.

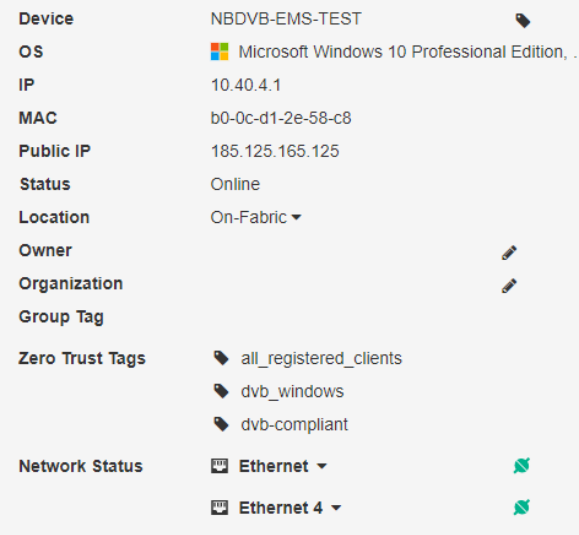


Abbildung 30: VPN-Status eines Clients

Auf dem Endpoint besteht nun allerdings keine Internetverbindung. Um dies genauer zu analysieren, wird der IPv4 Verkehr der Firewall genauer angeschaut.

```
fwemstest02 # diagnose debug flow trace start

fwemstest02 # id=20085 trace_id=45 func=print_pkt_detail line=5824 msg="vd-root:0 received a packet(proto=6, 10.40.4.1:57350->8.8.8.8:443) tun_id=0.0.0.0 from ssl.root
. flag [S], seq 3236187766, ack 0, win 64896"
id=20085 trace_id=45 func=init_ip_session_common line=6003 msg="allocate a new session-0001660d, tun_id=0.0.0.0"
id=20085 trace_id=45 func=vf_ip_route_input_common line=2604 msg="find a route: flag=04000000 gw-46.14.211.89 via port1"
id=20085 trace_id=45 func=fw_forward_handler line=712 msg="Denied by forward policy check (policy 0)"
[ec_ems_context_submit_work:410] Call submitted successfully.
    obj-id: 0, desc: REST API to get EMS Serial Number., entry: api/v1/system/serial_number.
```

Abbildung 31: IPv4-Debug auf Firewall

In diesem Ausschnitt ist ersichtlich, dass die IP 10.40.1.1 geblockt wird. Die Policy mit den ZTNA Tags greift also nicht. Stattdessen greift Policy 0, welche die Anfrage abweist. Darum hat der Endpoint keine Verbindung ins Internet.

Unter Policy & Objects -> ZTNA Tags, wird bis zum Verbinden des Clients mit dem VPN keine lokale IP-Adresse, kein Gerätenamen oder weitere Informationen angezeigt, obwohl der EMS sämtliche nützlichen Informationen zum Gerät hätte. Wird die VPN-Verbindung hergestellt werden die Tags aber geprüft und befüllt. Allerdings ist nur die IP ersichtlich und keine Endpoint Informationen.

Wird die VPN-Verbindung getrennt, ist der Internetzugriff wieder möglich. Die Tags auf der FortiGate sind leer, wenn kein Endpoint mit dem VPN verbunden ist.

4.3.3.3. Auswertung:

Die ZTNA Tags auf EMS 7.0.3 und FortiOS 7.0.3 funktionieren nicht, weil die Endpoints keinen Internetzugriff haben, sobald sie mit dem VPN verbunden sind. Die eigens dafür vorgesehene Policy, dass die Geräte mit dem Tag «compliant» Zugriff auf das Netz haben, wird übersprungen und gemäss Analyse von der Policy abgelöst, die alles blockiert. Da die Verbindung ins Internet aber zwingend notwendig ist, um überhaupt arbeiten zu können, wird diese Version von EMS nicht genutzt werden können. Die EMS Tags werden nicht richtig befüllt und die Endpoints auf der FortiGate gar nie richtig angezeigt.

4.4. Review Sprint 2022/W16

Das Sprint Review bezeichnet das Ende eines Sprints. Abgeschlossen wird der Sprint aber erst kurz vor dem Sprintmeeting am 19. April 2022 für den Sprint 2022/W17

Name	Beschreibung	Erledigt	Grund
Task 771	Firewall Policies mit ZTNA Tags	Nein	Bugs, Funktionalität
Task 768	Evaluation Endpoint Profiles	Nein	Task 771 priorisiert
Task 769	Endpoint Profiles für Clients definieren	Nein	Task 771 priorisiert
Task 764	VPN Verbindungsparameter für Firma festlegen	Nein	Task 771 priorisiert
Task 770	EMS AD Anbindung	Nein	Task 771 priorisiert
Task 778	"compliant" Tag mit unverschlüsseltem USB-Stick behalten	Nein	Task 771 priorisiert

Tabelle 56: Sprint Review 2022/W16

Gespräch mit Product Owner am Donnerstag, 14. April 2022:

Aufgrund von Problemen mit der Verbindung zwischen EMS und der FortiGate sind die weiteren Tasks nicht erledigt. Die versuchten Lösungsvarianten sind nicht zielführend. Die Demonstration der Software verläuft suboptimal. Es besteht weiterhin keine Verbindung ins Internet bei aktiver VPN-Verbindung. Ein Rollback auf 6.4.7 steht nicht zur Diskussion, die Kommunikation zwischen FortiGate und EMS ist ohne Websocket, die ab den Versionen 7.0+ verfügbar ist, nicht zufriedenstellend.

Task 771: Firewall Policies mit ZTNA Tags

Unter FortiOS 6.4.7 ohne Websocket:

Die ZTNA Tags auf EMS 7.0.3 und FortiOS 6.4.7 funktionieren nur verzögert. Es kann mehrere Minuten dauern, bis ein Gerät mit dem Tag «compliant» in der FortGate ersichtlich ist. Die Verbindung ins VPN kann dadurch teilweise gar nicht aufgebaut werden. Ist der Endpoint in der Firewall angekommen, dauert das Verbinden mit dem VPN bis zu 45 Sekunden.

Die Verbindung zwischen EMS und FortiOS ist instabil. Die Informationen die im EMS vorhanden sind, werden nicht vollständig in die FortiGate geladen. Es dauert mehrere Minuten, bis ein Client mit dem «compliant» Tag in der FortiGate ersichtlich wird. Die Verbindung des Endpoints auf das VPN und das Internet funktioniert, sobald dieser in die FortiGate geladen ist.

Unter FortiOS 7.0.3 mit Websocket Verbindung:

Die ZTNA Tags auf EMS 7.0.3 und FortiOS 7.0.3 funktionieren nicht, die Endpoints haben keinen Internetzugriff, sobald sie mit dem VPN verbunden sind. Die eigens dafür vorgesehene Policy, dass die Geräte mit dem Tag «compliant» Zugriff auf das Netz haben, wird übersprungen und gemäss Analyse von der Policy abgelöst, die alles blockiert. Da die Verbindung ins Internet aber zwingend notwendig ist, um überhaupt arbeiten zu können, wird diese Version von EMS nicht genutzt werden können. Die EMS Tags werden nicht richtig befüllt und die Endpoints auf der FortiGate nicht richtig angezeigt.

Feststellungen des Diplomanden:

Die Firewall Policy kann nicht zufriedenstellend mit den ZTNA-Tags eingesetzt werden. Das Debugging erfordert die ganze Woche und sämtliche StoryPoints, die zur Verfügung stehen. Diese Lösungsansätze hat der Diplomand geprüft:

- Up- und Downgrades von FortiOS
- Up- und Downgrades von FortiClient
- Up- und Downgrades von FortiClient EMS
- Firewall Konfiguration anpassen
- Grosse Anzahl von Reboots von EMS und Firewall
- Traffic Flow der verbundenen Endpoints analysiert
- Websocket Analysen zwischen FortiGate und FortiEMS
- Studieren der Release Notes / Known Issues von diversen Versionen
- Neuinstallationen von FortiClient EMS und FortiClients
- Endpoint Records prüfen
- Dynamische Einträge der Firewall prüfen
- NAC Daemon Debugging (Network Access Control)

Es gibt in den verschiedenen Versionen teilweise die gleichen Probleme, welche wiederum in anderen Versionen gelöst sind. Jedoch funktionieren in diesen Versionen andere Elemente nicht. Insgesamt kann der FortiClient EMS 7.0+ so nicht eingesetzt werden.

In dieser Tabelle sind die versuchten Kombinationen aus FortiOS, FortiClient und FortiClient EMS ersichtlich.

Versuchte Kombinationen, die einen stabilen Internetzugang nach der Verbindung mit dem VPN besitzen:

EMS Version	FortiClient Version	FortiOS/FortiGate Version	Stabil
7.0.3	7.0.3	6.4.7	Ja
7.0.3	7.0.3	7.0.3	Nein
7.0.3	7.0.3	7.0.4	Nein
7.0.3	7.0.3	7.0.5	Nein
7.0.3	7.0.3	7.2.0	Nein
7.0.2	7.0.3	7.2.0	Nein
6.4.8	7.0.3	7.0.3	Nein
7.0.3	7.0.3	6.4.8	Nein
7.0.2	7.0.2	6.4.8	Nein
7.0.2	7.0.3	7.0.3	Nein

Abbildung 32: Versuchte Kombinationen FortiOS, FortiClient und FortiClient EMS

Anforderungen Product Owner

Der Product Owner möchte, dass die nicht erledigten Tasks ins Backlog aufgenommen werden. Er gibt einen neuen Task für den Epic «Installation und Konfiguration EMS 7.0» vor:

- Task 779 - Support-Case bei Fortinet erstellen/bearbeiten, um die Problematik mit den Tags zu lösen

Aktuell genutzte Versionen:

Software	Version
FortiClient auf Windows Testgerät	7.0.3
FortiClient auf Linux Testgerät	7.0.3
FortiClient auf macOS Testgerät	7.0.3
FortiOS auf Testfirewall FortiGate 500E	7.0.5
FortiClient EMS	7.0.3

Tabelle 57: Aktuell genutzte Versionen nach Sprint 2022/W16

4.5. Sprint 2022/W17

Im Sprintmeeting des dritten Sprints definiert der PO weitere Tasks. In dieser Woche sind nur 8 StoryPoints zu vergeben, da am 18.04.2022 ein Feiertag ist. Diese Woche ist kürzer und die Anzahl an Tasks etwas zu hoch angesetzt. Der Product Owner entscheidet, dass mit den derzeit aktuellen Versionen von FortiClient (7.0.3), FortiClient EMS (7.0.3) und FortiOS (7.0.5) weitergetestet werden soll. Er verlangt für diesen Sprint folgende Tasks:

Name	Beschreibung	Startdatum	StoryPoints	Enddatum
Task 779	Support-Case bei Fortinet erstellen/bearbeiten	14.04.2022	2	20.04.2022
Task 768	Evaluation Endpoint Profiles	19.04.2022	2	20.04.2022
Task 769	Endpoint Profiles für Clients definieren	20.04.2022	1	21.04.2022
Task 764	VPN Verbindungsparameter für Firma festlegen	21.04.2022	1	21.04.2022
Task 772	VPN vor Login unter Windows / Linux / Mac einrichten, testen	21.04.2022	2	22.04.2022
Task 765	Client Rollout ablauf mit Client Management besprechen	22.04.2022	1	22.04.2022
Task 778	"compliant" Tag mit unverschlüsseltem USB-Stick behalten	-	1	-
Task 770	EMS AD Anbindung	-	1	-

Tabelle 58: Übersicht Sprint 2022/W17

4.5.1. Task 779: Support-Case bei Fortinet erstellen/bearbeiten

Um eine raschere Antwort von Fortinet zu erhalten, erstellt der Diplomand das Ticket bereits am 14. April 2022.

Basic Information | **Subject:** Firewall Policy using ZTNA Tags doesnt work as expected

Ticket Number:	5993037	**Serial Number:**	FG5H0E5818900027
Status:	RcvdCustFB	**Ticket Priority:**	P3
Creation Date:	2022-04-14	**Close Date:**	N/A
S/W Version:	7.0 Patch5	**Owner:**	Ahmed Saeed
Request Type:	Technical Assistance	**Category:**	FGT Firewall

Abbildung 33: Erstelltes Fortinet Ticket

Folgender Befehl soll gemäss Support von Fortinet auf der FortiGate ausgeführt werden:

« diagose firewall iprope list 100004 | grep 'policy index=6' -A 20 »

Das Ergebnis dieses Befehls wird dem Ticket angefügt und gibt folgenden Fehler aus:

```
fwemstest02 # diagnose firewall iprope list 100004 | grep 'policy index=6' -A 20
policy index=6 uuid_idx=536 action=accept
flag (8050121): log auth nat master use_src pol_stats
flag2 (6030): fw wsso log_fail resolve_sso
flag3 (a0): link-local best-route
schedule(always)
cos_fwd=255 cos_rev=255
group=00100004 av=00000000 au=00000003 split=00000000
host=0 chk_client_info=0x0 app_list=0 ips_view=0
misc=0
zone(1): 31 -> zone(1): 9
source(1): 10.40.4.0-10.40.4.255, uuid_idx=516,
dest(1): 0.0.0.0-255.255.255.255, uuid_idx=506,
user group(1): 16777218
service(1):
[0:0x0:0/(0,65535)->(0,65535)] helper:auto
ztna-ems-tag address (1): ERROR: Tried to convert non-legacy firewall address to legacy format!

policy index=0 uuid_idx=1 action=drop
flag (8010801): log d_rm master pol_stats
flag2 (4000): resolve_sso
```

Abbildung 34: Ergebnis CLI-Befehl von Fortinet

Die Lösung des Problems ist gemäss Fortinet die Version 7.0.6, welche im Monat Mai offiziell ausgegeben wird. Da Fortinet manchmal ein pre-release zur Verfügung stellt, wird angefragt, ob es zur Verfügung gestellt werden kann.

