# Untersuchung von Network Access Methoden und Optimierung einer bestehenden Lösung

**BACHELORARBEIT**

für die Prüfung zum

Bachelor of Science

des Studiengangs Informatik
Studienrichtung Informationstechnik

an der

Dualen Hochschule Baden-Württemberg Karlsruhe

von

Paul Schien

04.09.2023

| | |
|---|---|
| Matrikelnummer | 7816361 |
| Kurs | TINF20B3 |
| Ausbildungsfirma | Bundesanstalt für Wasserbau, Karlsruhe |
| Betreuer der Ausbildungsfirma | Dipl.-Ing. Uwe Ziesche |
| Gutachter der Studienakademie | Titel Matthias Merz |

**Erklärung**

(gemäß §5(4) der „Studien- und Prüfungsordnung DHBW Technik“ vom 01. 08. 2019)

Ich versichere hiermit, dass ich meine Bachelorarbeit mit dem Thema: „Untersuchung von Network Access Methoden und Optimierung einer bestehenden Lösung“ selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Karlsruhe, 04.09.2023 gez. Paul Schien

Ort, Datum Unterschrift

## Abstrakt

Die Sicherheit eines internen Netzes muss gewahrt werden, da es sich um ein Behördennetz handelt, gelten zusätzliche Auflagen des Bundesamtes für Sicherheit in der Informationstechnik. Um diese Sicherheit des Netzes gewährleisten zu können, muss zuverlässig erkannt werden, ob angeschlossene Endgeräte legitim sind. Da im Laufe der Zeit neue Geräte auf dem Markt kommen, müssen neue Problemstellungen bewältigt werden. Die Problemstellung zur Grundlage dieser Arbeit sind neue Dockingstationen für mobile Arbeitsgeräte, welche ein aktives Netzwerkinterface beinhalten. Die bisherige Netzwerkzugriffsmethode basiert auf dem erkannten Netzwerkinterface eines angeschlossenen Geräts. Durch die neueren Dockingstations als Zwischengerät werden die Endgeräte verschleiert und mit dieser Methode nicht mehr überprüft werden. Dazu werden verschiedene Methoden von den Herstellern MacMon, Cisco und Fortinet erläutert. Abschließend werden sie nach Sicherheit, Erfüllung der Vorgaben, möglicher Implementierung und verwendeter Infrastruktur verglichen.

## Abstract

The security of an internal network must be maintained. Since it is a Government network additional requirement of the Federal Office for Information Security apply. In order to guarantee the security of the network the legitimacy of connected devices must be recognized reliably. Over time as new devices come onto the market, new problems must be overcome. The problem underlying of this work are new docking stations for mobile work devices, which contain an active network interface. The current network access method is based on the detected network interface of a connected device. With the newer docking stations as an intermediate device, the end devices are disguised and can no longer be checked with this method. For this purpose, Various methods from the manufacturers Macmon, Cisco and Fortinet are explained. At the end they are compared according to security, availability according to the specifications, possible implementation and infrastructure used.

# Inhaltsverzeichnis

## Abbildungsverzeichnis



## Tabellenverzeichnis



## Abkürzungsverzeichnis

| | |
|---|---|
| BAW | Bundesanstalt für Wasserbau |
| IEEE | Institute of Electrical and Electronics Engineers |
| LAN | Local Area Network |
| WLAN | Wireless Local Area Network |
| RADIUS | Remote Authentication Dial-In User Service |
| ZTNA | Zero Trust Network Access |

# 1 Einführung

## 1.1 Motivation

## 1.2 IST-Zustand

Die bisherige Netzwerkzugangskontrolle für Endgeräte wird von einer Software von dem Hersteller macmon durchgeführt. Es handelt sich dabei um macmon NAC, welches auf einem lokalen Server vor Ort läuft und eine weite Verbreitung im Behörden Umfeld hat. Es basiert auf der Überprüfung von MAC-Adressen angeschlossenen Geräte am der Netzwerkhardware. Die Switche werden mit einer Konfiguration ausgestattet, welche der Software erlaubt über SNMP Daten und Einstellungen lesen sowie schreiben zu können. Macmon Nac liest alle verbundenen Geräte aus den Switchen und speichert sie in einer Datenbank. Durch Festlegen von Regeln in der Software kann jedes Gerät individuell oder durch Gruppenrichtlinien freigeschaltet werden.