Fortinet gibt via Ticket zu Protokoll, dass dieser Bug dem Bug 770877 ähnelt. Am 20.04 stellt die Fortinet der Firma die interim Version von FortiOS 7.0.6 build 0334 zur Verfügung. In dieser Version soll dieser Bug behoben werden. Damit verifiziert werden kann ob die Tags in der Policy funktionieren, wird in diesem Task auch ein kurzes Testing durchgeführt. Nach dem zur Verfügung stellen der Version ist kein weiterer Support durch Fortinet mehr gewährleistet, da es sich um kein offizielles Release handelt.

ZTNA

Bug ID	Description
765813	ZTNA access is systematically denied for ZTNA rule using SD-WAN zone as an incoming interface.
770350	ZTNA tags do not follow the correct policy when bound in a single policy. They also do not work with groups.
770877	Traffic was blocked by mismatched ZTNA EMS tags in a forwarding firewall policy.
777669	The secondary IP address in the EMS dynamic address table does not match the expected policy.

Abbildung 35: ZTNA Bug 770877

Funktionskontrolle von Policy #6:

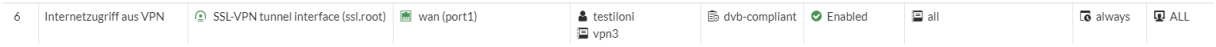


Abbildung 36: Policy 6 in FortiGate 500E

Unter Windows Client:

- Funktioniert auf Anhieb, keine Fehlermeldung mehr in der Policy
- Internetverbindung nach erfolgreichem Verbinden per VPN vorhanden
- Verliert die Internetverbindung nach undefinierbarer Zeit
- Erneutes Login in VPN = Kein Internetzugriff
- Tags neu synchronisieren, EMS neu starten

Mac Client:

- Weiterhin keine Verbindung ins Internet nach Aufbau VPN
- Neuinstallation von FortiClient ohne Erfolg
- Gerät auf FortiGate nicht ersichtlich unter ZTNA Tags
- Gerät nach EMS Neustart ersichtlich, weiterhin kein Internetzugriff im VPN

Linux:

- Keine Verbindung ins Internet möglich während VPN
- EMS neu starten behebt das Problem vorübergehend
- Verbindung ins Internet während VPN-Verbindung teilweise vorhanden

Die Eingabe des gleichen Befehls wie in FortiOS 7.0.3 gibt untenstehendes Resultat aus.
Fehlermeldung in der Policy ist nicht mehr zu sehen:

```
fwemstest02 # diag fire iprope list 100004 | grep 'policy index=6' -A 20
policy index=6 uuid_idx=557 action=accept
flag (8050121): log auth nat master use_src pol_stats
flag2 (6030): fw wsso log_fail resolve_sso
flag3 (a0): link-local best-route
schedule(always)
cos_fwd=255  cos_rev=255
group=00100004 av=00000000 au=00000003 split=00000000
host=0 chk_client_info=0x0 app_list=0 ips_view=0
misc=0
zone(1): 31 -> zone(1): 9
source(1): 10.40.4.0-10.40.4.255, uuid_idx=516,
dest(1): 0.0.0.0-255.255.255.255, uuid_idx=506,
user group(1): 16777218
service(1):
        [0:0x0:0/(0,65535)->(0,65535)] helper:auto
ztna-ems-tag address (1):  uuid_idx=523
        FCTEMS0000109967_dvb-compliant ID(88) ADDR(192.168.11.64) ADDR(192.168.11.73) ADDR(10.40.4.1)

policy index=0 uuid_idx=1 action=drop
flag (8010801): log d_rm master pol_stats
flag2 (4000): resolve_sso
```

Abbildung 37: Ergebnis CLI-Befehl Fortinet nach Update auf 7.0.6

4.5.1.1.1. Auswertung

Das Ticket ist geschlossen, da kein Support für die interim-Version 7.0.6 verfügbar ist. Die bisherige Fehlermeldung der FortiGate erscheint nicht mehr. Allerdings hat dies das Problem leider nicht gelöst. Der Fehler erscheint zwar nicht und die Tags werden sauber in die FortiGate synchronisiert. Allerdings werden die Tags nicht richtig mit den Endpoints befüllt. Mac-Clients sind gar nicht mehr ersichtlich und Windows sowie Linux Clients werden nach einiger Zeit nicht mehr erkannt und verlieren ihren Internetzugriff im VPN.

Das Update von FortiOS 7.0.5 auf 7.0.6 interim build0334 hat einen Fehler entfernt und die Internetverbindung funktioniert teilweise. Leider ist auch dies bis auf Weiteres nicht brauchbar, um EMS produktiv einzusetzen. Die Synchronisation zwischen EMS und der FortiGate muss manuell neu gestartet werden, damit die Endpoints ersichtlich sind.

4.5.2. Task 768: Evaluation Endpoint Profiles

In der Version 7.0.3 gibt es einige Quality of Life Veränderungen und Verbesserungen. Es können diverse Endpoint Profile für die jeweiligen Kategorien (z.B. Remote Access, Webfilter) erstellt werden und in den Policies dynamisch ausgewählt werden.

Folgende Endpoint Features können eingestellt werden:

Profile Name	Grundfunktionalität
Remote Access	SSL-VPN, IP-Sec VPN, VPN Tunnels
ZTNA Connection Rules	Zero Trust Network Access über ProxyServer
WebFilter	Webfilter nach Kategorien einstellbar etc.
Vulnerability Scan	FortiClient Vulnerability Scans ansetzen, triggern etc.
Sandbox	
Firewall	
Malware Protection	AntiVirus, Anti-Ransomware Tools, Schutz des Clients
System Settings	Einstellungen des FortiClients auf den Endpoints anpassen
Chromebook Features	

Tabelle 59: Endpoint Features

Für jede Kategorie gibt es eine «default»-Variante. Die Features lassen sich nach Belieben in den Einstellungen des EMS aktivieren oder deaktivieren. Während der ersten Phase des Testens, sind diese etwas angepasst worden, damit die Funktionalität der Tunnel, des VPN's etc. sichergestellt ist. In der Evaluation werden die verschiedenen Profile genauer analysiert. Viele der Einstellungen sind nicht systemrelevant und werden daher aussen vorgelassen. Der Fokus liegt auf den wichtigen Features und deren Einstellungsmöglichkeiten.

4.5.2.1. Remote Access

In den Remote Access Profilen können Einstellungen zu Virtual Private Networks gemacht werden. Es gibt diverse Einstellungen, die vorgenommen werden können.

Name	Optionen	Nutzen
Allow Personal VPN	ON / OFF	Zusätzliche VPN Verbindungen manuell im FortiClient hinzufügen
Show VPN before Logon	ON /OFF	VPN-Verbindung vor dem Windows Login anzeigen
Minimize FortiClient	ON / OFF	FortiClient minimieren, wenn VPN verbunden ist
Show Connection Progress	ON / OFF	Fortschritt der Verbindung in %-Angabe bei der Verbindung zum VPN anzeigen
Suppress VPN Notifications	ON / OFF	Benachrichtigungen zum VPN unterdrücken
Enable Secure Remote Access	ON / OFF	Sicheren Remote Zugriff erlauben
Current Connection	Tunnel auswählen	Remote Zugriff auf Tunnel auswählen
Always Up Max Tries	0 = unbegrenzt, 1 - X	Maximale Anzahl an Wiederverbindungsversuchen nach einem Verbindungsverlust
SSL VPN	ON / OFF, div. Weitere Einstellungen	SSL-VPN aktivieren oder deaktivieren
IPsec VPN	ON / OFF, div. Weitere Einstellungen	IPsec VPN aktivieren oder deaktivieren
VPN Tunnels	Tunnel hinzufügen, bearbeiten oder löschen	Tunnel hinzufügen, bearbeiten oder löschen

Tabelle 60: Remote Access Einstellungen

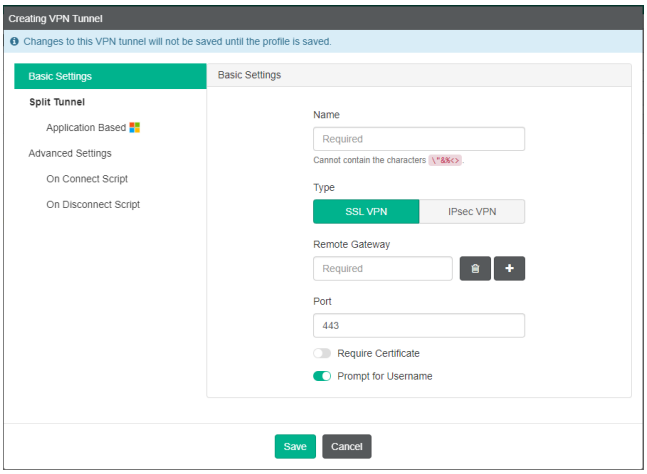


Abbildung 38: Einstellungen VPN unter Remote Access

Unter den « Advanced Settings » des VPNs können weitere Optionen gewählt werden. Unter Windows kann ein ZTNA Tag ausgewählt werden, welcher den Zugriff regelt. Darüber kann auch eine Meldung ausgegeben, wenn das Gerät nicht «compliant» ist. Als Alternative kann diese Variante allerdings nicht verwendet werden, da sie nur unter Windows funktioniert.

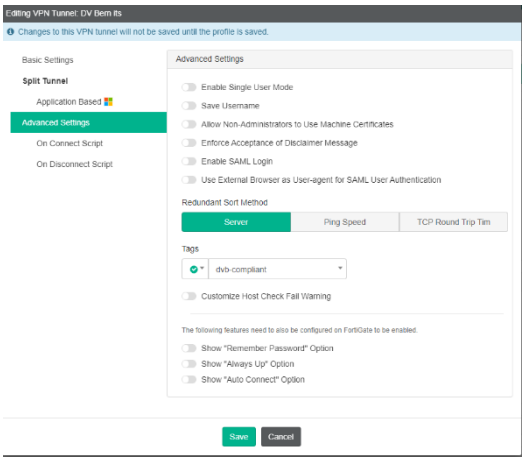


Abbildung 39: Fortgeschrittene Einstellungen für VPN

4.5.2.2. ZTNA Connection Rules

Die ZTNA Connection Rules werden benutzt, um einen Zugang via Proxy-Server (ZTNA Server) in ein VPN aufzubauen. Diese Rules werden nicht benutzt und werden nicht weiter erläutert.

4.5.2.3. Webfilter

Im Webfilter lassen sich Einstellungen zum Browsen im Web anpassen. So kann aus Kategorien ausgewählt werden, welche Art von Webseiten blockiert werden sollen. Weiter können Logs zu allen URLs eingestellt werden und diese Daten später verarbeitet werden. Der Webfilter im EMS ist aber innerhalb der Firma obsolet, da die Einstellungen zu Surfverhalten, Webfilter und SafeSearch bereits auf der FortiGate der Firma eingestellt sind. Dieses Feature kann aber benutzt werden, um die Geräte auch ausserhalb der Firma mit einem Webfilter zu überwachen.

4.5.2.4. Vulnerability Scan

Der Vulnerability Scan dient dem Einordnen der Endgeräte in 4 Sicherheitskategorien:

- Low
- Medium
- High
- Critical

Gemäss diesen Kategorien können die Endpoints gefiltert und entsprechend angegangen werden, damit sie in eine tiefere Kategorie fallen. Folgende Einstellungen sind möglich im Vulnerability Scan Profil:

Name	Optionen	Nutzen
Scan on Registration	ON / OFF	Wenn die Verbindung zwischen FortiClient und FortiClient EMS hergestellt wird, soll die Vulnerability gescannt werden.
Scan on Vulnerability Signature Update	ON / OFF	Bei einem Update der Signaturen soll der Endpoint gescannt werden.
Scan on OS Update	ON / OFF	Nach OS Updates soll der Scan ausgeführt und der Endpoint neu bewertet werden
Enable Proxy	ON / OFF	Proxy Server ein- oder ausschalten
Automatic Maintenance	ON /OFF	Automatische Wartung einschalten und konfigurieren oder ausschalten
Scheduled Scan	ON / OFF	Geplante Scans einschalten und konfigurieren oder ausschalten
Automatic Patching	ON / OFF	Automatisches Patchen von «Critical» Endpoints aktivieren oder deaktivieren
Exclusions	ON / OFF	Diverse Ausnahmen (z.B. Applikationen) die nicht vom Scan betroffen sein sollen

Tabelle 61: Vulnerability Scan Einstellungen

4.5.2.5. Malware Protection

In diesem Profil bietet Fortinet den eigenen Anti Virus, Anti-Ransomware und viele weitere Sicherheitsfeatures an. Diese Profile werden allerdings nicht verwendet, da in der Firma bereits ESET für diese Funktionen im Betrieb ist und dieser nicht abgelöst wird. Auf die genaue Auflistung der Möglichkeiten innerhalb dieser Profile wird verzichtet.

4.5.2.6. Sandbox

Mittels Sandbox können E-Mails, Anhänge, Dokumente und weitere verdächtige Dateien an eine FortiSandbox Appliance gesendet und analysiert werden. Dort werden sie auf Viren, Trojaner, Keylogger etc. untersucht, ohne dass diese Schaden an Endpoints anrichten können. Dazu werden allerdings Lizenzen für einen Sandbox Server oder für den Cloud-Dienst von Fortinet benötigt. Diese Lizenzen sind in der Firma nicht vorhanden.

4.5.2.7. Firewall

Der FortiClient EMS hat keine eigene Firewall eingebaut. Allerdings können in den Firewall Profilen die Einstellungen der FortiGate auf die jeweiligen Endpoints angepasst werden. Diese Einstellungen werden über die FortiGuard global über die gesamte Organisation angewandt und werden vom EMS nicht weiter angepasst. Die Firewall Profile werden deaktiviert und nicht weiter behandelt.

4.5.2.8. System Settings

In den System Settings werden die Einstellungen zum Verhalten der FortiClients auf den Endpoints angepasst. Folgende Einstellungen werden als wichtig/nützlich erachtet und können im Profil genutzt werden:

User Interface

Name	Optionen	Nutzen
Require Password to Disconnect from EMS	ON / OFF, Passwort setzen	Passworteingabe nötig, wenn sich ein Endpoint von EMS trennen will
Do not Allow User to Back up Configuration	ON / OFF	Dem User das sichern der Konfiguration des FortiClients verbieten oder erlauben
Allow User to Shutdown When Registered to EMS	ON / OFF	Bei einer aktiven Verbindung dem Benutzer das ausschalten des FortiCleints erlauben oder verbieten
Show Zero Ttrust Tag on FortiClient GUI	ON / OFF	Zero Trust Tags im Graphical User Interface des FortiClients anzeigen
Client-Based Logging When On-Fabric	ON / OFF	Wenn der Client On-Fabric ist, soll dieser die Client Logs anzeigen oder nicht anzeigen

Tabelle 62: User Interface Einstellungen in den System Settings

Log

Name	Optionen	Nutzen
Level	Info, Alert, Critical, Emergency, Warning, Error, Notice, Debug	Erstellt Logs die die gewählte Stufe und höhere ausgeben
Client Based Logging When On-Fabric	ON / OFF	Lokale Endpoint Logs aktivieren wenn On-Fabric

Tabelle 63: Log Einstellungen in den System Settings

Endpoint Control

Name	Optionen	Nutzen
Disable Disconnect	ON / OFF	Den Benutzern das trennen zur Telemetry Verbindung erlauben oder verbieten

Tabelle 64: Endpoint Control Einstellungen in den System Settings

4.5.2.9. Chromebook Feature

In der Firma werden keine Google Chromebooks oder Google Domains verwendet.

4.5.3. Task 769: Endpoint Profiles für Clients definieren

Features, welche die Firma benutzen wird:

- Remote Access
- Vulnerability Scan
- System Settings

Features, welche die Firma nicht benutzen wird:

- Sandbox
- Malware Protection
- Firewall
- Zero Trust Network Access
- Chormebook Features

4.5.3.1. Remote Access der Firma

Der einfacheren Verständlichkeit halber werden nur die Einstellungen aufgelistet, welche von Bedeutung sind.

Für Clients der Firma machen mehrere Profile Sinn. Zum einen werden 3 verschiedene SSL-VPN Verbindungen erstellt. Für die Remote Access Profile in der Firma werden jeweils ein weiteres Profil für die Erstellung von persönlichen, neuen VPN's erstellt. Es gibt einige Fälle, in denen ein weiteres VPN eingerichtet werden muss. Beispielsweise bei den Entwicklern, die auf das Netzwerk des Bundes o.Ä. zugreifen müssen.

Profil «dev-production »

Name	On / Off	Bemerkungen
Allow Personal VPN	Off	Zusätzliche VPN Verbindungen manuell im FortiClient hinzufügen
Show VPN before Logon - Use Windows Credentials	ON ON	VPN-Verbindung vor dem Windows Login anzeigen
Minimize FortiCLient Console on Connect	ON	FortiClient nach Verbinden mit VPN minimieren
SSL-VPN	ON	Verbindung mit SSL VPN herstellen erlauben
VPN Tunnel	ON	Tunnel für VPN einrichten

Tabelle 65: Endpoint Profil "dev-production"

Profil «dev-production-allow-personal»

Name	On / Off	Bemerkungen
Allow Personal VPN	ON	Zusätzliche VPN Verbindungen manuell im FortiClient hinzufügen
Show VPN before Logon - Use Windows Credentials	ON ON	VPN-Verbindung vor dem Windows Login anzeigen
Minimize FortiCLient Console on Connect	ON	FortiClient nach Verbinden mit VPN minimieren
SSL-VPN	ON	Verbindung mit SSL VPN herstellen erlauben
VPN Tunnel	ON	Tunnel für VPN einrichten

Tabelle 66: Endpoint Profil "dev-production-allow-personal"

Profil «its-production»

Name	On / Off	Bemerkungen
Allow Personal VPN	OFF	Zusätzliche VPN Verbindungen manuell im FortiClient hinzufügen
Show VPN before Logon - Use Windows Credentials	ON ON	VPN-Verbindung vor dem Windows Login anzeigen
Minimize FortiCLient Console on Connect	ON	FortiClient nach Verbinden mit VPN minimieren
SSL-VPN	ON	Verbindung mit SSL VPN herstellen erlauben
VPN Tunnel	ON	Tunnel für VPN einrichten

Tabelle 67: Endpoint Profil "its-production"

Profil «its-production-allow-personal»

Name	On / Off	Bemerkungen
Allow Personal VPN	ON	Zusätzliche VPN Verbindungen manuell im FortiClient hinzufügen
Show VPN before Logon - Use Windows Credentials	ON ON	VPN-Verbindung vor dem Windows Login anzeigen
Minimize FortiCLient Console on Connect	ON	FortiClient nach Verbinden mit VPN minimieren
SSL-VPN	ON	Verbindung mit SSL VPN herstellen erlauben
VPN Tunnel	ON	Tunnel für VPN einrichten

Tabelle 68: Endpoint Profil "its-production-allow-personal

Profil «office-production»

Name	On / Off	Bemerkungen
Allow Personal VPN	OFF	Zusätzliche VPN Verbindungen manuell im FortiClient hinzufügen
Show VPN before Logon - Use Windows Credentials	ON ON	VPN-Verbindung vor dem Windows Login anzeigen
Minimize FortiCLient Console on Connect	ON	FortiClient nach Verbinden mit VPN minimieren
SSL-VPN	ON	Verbindung mit SSL VPN herstellen erlauben
VPN Tunnel	ON	Tunnel für VPN einrichten

Abbildung 40: Endpoint Profil "office-production"

Remote Access Profiles

Name	Updated
Default	2022-04-19 13:39
its-production	2022-04-22 16:14
dev-production	2022-04-19 16:03
dev-production-allow-personal	2022-04-19 16:03
office-production	2022-04-19 16:03
its-production-allow-personal	2022-04-22 14:25

Abbildung 41: Übersicht Remote Access Profiles

Die verschiedenen Profile haben jeweils eine andere Verbindung ins interne Netzwerk mit individuellen Berechtigungen, je nach zugewiesenem Profil.

4.5.3.2. Vulnerability Scan

Die Einstellungen für den Vulnerability Scan sind standardmässig nur während OS Update eingeschaltet. Ein täglicher Scan macht Sinn, da die HomeOffice Pflicht aufgehoben und die Angestellten vermehrt ins Büro kommen.

Einstellungen in der Firma

Name	On / Off	Bemerkungen
Scan on Registration	ON	Schwachstellen-Suche bei VPN Verbindung
Scan on OS Updates	ON	Bei Updates des Betriebssystems den Scan starten
Scheduled Scan	ON	Einstellungen für geplante Scans

Tabelle 69: Einstellungen Vulnerability Scan in der Firma

Ein Vulnerability Scan dauert je nach Gerät zwischen 2 und 10 Minuten. Da der Scan im Hintergrund läuft, stört dies den User nicht weiter.

4.5.3.3. System Settings

Name	On / Off	Bemerkungen
Require Password to Disconnect from EMS	ON	Passworteingabe anfordern, wenn die Verbindung zum EMS getrennt wird
Allow User to Shutdown when connected to EMS	OFF	Den Usern erlauben oder verbieten, FortiClient zu beenden, wenn er beim EMS registriert ist
Show Zero Trust Tag	ON	Zero Trust Status anzeigen

Tabelle 70: Einstellungen System Settings in der Firma

Zero Trust Tag kann helfen, die Nutzer:innen selbst auf ein Problem aufmerksam zu machen. Dies erleichtert dem Support die Arbeit, da wahrscheinlich die Voraussetzungen für den «compliant»-Tag nicht erfüllt sind.

Ausserdem soll es den Mitarbeiterinnen und Mitarbeiter nicht erlaubt sein, die Verbindung zum EMS zu trennen, um eine weitere VPN-Verbindung einzurichten. Wer eine weitere VPN Verbindung braucht, muss dies via Anfrage bei der Vorgesetzten Person beantragen. Das Beenden des FortiClient bei aktiver Verbindung zum EMS wird nicht gestattet.

Die Log Einstellungen können auf «Default» belassen werden.

4.5.4. Task 764: VPN Verbindungsparameter für Firma festlegen

In der Firma gibt es standardmässig bereits 3 VPN Verbindungen für Entwickler (DEV), die Services (ITS) und die Administration (Office).

Die bereits produktiv im Einsatz stehenden VPNs werden beibehalten und übernommen:

FIRMA DEV: vpn.firma.ch/dev

FIRMA Services: vpn.firma.ch/its

FIRMA Office : vpn.firma.ch/office

4.5.5. Task 772: VPN vor Login unter Windows / Linux / Mac einrichten, testen

Um eine möglichst angenehme Benutzererfahrung zu erreichen, soll es möglich sein sich vor dem Windows Login mit dem VPN der Firma zu verbinden. Die Option «Show VPN before Logon» soll in den Endpoint Profiles aktiviert werden.

Windows:

- VPN vor Login OK («compliant» und nicht «compliant»)
- Mit Windows Anmeldung kann nicht getestet werden, da kein Active Directory Server zum Testen zur Verfügung steht

Abbildung 42: VPN vor Login unter Windows

Linux und MacOS:

Die Option VPN vor Login steht nur Windows-Usern zur Verfügung. Unter Linux und Mac könnte eine VPN Verbindung via Script vor dem Login ermöglicht werden. Das VPN läuft aber via FortiClient und verhält sich nicht wie die standardmässigen VPNs. Die Verbindung mittels FortiClient vor dem Login aufzubauen ist nicht möglich.

Fazit:

Das VPN vor Login funktioniert nur unter Windows. Das Logo von Fortinet ist unter den Anmeldeoptionen ersichtlich. Nach Auswahl des VPN-Tunnels und der Eingabe der geforderten Benutzerdaten verbindet sich das VPN in unter 30 Sekunden und meldet den Benutzer bei Windows an. Da die Anmeldung bei Windows am Testobjekt ein anderes Passwort benötigt, muss dieses ebenfalls noch eingegeben werden. Die Anmeldung funktioniert und das VPN ist nach dem Anmelden verbunden.

4.5.6. Task 765: Client Rollout Ablauf mit Client Management besprechen

Herr Schmid ist der Client Management Verantwortliche der Firma. Der Ablauf des FortiClient 7.0.3 wird an einem Termin mit ihm besprochen, falls EMS 7.0.3 live gehen kann.

Besprechung am 22. April 2022 um 08:30 Uhr

Folgende Schritte müssen unternommen werden, um die Windows Endpoints auf eine neue Version zu aktualisieren:

- Nächstes Wartungsfenster definieren/erörtern
- Gesamte Firma informieren, dass Geräte sich neustarten werden:
    - Informationen zum Troubleshooting
    - Wie lange dauert es
    - Was wenn kein VPN
    - Wo melden bei technischen Problemen?
- FortiClient Installer aus EMS bereitstellen
- Aufnahme in HighSystems Client Management Tool
- Durch Client Management: Deinstallation von allen FortiClients, die derzeit installiert sind
- Durch Client Management: Rollout der neuen FortiClients 7.0.3

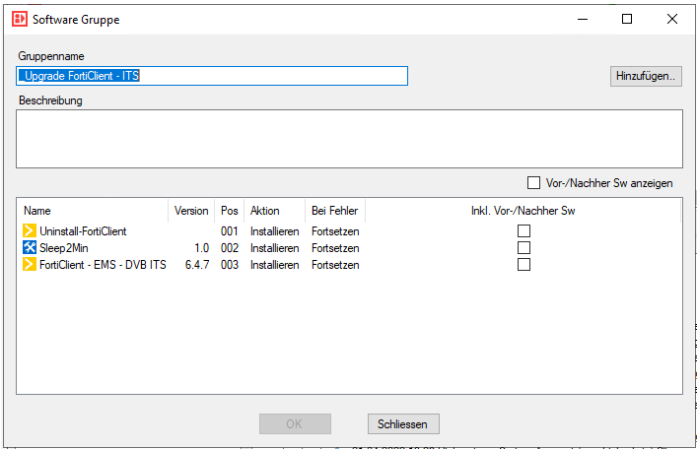


Abbildung 43: Sofware Rollout für FortiClient 7.0.3

Im Highsystem können Software-Pakete erstellt werden, welche an alle Clients der Firma zur Installation versendet werden. Zuerst wird der FortiClient deinstalliert (Version egal), wonach sich das Gerät ohne Ankündigung neustarten wird. Nach dem Neustart wird 2 Minuten gewartet bevor der FortiClient mit der aktuellen Version installiert wird. Es wird ein weiterer Neustart empfohlen, ist aber technisch nicht notwendig.

Mac Endpoints:

Die Endpoints mit macOS müssen manuell auf die neuste Version aktualisiert werden. Derzeit sind aber nur wenige Geräte in der Firma mit macOS bestückt. Der Aufwand ist deshalb überschaubar. Zusätzlich müssen die Geräte nicht neugestartet werden, um das Update abzuschliessen.

Linux Endpoints:

Ähnlich den Macs müssen die Linux Clients manuell auf die neuste Version aktualisiert werden. Hier ist der Aufwand etwas grösser, da ca. 15 Geräte mit Linux Ubuntu 18+ ausgestattet sind. Die User, die

mit Linux Ubuntu arbeiten werden separat angegangen und manuell auf das neuste Update gehoben. Die Verbindung zum EMS geht während der Installation der neuen Version nicht verloren.

4.5.7. Task 778: "compliant" Tag mit unverschlüsseltem USB-Stick behalten

Wird ein unverschlüsselter Stick an einen Windows-Endpoint gehängt, verliert dieser den «compliant»-Tag. Dies, weil der FortiClient sämtliche Laufwerke des Endpoints prüft und dies dann dem EMS meldet.

Unter FortiClient 6.4.2 gibt es einen entsprechenden «Known Issues» Eintrag mit der Bug ID 667757:

667757	Bitlocker Zero Trust tagging rule does not match on endpoint with USB drive attached.

Abbildung 44: Known Issue 667757 unter FortiClient 6.4.2

Der Bug ist aus einer alten FortiClient Version. Bei aktiver VPN Verbindung verliert das Gerät den «Bitlocker enabled»-Status, sobald eine externe Festplatte oder ein USB-Stick angeschlossen wird. Ist das angeschlossene Laufwerk mit Bitlocker verschlüsselt, behält der Client seinen «Bitlocker enabled»-Status.

Testing:

USB Stick der Firma, verschlüsselt mit Bitlocker. Der Tag bleibt beim Verbinden des Geräts bestehen. Wird der Stick wieder entschlüsselt verliert der Client den Tag innert weniger Sekunden.

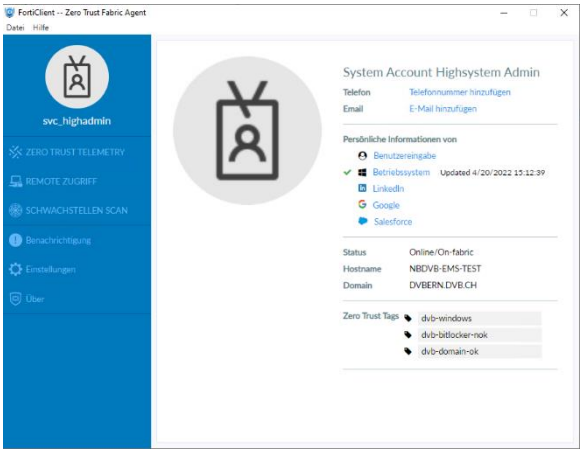


Abbildung 45: Bitlocker nicht aktiv bei USB Sticks ohne Verschlüsselung

Mittels EMS kann nicht gewählt werden, welche Festplatten/SSD usw. verschlüsselt sein müssen, damit die Regel angewendet wird. Dort besteht also keine Möglichkeit. Dem Product Owner wird angeboten, ein Supportticket bei Boll zu eröffnen. Dieses wird am 25. April erstellt.

4.6. Review Sprint 2022/W17

Das Sprint Review bezeichnet das Ende eines Sprints. Abgeschlossen wird der Sprint kurz vor dem Sprintmeeting am 25. April für den Sprint 2022/W18

Name	Beschreibung	Erledigt	Grund
Task 779	Support-Case bei Fortinet erstellen/bearbeiten	Ja	
Task 768	Evaluation Endpoint Profiles	Ja	
Task 769	Endpoint Profiles für Clients definieren	Ja	
Task 764	VPN Verbindungsparameter für Firma festlegen	Ja	
Task 772	VPN vor Login unter Windows / Linux / Mac einrichten, testen	Ja	
Task 765	Client Rollout Ablauf mit Client Management besprechen	Ja	
Task 778	"compliant" Tag mit unverschlüsseltem USB-Stick behalten	Nein	Keine passende Lösung gefunden
Task 770	EMS AD Anbindung	Nein	Kein Testserver vorhanden

Tabelle 71: Sprint Review 2022/W17

Gespräch mit Product Owner am Freitag, 22. April 2022:

Die meisten Tasks sind abgearbeitet. Nach der Demonstration des EMS hat der Product Owner entschieden, die produktive Umsetzung einzustellen. Die verbleibenden Tasks sollen auf dem Testsystem zu Ende geführt werden. Eine Umsetzung in der Firma ist mit den momentanen Problemen nicht möglich.

Abgeschlossene Tasks

Task 765: Client Rollout Ablauf mit Client Management besprechen:

Der Austausch mit dem Verantwortlichen des Client Management verläuft positiv. Die Anforderungen zur Umsetzung können geklärt werden ohne dabei die Sicht der Mitarbeiter:innen zu vernachlässigen.

Task 772: VPN vor Login unter Windows / Linux / Mac einrichten, testen

Das Testen dieses Feature funktionierte einwandfrei. Leider funktioniert die Option nur unter Windows und nicht unter MacOS oder Linux. Da aber ca. 90% der Geräte in der Firma mit Windows laufen und nur vereinzelt MacOS Produkte im Umlauf sind, ist dies zu vernachlässigen.

Task 768: Evaluation Endpoint Profiles

Die Profile unter EMS 7.0.3 sind etwas einfacher zu gestalten als in den älteren Versionen von EMS. So können die Profile erstellt werden und später in den Policies dynamisch eingerichtet werden.

Task 769: Endpoint Profiles für Clients definieren

Die Profile für die Endpoints der Firma sind definiert. Sie können in den Policy-Einstellungen des EMS dynamisch zugeordnet werden. Die Einrichtung verläuft ohne Probleme.

Task 779: Support-Case bei Fortinet erstellen/bearbeiten

Der Case ist eröffnet und die Pre-Release-Version 7.0.6 kann getestet werden. Die Ergebnisse sind allerdings ernüchternd. Während der ursprüngliche Fehler nicht mehr auftaucht, funktionieren die Tags weiterhin nicht wie gewünscht. Der Case bei Fortinet ist geschlossen, da für den interims build kein Support verfügbar ist.

Unter Mac funktioniert die neue Version nicht, die Internetverbindung kann nicht hergestellt werden. Unter Windows und Linux besteht teilweise eine Verbindung, die nach undefinierbarer Zeit wieder abbricht. Die Endpoints werden vom EMS nicht korrekt an die FortiGate übertragen. Schlägt die Verbindung ins Internet via VPN fehl, kann der Daemon neu gestartet werden, resp. die Verbindung zum EMS neugestartet werden, damit es zeitweise funktioniert.

Nicht abgeschlossene Tasks

Task 778: "compliant" Tag mit unverschlüsseltem USB-Stick behalten:

Zu diesem Task wird ein Folgetask vorgeschlagen. Es soll ein Ticket bei einer Partnerfirma (Boll) erstellt werden, falls bereits ein Fix oder ein Workaround besteht. Mittels EMS kann keine zufriedenstellende Lösung gefunden werden. Supportticket bei Boll am 25.04.2022 erstellt.

Task 770: EMS AD Anbindung:

Zu diesem Task wird ein Folgetask vorgeschlagen. Die Anbindung ans AD kann nicht geprüft werden. Allerdings gibt es eine Referenzinstallation bei einem Kundensystem. Anhand dieser kann geprüft werden, ob die Anbindung ans AD funktioniert. Die Einstellungen sind einfach gehalten. Eine Testverbindung auf den Domain Controller der Firma kann aus technischen Gründen nicht hergestellt werden.

Anforderungen Product Owner

Der Product Owner erstellt einen neuen Task für den Epic «Installation und Konfiguration EMS 7.0»:

- Task 784: Endpoint Policies in EMS 7.0.3 erstellen und testen

Aktuell genutzte Versionen:

Software	Version
FortiClient auf Windows Testgerät	7.0.3
FortiClient auf Linux Testgerät	7.0.3
FortiClient auf macOS Testgerät	7.0.3
FortiOS auf Testfirewall FortiGate 500E	7.0.6 interim build
FortiClient EMS	7.0.3

Tabelle 72: Aktuell genutzte Versionen nach Sprint 2022/W17

4.7. Sprint 2022/W18

Im Sprintmeeting des letzten Sprints bestätigt der Product Owner seine Entscheidung, die produktive Umsetzung von EMS 7.0.3 in der Firma per sofort zu stoppen. Die Instabilität führt zu mehr Problemen als der Nutzen, der EMS bringt. Die durchführbaren Tasks sollen auf der Testumgebung beendet werden. Der Diplomand hat den Auftrag erhalten, neue Versionen von FortiClient EMS bei deren Release zu prüfen.

Der letzte Sprint beginnt am 25. April 2022 und endet am 29. April. Für den letzten Sprint verlangt der Product Owner folgende Tasks:

Name	Beschreibung	Startdatum	StoryPoints	Enddatum
Task 773	FortiClient Installer für Endpoint Profile zur Verfügung stellen (ITS, DEV und Office)	25.04.2022	4	27.04.2022
Task 777	Testen des Installers FortiClient 7.0.3 mit Firmeneinstellungen für Update	27.04.2022	2	28.04.2022
Task 770	EMS AD Anbindung	28.04.2022	1	29.04.2022
Task 778	«compliant» Tag mit unverschlüsseltem USB-Stick behalten	19.04.2022	1	-
Task 784	Endpoint Policies in EMS 7.0.3 erstellen und testen	28.04.2022	2	29.04.2022

Tabelle 73: Übersicht Sprint 2022/W18

4.7.1. Task 770: EMS AD Anbindung

Die Anbindung an ein Active Directory Server erlaubt es, sämtliche User und Endpoints in das EMS zu laden. Die Anbindung des EMS an das Active Directory kann in der Testumgebung nicht durchgeführt werden, da kein Server dazu bereitsteht. Bei der Umsetzung von EMS bei einem Kunden, ist die Anbindung ans Active Directory aber problemlos durchgelaufen

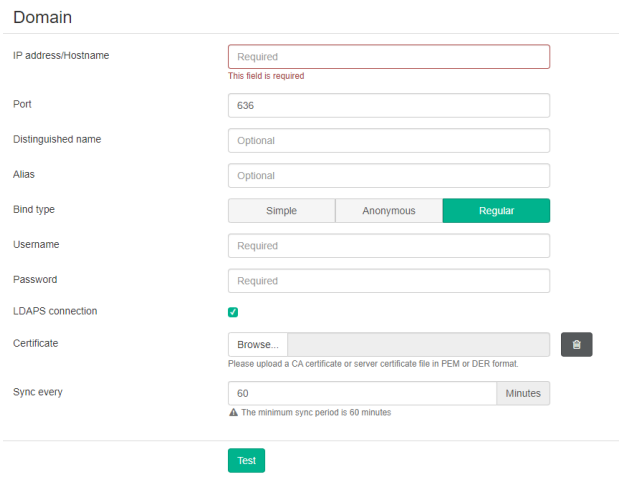


Abbildung 47: Anbindung EMS Übersicht

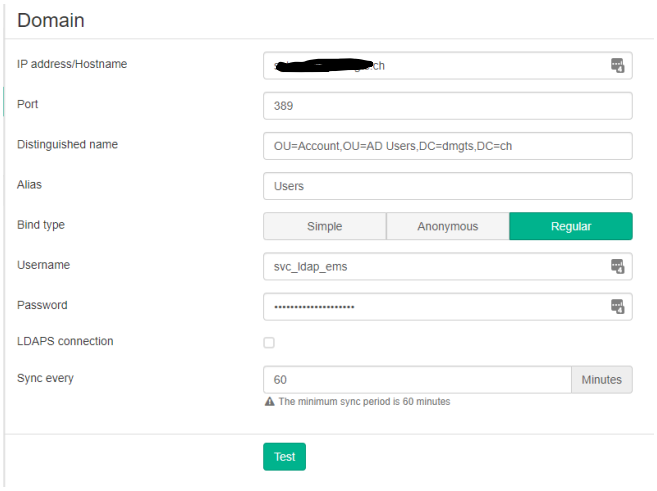


Abbildung 46: Anbindung EMS bei Kunde

Die Einstellungen auf dem Produktiven Server sind einfach. Nach dem Test kann der Server angebunden werden und alle User werden in den EMS geladen und alle 60 Minuten mit dem Active Directory synchronisiert.

Unter «Domains» werden die definierten Ordner vom AD alle 60 Minuten synchronisiert. Die Workgroups sind nur im EMS ersichtlich und werden dazu gebraucht, um die Clients innerhalb der Firma zu unterscheiden und gruppieren. In diesem Fall nach Abteilungen. Auf diese Workgroups werden die Policies und somit die Endpoint Profile angewandt.

Die Geräte können manuell oder mittels Group Assignment Rules in die Workgroups verschoben. Die Endpoint Profile werden mittels Policies angwendet.

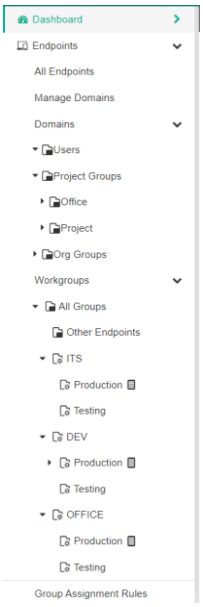


Abbildung 48: Workgroups in EMS

Aus dem AD werden lediglich die User synchronisiert. Die Geräte werden durch den FortiClient in den EMS geladen.

Domain Name	Devices	Users	Last Sync	Sync Every	Address
Users	0	178	2022-04-26 09:30:09	60 minutes	[redacted]
Project Groups	0	0	2022-04-26 09:31:09	60 minutes	[redacted]
Org Groups	0	0	2022-04-26 09:29:09	60 minutes	[redacted]

Abbildung 49: Synchronisierte User aus AD

4.7.2. Task 784: Endpoint Policies in EMS 7.0.3 erstellen und testen

Die erstellen Endpoint Profile lassen sich dynamisch in der Endpoint Policy anweden. Die Policies lassen sich auch die definierten Gruppen der Workgroups anwenden.

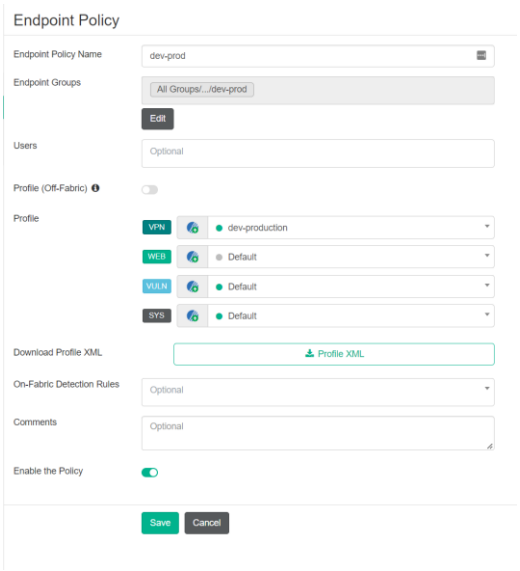


Abbildung 50: Endpoint Policy "dev-prod"

Für die verschiedenen Abteilungen ITS, DEV und Office wird jeweils eine Policy mit den zugehörigen Profilen erstellt. Sind die Endpoints in der richtigen Workgroup werden die definierten Profile angewandt.

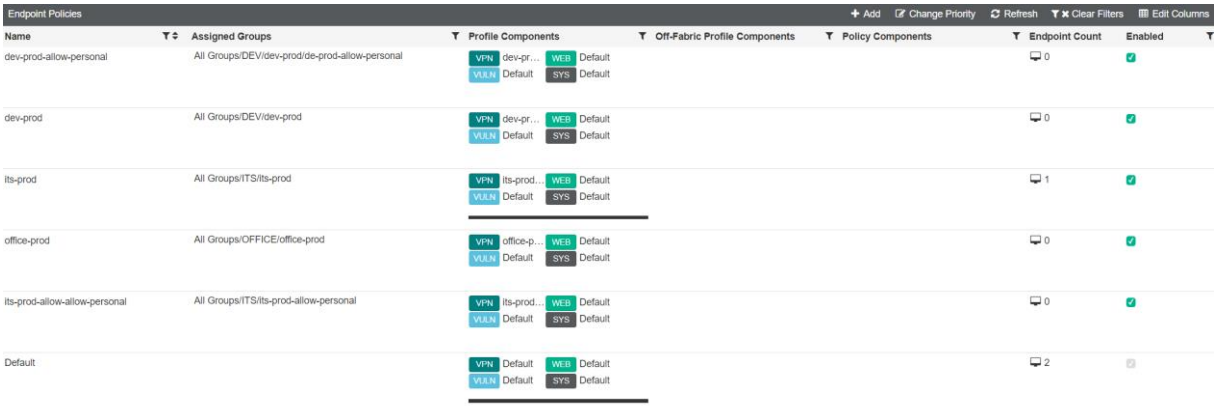


Abbildung 51: Übersicht der Endpoint Policies

Um Clients in die richtigen Workgroups zu verschieben, werden Custom Installer erstellt. Die Installer werden so angepasst, dass ein Client nach der Installation in eine definierte Gruppe verschoben wird. Ist der Client in der Gruppe, wird die entsprechende Policy und das Endpoint Profil angewendet.

4.7.3. Task 773: FortiClient Installer für Endpoint Profile zur Verfügung stellen (ITS, DEV und Office

Via FortiClient EMS können Custom Installer erstellt werden. Damit ein Custom Installer erstellt werden kann, muss zuerst die gewünschte Version auf den EMS hochgeladen werden. Die gewünschte Version ist 7.0.3, welche auf der Downloadseite von Fortinet zum Download bereitsteht. Zusätzlich wird die Version 6.4.7 heruntergeladen, um später diverse Tests durchzuführen.

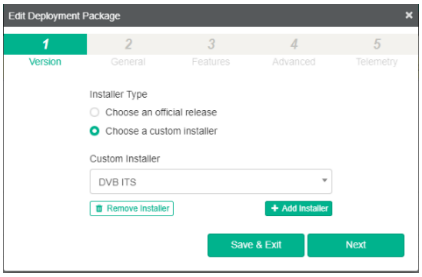


Abbildung 52: Custom Installer, Version wählen

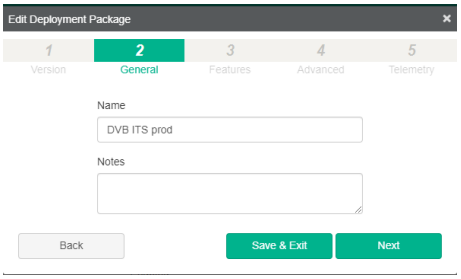


Abbildung 53: Custom Installer, generelle Informationen

Der wichtigste Punkt bei der Bearbeitung des Installers sind die Features. Werden einige Features nicht angewählt, muss sichergestellt sein, dass diese in naher Zukunft nicht benutzt werden. Nicht installierte Features können via Policy nicht auf den Client appliziert werden und aus diesem Grund nicht benutzt werden. Die Devise ist also: Lieber zu viele Features aktivieren, die man ausblenden kann, als zu wenig Features. Installiert man z.B. den Webfilter nicht und möchte in einem späteren Schritt den Webfilter Off-Fabric (Ausserhalb des internen Netzes) anwenden, müsste man einen neuen Installer erstellen und ausrollen.

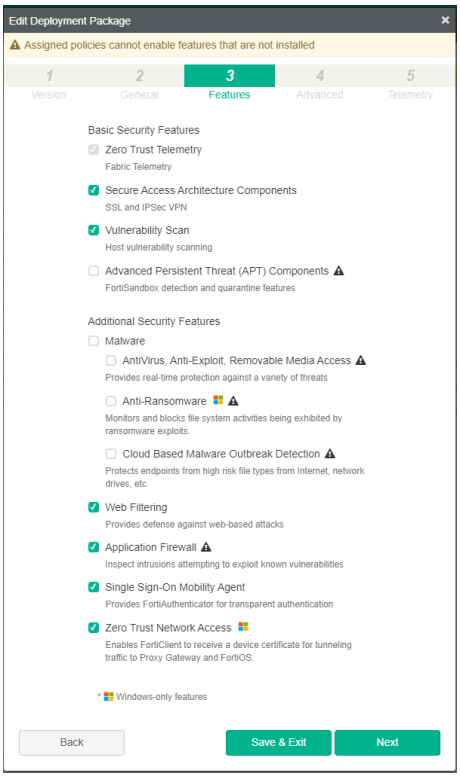


Abbildung 54: Custom Installer, Features auswählen

Der nächste Punkt sind die Advanced Einstellungen des Clients:

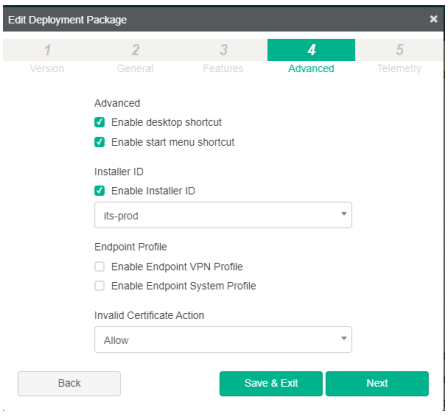


Abbildung 55: Custom Installer, Advanced Einstellungen

Die definierten Endpoint Profile lassen sich bereits im Custom Installer anwenden. Es ist allerdings möglich, dass ein User zu einem späteren Zeitpunkt ein anderes Profil braucht. Dies lässt sich dann nicht mehr applizieren und eine Neuinstallation mit dem richtigen Installer ist notwendig.

Durch das Erstellen einer Installer ID, können Group Assignment Rules die hinzugefügten Clients in die richtigen Ordner verschieben. Es ist auch möglich für alle Untergruppen ebenfalls einen Installer bereitzustellen. Da dies eigentlich nur wenige Personen betrifft, könnten diese auch manuell in die Untergruppen verschoben werden. Wird aber eine Installer ID auf eine Gruppe «dev» mit der Untergruppe «dev-allow-personal» angewandt und ein Client verschoben, führt dies zu Problemen. Denn sobald die Group Assignment Rule automatisch angewandt wird, wird der Client wieder zurück

in die Hauptgruppe verschoben und die Policy angepasst. Deshalb empfiehlt es sich die Workgroups so zu gestalten, dass keine Konflikte entstehen.

Die wenigen Personen, die ein zusätzliches VPN benötigen können von Hand in die Gruppe verschoben werden.

4.7.4. Task 777: Testen des Installers FortiClient 7.0.3 mit Firmeneinstellungen für Update

Übersicht Testfälle

Nr.	Test	Resultat
#1	Custom Installer über bestehende Installation mit EMS Verbindung	Nicht zu empfehlen, theoretisch machbar
#2	Installation von Custom Installer ohne vorherige Installation	Funktioniert wie gewünscht
#3	Installer von 6.4.7 auf 7.0.3 ohne Neustart	Theoretisch machbar, neuer Bug entdeckt
#4	Custom Installer «office» testen:	Funktioniert wie gewünscht
#5	Custom Installer «dev» testen	Funktioniert wie gewünscht
#6	Upgrade Custom Installer von 6.4.7 auf 7.0.3	Theoretisch machbar gleicher Bug wie bei Test#3
#7	Verschieben Clients von «dev» nach «dev-allow-personal»	Änderungen werden angewandt, Group Assignment Rule verschiebt den Client wieder zurück

Testfall #1: Custom Installer über bestehende Installation installieren, die bereits mit EMS verbunden ist

- Group Assignment funktioniert nicht
- Verbindung zu EMS bleibt bestehen
- VPN Verbindung wird nicht angepasst
- Client wird nicht in Workgroup verschoben
- Custom Installer können nur durch Systemadministratoren deinstalliert werden

Testfall #2: Installation von Custom Installer ohne vorherige Installation

- Registriert sich automatisch an EMS
- Bezieht Lizenz wie gewünscht
- Wird in richtige Gruppe verschoben
- Group Assignment Rule funktioniert

Testfall #3: Installer von 6.4.7 auf 7.0.3 ohne Neustart

- Upgrade ohne Neustart möglich
- Verbindung zu EMS bleibt bestehen
- Neuer Bug: RemoteZugriff wechselt automatisch auf Haupttab innert 1.5 Sekunden
- Eingabe VPN Angaben nicht möglich

Testfall #4: Custom Installer «office» testen:

- Installation via HighSystem möglich
- Installation «office» erfolgreich
- VPN Verbindung korrekt
- Gruppenzuordnung korrekt

Testfall #5: Custom Installer «dev» testen

- Installation via HighSystem möglich
- Installation «dev» erfolgreich
- VPN Verbindung korrekt
- Gruppenzuordnung korrekt

Testfall #6: Upgrade Custom Installer von 6.4.7 auf 7.0.3

- EMS verbunden
- Upgrade auf 7.0.3 ohne automatischen Neustart
- Bug: RemoteZugriff wechselt automatisch auf Haupttab innert 1.5 Sekunden
- Über Taskleiste auch keine Verbindung möglich
- VPN vor Login funktioniert, meldet korrekt an

Testfall #7: Verschieben Clients von «dev» nach «dev-allow-personal»

- Verschieben funktioniert problemlos
- RemoteZugriff wird geändert
- Neue VPN Verbindung kann hinzugefügt werden
- Group Assignment Rule verschiebt den Client wieder nach «dev»

Der Client wird beim Scheduled Run der Group Assignment Rules wieder in die Ursprungsgruppe verschoben. Die Rules können aber ausgeschaltet werden, somit müssten künftige Neueintritte manuell im EMS in die Untergruppe verschoben werden.

4.7.5. Task 778: «compliant» Tag mit unverschlüsseltem USB-Stick behalten

Der Diplomand hat sämtliche Logfiles des FortiClient, FortiClient EMS und der FortiGate zur Untersuchung zur Verfügung gestellt.

Das Ticket beim Vertreter von Fortinet liefert leider keine Lösung zu diesem Problem. Laut Herstellersupport sei das Verhalten, dass beim Anschliessen eines unverschlüsselten USB Sticks der Bitlocker Tag verloren geht, ein zu erwartendes Verhalten.

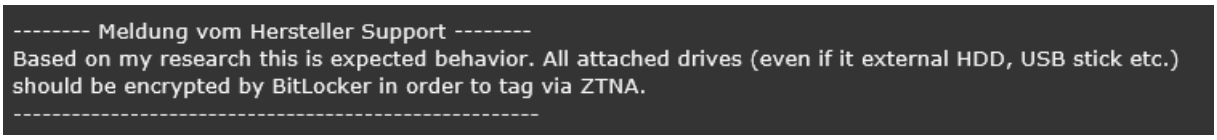


Abbildung 56: Ausschnitt der Meldung des Herstellersupports

4.8. Review Sprint 2022/18

Das Sprint Review bezeichnet das Ende eines Sprints. Abgeschlossen wird der Sprint am 2. Mai 2022. Die verbleibenden Tasks, die nicht angegangen werden können, werden in das Product Backlog verschoben.

Name	Beschreibung	Erledigt	Grund
Task 773	FortiClient Installer für Endpoint Profile zur Verfügung stellen (ITS, DEV und Office)	ja	
Task 777	Testen des Installers FortiClient 7.0.3 mit Firmeneinstellungen für Update	Ja	
Task 770	EMS AD Anbindung	Ja	
Task 784	Endpoint Policies in EMS 7.0.3 erstellen und testen	Ja	
Task 778	«compliant» Tag mit unverschlüsseltem USB-Stick behalten	Ja	

Gespräch mit Product Owner am Freitag, 29. April 2022:

Die gewünschten Tasks können auf der Testumgebung abgeschlossen werden. Die Umsetzung für die produktive Nutzung von EMS ist derzeit aufgeschoben, bis die Probleme seitens Fortinet beseitigt werden.

Abgeschlossene Tasks

Task 773: FortiClient Installer für Endpoint Profile zur Verfügung stellen (ITS, DEV und Office)

Die Installer können im GUI des EMS erstellt werden. Es wird pro Bereich innerhalb der Firma ein Installer für ITS, DEV und Office erstellt. Die Erstellung ergibt keine weiteren Probleme.

Task 777: Testen des Installers FortiClient 7.0.3 mit Firmeneinstellungen für Update

Die Installer funktionieren bei einem Clean-Install. Wird aber ein bestehender FortiClient von 6.4.7 mit dem neuen Installer direkt aktualisiert, gibt es einen neuen Bug. Das VPN lässt sich nicht mehr verbinden, auch wenn EMS verbunden ist.

Die Installer werden einer Installer-ID zugewiesen, welche wiederum für die Group Assignment Rules verwendet werden können. Ein weiteres Problem stellen diese Rules dar. Werden diese ausgeführt verschieben sich die Endpoints wieder in die Gruppe, die der Installer ID zugeordnet ist.

Task 770: EMS AD Anbindung

Dieser Task kann auch diese Woche nicht abschliessend gelöst werden. Die Produktive Umgebung des Kunden kann analysiert werden, die Anbindung von EMS an das Active Directory wird keine Probleme bereiten. Dem Product Owner reicht diese Antwort, damit der Task als erfüllt gilt.

Task 784: Endpoint Policies in EMS 7.0.3 erstellen und testen

Die erstellen Policies können auf die Endpoint Groups angewendet werden. Die zuvor definierten Profile können ausgewählt und erfolgreich angewandt werden.

Task 778: «compliant» Tag mit unverschlüsseltem USB-Stick behalten

Die Kommunikation mit Boll stellt sich als aufwendig heraus. Sie sind sehr freundlich und hilfsbereit, verlangen aber meist die Situation 2-3 erklärt inkl. Logfiles des EMS, des FortiClients und der FortiGate. Boll als Vertriebspartner nimmt Kontakt zum Hersteller Fortinet auf und erläutert unsere Situation. Die Antwort ist, dass das gezeigte Verhalten mit dem Verlieren des Tags beabsichtigt sei. Es können bei einer Implementation also nur noch Bitlocker verschlüsselte USB-Sticks verwendet werden.

Anforderungen Product Owner

Alle Tasks, die nicht abgeschlossen werden können sollen ins Product Backlog verschoben werden. Probleme und Bugs sollen dokumentiert werden und bei neuen Releases soll der Diplomand prüfen, ob diese behoben sind.

Aktuell genutzte Versionen:

Software	Version
FortiClient auf Windows Testgerät	7.0.3
FortiClient auf Linux Testgerät	7.0.3
FortiClient auf macOS Testgerät	7.0.3
FortiOS auf Testfirewall FortiGate 500E	7.0.6 interim build
FortiClient EMS	7.0.3

Tabelle 74: Aktuell genutzte Versionen nach Sprint 2022/W18

5. Offene, nicht abschliessbare Tasks im Product Backlog, Epic «Installation und Konfiguration EMS 7.0»

Im Product Backlog bestehen weiterhin Tasks, die nicht erledigt werden können. Die offenen oder blockierten Tasks werden hier nochmals zur Übersicht erwähnt.

Task	Status	Grund
Task 771: Firewall Policies mit ZTNA Tags	Blockiert	Verbindung zwischen FortiGate und EMS instabil, diverse Bugs
Task 776: Dokumentation für Präsentation an Show and Tell	Blockiert	Die Firmeninterne Präsentation des EMS kann derzeit nicht durchgeführt werden
Task 775: Konfiguration EMS Produktion abschliessen	Blockiert	Der Product Owner hat die produktive Inbetriebnahme aufgrund Instabilität der Lösung gestoppt
Task 774: FortiGate Update auf 7.0.5	Blockiert	Produktives Firewall-Update auf 7.0.5 aufgrund Bugs nicht als Task in einem Sprint definiert
Task 778: «compliant» Tag mit unverschlüsseltem USB Stick behalten	Blockiert, ungelöst	Laut Herstellersupport ist dies «zu erwartendes Verhalten».

Abbildung 57: Product Backlog nach Sprints

Weiteres Vorgehen gemäss Product Owner

Es ist nicht möglich, die Installation Produktiv zu stellen. Sämtliche Analysen und Vorbereitungen sind auf der Testumgebung getroffen und eingerichtet. Die Testinstallation von EMS 7.0.3 bleibt bestehen und sobald eine Lösung für die Bugs besteht und der EMS funktionsfähig ist, wird EMS auch produktiv eingesetzt.

Task 774: FortiGate Update auf 7.0.5:

Das Update kann aufgrund eines Bugs nicht durchgeführt werden. Der Bug ist bei Fortinet dokumentiert, weshalb dieser Task in keinem Sprint ersichtlich ist.

BUG ID 783112 - FortiGate goes into conserve caused due to high memory usage of WAD user-info process

783112	FortiGate goes into conserve mode due to high memory usage of WAD `user-info` process. The WAD `user-info` process will query the user count information from the LDAP server every 24 hours. If any of the LDAP query messages are closed by exceptions, there is a memory leak. If `obtain-user-info` is enabled under `config user ldap`, this memory leak will be triggered on daily basis. **Workaround**: create an automation stitch to restart the WAD daemon every day to avoid conserve mode.

Task 776: Dokumentation für Präsentation an Show and Tell

Das Show and Tell ist innerhalb der Firma vergleichbar mit einer Produktvorstellung. Der EMS sollte vorgestellt, dokumentiert und vorgeführt werden. Die technischen Probleme verhindern diesen Task.

Task 775: Konfiguration EMS Produktion abschliessen

Das Abschliessen der produktiven Umgebung wird durch diverse Probleme verhindert. Die Endpoints werden nicht wie beschrieben in die synchronisierten ZTNA Tags der FortiGate geladen. Während der Verbindung im VPN besteht kein Internetzugriff. Die Websocket Verbindung muss jeweils neu initialisiert werden, damit der Endpoint angezeigt wird und die Policy sauber appliziert wird. Unter FortiOS 7.0.6 hat das MacBook nie mehr Internetzugriff im VPN erhalten.

Die Verbindung zwischen EMS und FortiGate ist weiterhin nicht konstant. Nach einer unbestimmten Zeit gehen die Endpoints in der FortiGate verloren.

5.1. Product Backlog, Epic «Installation und Konfiguration EMS 7.0»

Task Nr.	Beschrieb	Status
759	EMS Testinstallation von Version 6.4.7 auf 7.0.3 aktualisieren	Fertig
760	Testen des Updates von FortiClient 6.4.7 auf Version 7.0.3 unter Windows 10	Fertig
761	Testen des Updates von FortiClient 6.4.7 auf Version 7.0.3 unter Linux Ubuntu 20	Fertig
762	Testen des Updates von FortiClient 6.4.7 auf Version 7.0.3 unter macOS 12.3.1 Monterey	Fertig
763	ZTNA Tags auf ihre Funktionalität hin überprüfen	Fertig
764	VPN Verbindungsparameter für Firma festlegen	Fertig
765	Client-Rollout: Ablauf mit Client Management besprechen	Fertig
766	Mögliche ZTNA Tags definieren	Fertig
767	Evaluation ZTNA Tags Feature	Fertig
768	Evaluation Endpoint Profiles	Fertig
769	Endpoint Profiles für Clients definieren	Fertig
770	EMS AD Anbindung	Fertig
771	Firewall Policies mit ZTNA Tags	BLOCKED
772	VPN vor Login unter Windows / Linux / Mac einrichten und testen	Fertig
773	FortiClient Installer für Endpoint Profile zur Verfügung stellen (ITS, DEV und Office)	Fertig
774	FortiGate Update auf 7.0.5	BLOCKED
775	Konfiguration EMS Produktion abschliessen	BLOCKED
776	Dokumentation für Präsentation am Show and Tell	BLOCKED
777	Testen des Installers FortiClient 7.0.3 mit Firmensettings für Update	Fertig
778	"compliant" Tag mit unverschlüsseltem USB-Stick behalten	BLOCKED
779	Support-Case bei Fortinet erstellen/bearbeiten	Fertig
784	Endpoint Policies in EMS 7.0.3 erstellen und testen	Fertig

Abbildung 58: Product Backlog, Epic "Installation und Konfiguration EMS 7.0" nach Sprints

6. Ziel- und Anforderungserfüllung

Um zu definieren, ob das Projekt erfolgreich ist, müssen die Ziele und Anforderungen auf deren Erfüllung geprüft werden. Dazu werden zuerst die Ziele auf ihre Erfüllung geprüft, da diese aus den Anforderungen der entstanden sind. Im zweiten Schritt werden die Anforderungen auf ihre Erfüllung geprüft.

6.1. Übersicht Ziele

Nr.	Ziel	Priorität	Erfüllt
1	Ein Windows-Firmengerät kann von einem «Standard-Gerät» unterschieden werden	MUSS	Ja
2	Die Lösung erkennt ein Firmengerät anhand definierter Eigenschaften	MUSS	Ja
3	Die Lösung erkennt innerhalb von 1 Minute, wenn ein Firmengerät nicht mehr den Anforderungen entspricht	MUSS	Ja
4	Ist ein Firmengerät nicht mehr unternehmenskonform wird das Gerät innert 10 Sekunden nach Erkennung vom Netzwerk isoliert	MUSS	Ja
5	Ist ein Gerät nicht autorisiert wird eine entsprechende Meldung ausgegeben	KANN	Jein
6	Die Lösung kann anhand des Firmengerätes bestimmen welches Operating System (OS) auf dem Gerät läuft und kann dies kennzeichnen	KANN	Ja
7	Die Testumgebung ist am 4. April einsatzbereit	MUSS	Ja
8	Das Windows-Testgerät entspricht dem Standard-Setup der Firma und ist aktualisiert	SOLL	Ja
9	Das Linux-Testgerät entspricht dem Standard-Setup der Firma und ist aktualisiert	SOLL	Ja
10	Das macOS-Testgerät läuft unter der aktuellen macOS Version 12, Monterey	SOLL	Ja
11	Das Testen ist bis am 30 April vollumfänglich abgeschlossen und Fehler sind bekannt und in Bearbeitung oder behoben	MUSS	Ja
12	Der Einsatz der Lösung soll bis am 13. Mai erfolgen	SOLL	Nein
13	Ein nicht konformes Gerät hat zu keinem Zeitpunkt Zugriff auf sensible Daten, wenn es per VPN verbunden ist	MUSS	Ja
14	VPN-Verbindung wird innert 20 Sekunden erfolgreich aufgebaut	MUSS	Ja
15	Windows-Benutzer:innen können sich mit VPN vor Login anmelden	SOLL	Ja
16	Die Kosten für das Projekt belaufen sich jährlich unter 5'000 CHF	SOLL	Ja
17	Bei einer Verbindung mit VPN hat ein konformes Gerät immer Zugriff auf entsprechende Ressourcen	SOLL	Nein

Tabelle 75: Übersicht Zielerreichung

6.1.1. Erfüllte Ziele

Die folgenden Ziele konnten erarbeitet werden und sind erfüllt:

Ziel #1, MUSS: Ein Windows-Firmengerät kann von einem «Standard-Gerät» unterschieden werden

- Mithilfe des Tags «windows» zur Erkennung des OS können die Geräte unterschieden werden. EMS erkennt die Geräte in der Übersicht der Endpoints ebenfalls.

Ziel #2, MUSS: Die Lösung erkennt ein Firmengerät anhand definierter Eigenschaften

- Dieses Ziel kann mittels «compliant» Tag erfüllt werden. Der Tag funktioniert einwandfrei.

Ziel #3, MUSS: Die Lösung erkennt innerhalb von 1 Minute, wenn ein Firmengerät nicht mehr den Anforderungen entspricht

- Der FortiClient auf den Endpoints sendet seine Informationen alle 60 Sekunden zum EMS. Ist ein Gerät nicht mehr «compliant» sendet er diese zuverlässig.

Ziel #4, MUSS: Ist ein Firmengerät nicht mehr unternehmenskonform wird das Gerät innert 10 Sekunden nach Erkennung vom Netzwerk isoliert

- Erhält der EMS die Information, dass ein Endpoint nicht mehr konform ist, erhält er den Tag nicht mehr und hat innert 10 Sekunden keinen Internetzugriff mehr.

Ziel #6, KANN: Die Lösung kann anhand des Firmengerätes bestimmen welches Operating System (OS) auf dem Gerät läuft und kann dies kennzeichnen

- Der EMS kann die Geräte, die verbunden sind, unterscheiden und zeigt dies visuell an.

Ziel #7, MUSS: Die Testumgebung ist am 4. April einsatzbereit

- Die Testumgebung steht am 4. April zur Verfügung und ist eingerichtet.

Ziel 8#, SOLL: Das Windows-Testgerät entspricht dem Standard-Setup der Firma und ist aktualisiert

- Gemäss Firmenstandard konfiguriert und während des Projekts aktuell gehalten

Ziel #9, SOLL: Das Linux-Testgerät entspricht dem Standard-Setup der Firma und ist aktualisiert

- Gemäss Firmenstandard konfiguriert und während des Projekts aktuell gehalten

Ziel #10, SOLL: Das macOS-Testgerät läuft unter der aktuellen macOS Version 12, Monterey

- MacBook auf Version 12 Monterey aktualisiert und eingerichtet

Ziel #11: Das Testen ist bis am 30 April vollumfänglich abgeschlossen und Fehler sind bekannt und in Bearbeitung oder behoben

- Die Tests sind vor dem 30. April abgeschlossen und die meisten Fehler können identifiziert werden. Probleme sind leider noch offen.

Ziel #13, MUSS: Ein nicht konformes Gerät hat zu keinem Zeitpunkt Zugriff auf sensible Daten, wenn es per VPN verbunden ist

- Endpoints ohne den «compliant» Tag haben keinen Zugriff auf das interne Netzwerk.

Ziel #14, MUSS: VPN-Verbindung wird innert 20 Sekunden erfolgreich aufgebaut

- Die Verbindung an der Testumgebung wird innerhalb 20 Sekunden aufgebaut. Mit Multifaktor wird dies aufgrund Benutzereingabe etwas länger dauern.

Ziel #15, MUSS: Windows-Benutzer:innen können sich mit VPN vor Login anmelden

- Die Benutzer können sich weiterhin am VPN anmelden und arbeiten. In der Testumgebung funktioniert dies nur bedingt.

Ziel #16, MUSS: Die Kosten für das Projekt belaufen sich jährlich unter 5'000 CHF

- Die Kosten für die Lizenzierung, sind unter 5000 CHF. Die Wartung, Aktualisierung und die Serverkosten werden intern nicht verrechnet.

6.1.2. Nicht erfüllte Ziele

Die folgenden Ziele konnten nicht, oder nur teilweise erfüllt werden:

Ziel #12, SOLL: Der Einsatz der Lösung soll bis am 13. Mai erfolgen

- Die Umsetzung ist gestoppt und kann deshalb nicht erfolgen. Die Lizenzen sind beschafft und die Umsetzung erfolgt sobald die Lösung keine Bugs mehr aufweist.

Ziel #17, SOLL: Bei einer Verbindung mit VPN hat ein konformes Gerät immer Zugriff auf entsprechende Ressourcen

- Aufgrund der Bugs kann der Zugriff auf das Internet nicht gewährleistet werden. Die VPN-Verbindung bleibt bestehen, die Internetverbindung allerdings nicht.

Spezialfall Ziel #5, KANN: Ist ein Gerät nicht autorisiert wird eine entsprechende Meldung ausgegeben

- Dieses Ziel kann erreicht werden, funktioniert aber nur unter Windows-Geräten. Es ist teilweise erfüllt.

6.2. Übersicht Anforderungen

Nach der Zielerfüllung, sollen nun die Anforderungen überprüft werden. Die meisten Anforderungen konnten umgesetzt werden.

Req. Nr.	Anforderung	Erfüllt
Req1	Definieren, was ein Firmengerät zu einem Firmengerät macht	Ja
Req2	Definition von Anforderungen an Clients, die es zu erfüllen gilt	Ja
Req3	Überwachung der Zugriffe auf das interne Netzwerk	Ja
Req4	Zugriff über VPN nur von Firmengeräten erlauben	Ja
Req5	Isolieren von Geräten, die nicht von der Firma stammen und sich via VPN zu verbinden versuchen	Ja
Req6	Erkennen von Firmengeräten, die sich via VPN verbinden	Ja
Req7	Isolation von Firmengeräten, die die definierten Anforderungen nicht vollständig erfüllen	Ja
Req8	VPN vor Login bei Windows Geräten einrichten	Ja
Req9	Hohe Stabilität der VPN-Verbindung, keine Timeouts	Ja
Req10	VPN-Verfügbarkeit jederzeit und von überall möglich	Ja
Req11	Keine Einschränkungen der Zugriffe während der VPN-Verbindung	Nein
Req12	Möglichst identischer Ablauf zum Herstellen einer Verbindung	Ja
Req13	Verknüpfungen auf Desktop und Icons der Lösung sollen gleich sein	Ja
Req14	Der Mehrwert für die Firma übersteigt die Kosten der Lösung	Nein
Req15	Die Lösung ist durch das Client Management der Firma verwaltbar	Ja
Req16	Die Lösung wird laufend aktualisiert	Ja

Tabelle 76: Übersicht der erfüllten Anforderungen

6.2.1. Erfüllte Anforderungen

Req1: Definieren, was ein Firmengerät zu einem Firmengerät macht

- Die Definition eines Firmengerätes ist erfolgreich durchgeführt. Dazu wird der Tag «compliant» genutzt. Die Definition befindet sich oben im Anhang.

Req2: Definition von Anforderungen an Clients, die es zu erfüllen gilt

- Die Anforderungen an ein Gerät können nicht gemäss der Definition eines Firmengeräts übernommen werden. Der FortiClient erkennt unter MacOS und Linux die Anti Virus Software nicht. Dennoch können Anforderungen an alle Geräte gestellt werden.

Req3: Überwachung der Zugriffe auf das interne Netzwerk

- Der Zugriff kann über die FortiGate verfolgt werden. Ist ein Gerät verbunden, wird die IP angezeigt und kann anhand dieser im EMS einem Gerät zugewiesen werden.

Req4: Zugriff über VPN nur von Firmengeräten erlauben

- Die Funktionalität der Tags zwischen EMS und dem FortiClient auf den Endpoints hat zuverlässig funktioniert. Der Zugriff aufs VPN hat immer funktioniert.

Req5: Isolieren von Geräten, die nicht von der Firma stammen und sich via VPN zu verbinden versuchen

- Geräte mit einem FortiClient, ohne Verbindung zum EMS, können zu keiner Zeit eine Verbindung aufbauen.

Req6: Erkennen von Firmengeräten, die sich via VPN verbinden

- Anhang der Tags können die Firmengeräte erfolgreich identifiziert werden.

Req7: Isolation von Firmengeräten, die die definierten Anforderungen nicht vollständig erfüllen

- Sind die Regeln der Tags nicht erfüllt, wird das Gerät vom Netzwerk isoliert.

Req8: VPN vor Login bei Windows Geräten einrichten

- Das VPN vor Login kann bei Windows Geräten gemacht werden.

Req9: Hohe Stabilität der VPN-Verbindung, keine Timeouts

- Die VPN-Verbindung selbst ist stabil und funktioniert zuverlässig.

Req10: VPN-Verfügbarkeit jederzeit und von überall möglich

- Das VPN kann von einem Hotspot, Heimnetzwerk oder Starbucks verbunden werden.

Req12: Möglichst identischer Ablauf zum Herstellen einer Verbindung

- Der Ablauf hat sich nicht geändert, der FortiClient mit der VPN-Verbindung wird identisch zu früheren Versionen gestartet.

Req13: Verknüpfungen auf Desktop und Icons der Lösung sollen gleich sein

- Die Verknüpfungen können bereits im Installer des «Custom Installer» eingerichtet werden.

Req15: Die Lösung ist durch das Client Management der Firma verwaltbar

- Die generierten Installer können dem Client Management mit entsprechender Info zur Verfügung gestellt werden.

Req16: Die Lösung wird laufend aktualisiert

- Da die Lösung derzeit nicht produktiv im Einsatz ist, muss sie zwingend aktualisiert werden sobald Updates vorhanden sind.

6.2.2. Nicht erfüllte Anforderungen

Req11: Keine Einschränkungen der Zugriffe während der VPN-Verbindung

- Die Internetverbindung kann weiterhin nicht stabil aufrechterhalten werden.

Req14: Der Mehrwert für die Firma übersteigt die Kosten der Lösung

- Derzeit kann dies leider nicht erfüllt werden. Wenn der EMS produktiv geht und alle Probleme beseitigt wurden, wird der Mehrwert gegeben sein.

7. Reflexion

Der Start der Arbeit verlief optimal. Die gesamte Testumgebung mit der Firewall, den Lizenzen, den drei Notebooks war einsatzbereit. Der erste Sprint verlief ohne grosse Zwischenfälle. Die Lösung erschien bereits greifbar.

Im zweiten Sprint folgten dann aber Rückschlag auf Rückschlag. Die Grundfunktionen der Lösung funktionierte nicht wie beschrieben. Tags wurden nicht mit der Firewall synchronisiert, die Verbindung ins Internet funktionierte nicht, die Geräte waren in der Firewall nur kurz ersichtlich und verschwanden dann wieder. Die Kommunikation zwischen EMS und FortiGate brach in zufälligem Muster zusammen. Frustrierend zu Beginn der Probleme war, dass nicht mit Sicherheit die FortiGate oder der EMS als Problemquelle adressiert werden konnte. So wurde die Firewall neu konfiguriert, auf verschiedenste höhere und tiefere Versionen zusammen mit EMS konfiguriert. Der EMS wurde zwei Mal komplett neu installiert und das Debugging in der Firewall führte zu keinen brauchbaren Lösungen.

Mit der Version 7.0.6 im dritten Sprint keimte nochmals Hoffnung auf, was das Problem an der Firewall Policy anbelangt. Eine Fehlermeldung, die bei der Adressierung der ZTNA Policy auftrat, konnte behoben werden. Die generellen Probleme mit dem Websocket, den fehlenden Endpoints in der FortiGate blieben aber unverändert. Das MacBook konnte überhaupt keine Verbindung mehr ins Internet herstellen.

Vor dem vierten Sprint wurde das Projekt durch den Product Owner gestoppt. Die Tasks, die innerhalb der Testumgebung umgesetzt und getestet werden können, sollen im vierten Sprint erledigt werden.

Die Dokumentation eines agilen Projekts gestaltet sich als äusserst aufwendig. Die grösste Herausforderung war, den roten Faden nicht aus den Augen zu verlieren.

7.1. Ausblick EMS

Fortinet wird im Mai 2022 ein Release für den FortiClient EMS 7.0.4 veröffentlichen. Gemäss dem Product Owner soll mit diesem Release weiter getestet werden.

Die wichtigsten Punkte, die erfüllt werden müssen, damit EMS produktiv genutzt werden kann:

- Websocket zwischen EMS und FortiGate stabil
- ZTNA Tags in der Firewall nutzbar
- Verbindung ins Internet während VPN Verbindung bleibt bestehen

7.2. Weiterführende Möglichkeiten mit EMS

Der EMS bietet eine breite Funktionspalette nebst den Zero Trust Tags an. Während Endpoints verwaltet und markiert werden können, kann ein firmeneigener Installer generiert werden, der sich direkt mit dem FortiClient EMS verbindet.

Eine weitere Möglichkeit ist ein ZTNA Access Proxy. Mit dieser Lösung fällt das SSL-VPN weg und Endpoints verbinden sich via HTTPS mit dem Access Proxy. Dieser wiederum prüft die Identität des Gerätes, des Users und der Tags, die der Endpoint mitliefert. Sind diese Informationen korrekt, leitet er diese an den EMS weiter. Diese Lösung ist in der Zieldefinition nicht aufgeführt, da sie das SSL-VPN ersetzen würde.

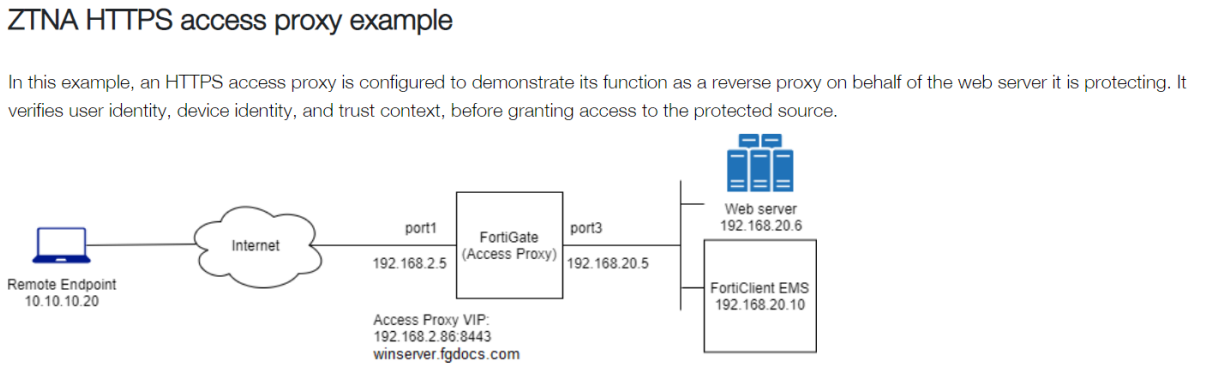


Abbildung 59: ZTNA HTTPS access proxy Beispiel

7.3. Lessons learned

Das Projekt war äusserst lehrreich, da ich bisher keine Erfahrungen mit SCRUM hatte. Die Idee von SCRUM ist äusserst gewinnbringend und ich würde dies gern in Zukunft weiter einsetzen. Dabei werde ich aber folgende Punkte berücksichtigen:

- Bei agilen Projekten, insbesondere SCRUM, genügend StoryPoints einplanen, damit auch unvorhergesehenes einigermassen abgefedert werden kann.
- Beim Auftreten von Problemen, sofort die zuständige Stelle informieren, damit entsprechend gehandelt werden kann und nicht erst versuchen das Problem im Stillen zu lösen
- Bei Sprintplanung auch mal sagen, wenn etwas zu optimistisch eingeschätzt wurde

Bei der Arbeit mit EMS oder allgemein Fortinet, sind auch einige Dinge hängen geblieben:

- Bevor irgendetwas aktualisiert wird, die Known Issues konsultieren und abgleichen mit der installierten Version
- Wann immer möglich, ein Update oder eine Aktualisierung vorgängig in einer Testumgebung testen
- Positive Grundeinstellung behalten, aber auf alles gefasst sein

Bei der Erstellung der Diplomarbeit sind auch noch ein, zwei Punkte aufgetaucht:

- Ein agiles Projekt zu dokumentieren ist für die Verständlichkeit äusserst aufwendig
- Der Rote Faden durch das Dokument zu ziehen ist anspruchsvoll

8. Anhang A

8.1. Anhang A1, SCRUM Grundlagen

Scrum kommt aus der Softwareentwicklung und wird für Teamarbeiten genutzt. Es arbeiten mehrere Personen zeitgleich an einem Projekt, um am Ende ein Produkt zu erhalten. In Scrum gibt es drei Artefakte, die der Transparenz dienen:

- Product Backlog
    - Katalog mit allen Anforderungen als To-Do Liste
    - Wird vom Product Owner weiterentwickelt
    - Wird an Produkt angepasst
- Sprint Backlog
    - Sammlung der Anforderungen die in einem Sprint bearbeitet werden sollen
    - Einzelne Aufgaben des Sprint Backlogs werden «Tasks» genannt.
- Product Increment
    - Am Ende des Sprints steht ein funktionsfähiges Zwischenprodukt
    - Der Product Owner entscheidet, ob das Produkt ausgeliefert wird oder ob weiter am Produkt gefeilt wird

Team:

Ein Scrum-Team besteht aus 2-9 Personen. Dieses Team setzt sich aus diversen Akteuren zusammen und ist selbstorganisiert. So Mitarbeiter:innen aus verschiedenen Sparten zeitgleich am Produkt arbeiten.

Product Owner (PO):

Der Produktmanager ist der Projektverantwortliche. Die Zuständigkeit für das Backlog obliegt seiner Verantwortung. Er kann dieses jederzeit anpassen und Anforderungen hinzufügen, bearbeiten oder streichen.

Scrum Master:

Der Scrum Master ist quasi ein Moderator. Er führt das Team durch Meetings und ist die Ansprechperson für Aussenstehende.

Was sind Sprints?

Ein Sprint bestimmt, was in welchem Zeitraum erledigt wird. Ein Sprint besteht aus 4 Elementen und dauert in der Regel zwei Wochen.

Sprint Planning

Das Sprint Planning steht vor jedem Sprint an. Darin definiert der Product Owner, welche Tasks im Sprint erledigt werden sollen.

Daily Scrums

Tägliches Treffen von ca. 15 Minuten Dauer mit dem Projektteam, in welchem der aktuelle Stand jeder Person abgefragt wird und wie sie den bevorstehenden Tag nutzen werden.

Sprint Review

Das Sprint Review wird mit dem PO und weiteren Stakeholdern durchgeführt («Done). Das Team stellt das einsatzfähige Produkt vor. Der PO entscheidet darüber, ob das Produkt ausgeliefert wird oder Anpassungen am Product Backlog vorgenommen werden müssen.

Sprint Retrospektive

In der Retrospektive geht es um die Arbeit des SCRUM-Teams. Es werden in erster Linie positive Rückmeldungen über die Zusammenarbeit des Teams gegeben. Es dient aber auch dazu, allfällige Verbesserungen anzusprechen und im nächsten Sprint einzusetzen.

Definition of Done (DoD)

Damit ein Produkt «Done» sein kann, müssen eine Reihe von Elementen abgeschlossen werden. Erst wenn diese definierten Elemente erfüllt sind, kann ein Produkt oder eine User Story abgeschlossen werden.

User Story

Eine aus Sicht des Users gemachte Erklärung eines Software-Features mit vorgegebener Struktur.

Struktur: Als Benutzer will ich «Aktion», um «Ergebnis» zu erzielen.

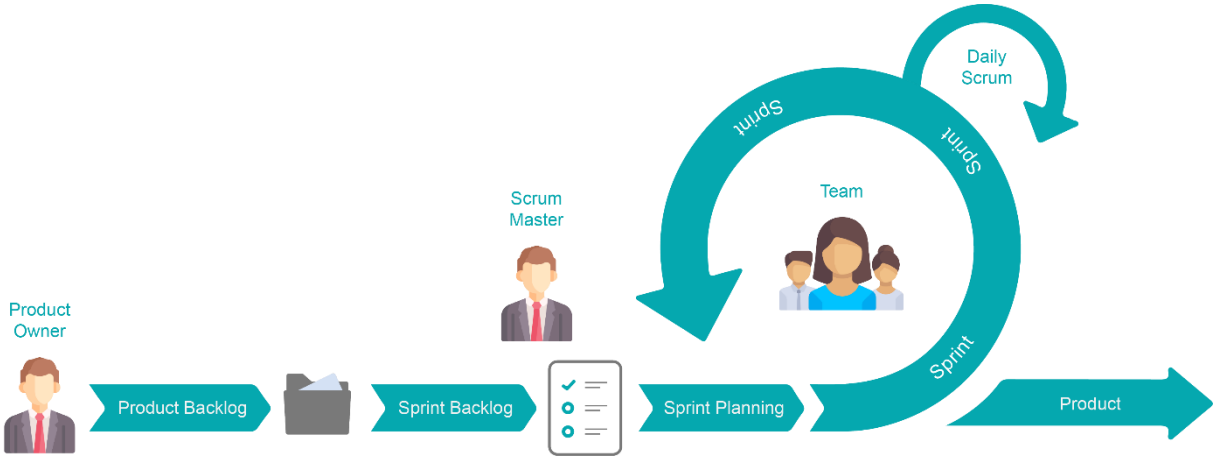


Abbildung 60: Übersicht SCRUM Methode

9. Verzeichnisse

9.1. Abbildungsverzeichnis

9.2. Tabellenverzeichnis

9.3. Quellenverzeichnis

Eine Übersicht der Quellen, die während der Arbeit genutzt wurden.

9.3.1. Internetquellen

Fortinet, ohne Datum, New Features – ZTNA HTTPS access proxy example:

- https://docs.fortinet.com/document/fortigate/7.0.0/new-features/325639/ztna-https-access-proxy-example

Fortinet, 10. Mai 2022, FortiGate / FortiOS 7.0.5 Administration Guide:

- heruntergeladen am 05. April 2022
- von http://docs.fortinet.com/document/fortigate/7.0.5/administration-guide/954635/getting-started

Fortinet, ohne Datum, FortiClient 7.0.3 EMS Administration Guide

- heruntergeladen am 05. April 2022
- von http://docs.fortinet.com/document/forticlient/7.0.3/ems-administration-guide/24450/introduction

Fortinet, ohne Datum, FortiClient 7.0.2 EMS Administration Guide

- heruntergeladen am 23. Januar 2022
- von http://docs.fortinet.com/document/forticlient/7.0.2/ems-administration-guide/24450/introduction

Fortinet, 27. April 2022, FortiClient 7.0.0 New Features

- http://docs.fortinet.com/document/forticlient/7.0.0/new-features/415575/overview

Fortinet, 21. April 2022, FortiClient 7.0.0 EMS Compatibility Chart

- heruntergeladen am 01. April 2022
- von https://docs.fortinet.com/document/forticlient/7.0.0/ems-compatibility-chart

Fortinet, ohne Datum, FortiClient 7.0.3 EMS Release Notes

- http://docs.fortinet.com/document/forticlient/7.0.3/ems-release-notes/717049/introduction

Fortinet, 10. Mai 2022, FortiOS Release Notes

- https://docs.fortinet.com/document/fortigate/7.0.5/fortios-release-notes/236526/known-issues

Fortinet, ohne Datum, FortiClient 6.4, diverse Dokumente

- https://docs.fortinet.com/product/forticlient/6.4

Fortinet, ohne Datum, FortiClient 6.2, diverse Dokumente

- https://docs.fortinet.com/product/forticlient/6.2

9.4. Glossar

Im Glossar werden die wichtigsten Abkürzungen und Begriffe nochmals kurz erläutert.

Abkürzung/Begriff		Erkärung
EMS	Endpoint Management Server	Verwalten, Organisieren und Gruppieren von verbunden Endpunkten mit FortiClient installiert.
VDI	Virtual Desktop Instance	Ein virtuelles Windows-Gerät, in der Firma meist in Citrix eingesetzt.
VPN	Virtual Private Network	Verbindung mit definierten Werten, die einen Tunnel in die Firma öffnet um auf Firmendaten zuzugreifen.
Citrix	Citrix Workspace	Ermöglich den Zugriff auf virtuelle Anwendungen oder dedizierte Desktops.
Lifecycle	Lebenszyklus von Geräten	Ein Lebenszyklus bei den Clients bedeutet, dass sie nach einer definierten Anzahl von Jahre durch neue Geräte ersetzt werden. Im Falle der Firma werden alle Desktop-PC's durch Laptops ersetzt.
Fortinet	Fortinet Inc.	Fortinet ist eine Firma, die Software, Hardware und Dienste im Bereich Informationssicherheit herstellt und vertreibt. Dazu gehören unter anderem Firewalls, VPN-Clients, AccessPoints und Anti Virus.
SCRUM	SCRUM	Agiles Vorgehensmodell in Projekten. Es wird meist in der Softwareentwicklung eingesetzt.
PO	Product Owner	Fachliche:r Vertreter:in der Stakeholder und verantwortlich für das zu entwickelnde Produkt.
Endpoint	Endpunkt, Client, Benutzerinstanz	Der Endpunkt ist meist ein Benutzergerät, wie Laptop, Personal Computer oder Smartphone.

Abbildung 61: Glossar

10. Schlusswort

Die Arbeit am EMS hat mir gefallen. Zu Beginn war ich topmotiviert und kam schnell voran. Ich zeigte Eigeninitiative und wollte alles korrekt machen. Die sehr vielen Bugs und Issues im EMS oder der FortiGate dämpften die Motivation und Freude, es wurde mühselig und das Debugging brauchte Stunden vor dem Laptop, ohne eine Lösung zu finden. Ich bin ein wenig überrascht, dass ein derart halb-fertiges Produkt auf den Markt kommt. Dennoch habe ich durchgehalten und blieb zuversichtlich, dass zumindest die Testumgebung funktionieren würde.

Ich bin froh, wenn ein neuer Release für EMS kommt. Denn es fuchst mich gewaltig, dass der EMS jetzt noch nicht produktiv im Einsatz sein kann. Darum bleibe ich weiterhin am Ball.

11. Danksagungen

Ich möchte der ganzen Firma danken, dass ich ein so spannendes Sicherheitsprojekt durchführen durfte. All die Aspekte, die es zu beachten gibt, gaben mir einen Einblick in die verstrickte Arbeit des Sicherheitsbeauftragten.

Speziell bedanken möchte ich mich bei:

Mathias Edlund **IT-Architekt der Firma**

Danke Mäthu, deinetwegen nehme ich mir den Grundsatz «positiv bleiben» in der IT zu Herzen. Es funktioniert tatsächlich. Zusätzlich möchte ich dir danken, dass du dir Zeit für mich genommen hast, wenn ich mal wieder vor einer Mauer stand und versuchte sie zu durchbrechen, statt drumherum oder darüber zu gehen. Als letztes noch ein grosser Merci für das Durchlesen der Arbeit und das zurückgeben des roten Fadens, den ich ab und zu verloren habe.

Jens Müller **Diplombetreuer, Abteilungsleiter Netzwerk und Linux**

Merci, dass du mir dieses Projekt vorgeschlagen hast. Es war eine super Erfahrung und ich verlasse meinen temporären, ruhigen Arbeitsplatz in eurem Büro nur sehr ungern.

Fabian Hirter **Diplombetreuer der TEKO Bern**

Danke für die benötigten Informationen und deine Geduld, wenn ich mal ein wenig abgeschweift bin. Ich hoffe, die Arbeit gefällt dir einigermassen. Bis Bald!

Marc Rindlisbacher **Abteilungsleiter Servicemanagement und System Administration**

Dank deiner Beharrlichkeit habe ich mich überhaupt entschlossen, die Arbeit nochmals zu versuchen. Ohne deinen Schubser hätte ich sie wahrscheinlich nicht mehr gemacht.

Dan Oppliger **Bereichsleiter IT Services und Auftraggeber**

Du hast mich mehrmals aus dem Büro geschleift, damit ich auf andere Gedanken komme. Der Ausgleich mit dem Squash über Mittag hat mir sehr geholfen, die Arbeit für eine gute Stunde völlig aus meinen Gedanken zu streichen.

Adrian Fröhlich **Projektleiter**

Merci Ädu für das Durchlesen, der etwas über 120 Seiten. Deine Korrekturen und Anmerkungen waren äusserst hilfreich.

12. Eigenständigkeitserklärung

Ich bestätige, dass ich die vorliegende Diplomarbeit selbstständig verfasst und alle benutzten Quellen gekennzeichnet habe. Diese Arbeit wurde weder in gleicher noch in ähnlicher Form bereits einer Prüfungskommission vorgelegt.

Name / Vorname **Leu Samuel**

Ort, Datum: Kerzers, 16. Mai 2022

Unterschrift Diplomand: S. L