Wenn ein Gerät an das Netzwerk angeschlossen und somit ein Link-Up an dem Switch Port festgestellt wird, reagiert macmon und schaut in der Datenbank nach, wie mit diesem Gerät umgegangen werden soll. Durch die Möglichkeit auf den Switchs Einstellungen ändern zu können, wird dort entsprechend dem internen Regelwerk der Port auf das passende VLan umgeschaltet und somit das Gerät freigeschaltet. Die Endgeräte für Mitarbeiter sind vereinzelt stationäre PCs, jedoch werden immer häufiger mobile Arbeitsgeräte – Laptops – eingesetzt. Zur Verwendung am Arbeitsplatz dienen Dockingstations, um mehrere Bildschirme als auch um externe Maus und Tastatur anzuschließen. Dabei handelt es sich um passive Stationen, welche mit einem proprietären Anschluss für einen Laptop-typ ausgestattet sind.

Das eingesetzte Regelwerk für macmon NAC schaltet nicht autorisierte Geräte in ein VLan, welches nicht geroutet wird und somit kein Internetzugang besitzt. Außerdem werden alle Geräte mit einer Abwesenheit von mehr als 3 Monaten aus den autorisierten Geräten entfernt, wodurch diese keinen Zugriff auf das Netzwerk besitzen.

# 2 Projektbeschreibung

## 2.1 Aufgabenstellung

Das derzeit eingesetzte Network-Access-Control System, welches im dem IST-Zustand beschrieben wird, basiert nur auf der Prüfung von MAC-Adressen der IT-Geräte. Neuartige Dockingstations besitzen ein aktives Netzwerkinterface mit eigener Mac-Adresse, wodurch die dahinter angeschlossenen Geräte in der Regel nicht mehr mit der Mac-Adresse identifiziert werden können.

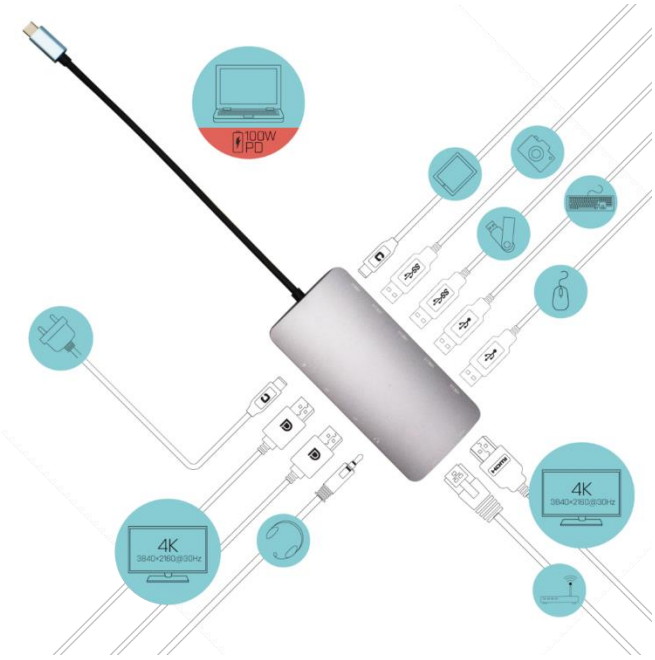


Abbildung 1: Anschlüsse und Verwendung vom Nanodocker Pro 2

Bei der neuartigen Dockingstation handelt es sich beispielhaft um das Produkt c31 Nanodock Pro 2 von dem Hersteller i-tec. Diese ermöglicht es angeschlossene Geräte über USC-C mit 100W zu versorgen. Es können über vier weitere USB-A und einen USB-C Port Geräte verwendet werden. Zur Bildschirmerweiterung sind zwei DisplayPort und ein HDMI Anschluss vorhanden. Neben dem HDMI Port befindet sich ein LAN-Anschluss, welcher bis zu 1000 Mbps unterstützt.

## 2.2 Vorgehen

# 3 Grundlagen

## 3.1 Protokolle

### 3.1.1 802.1X

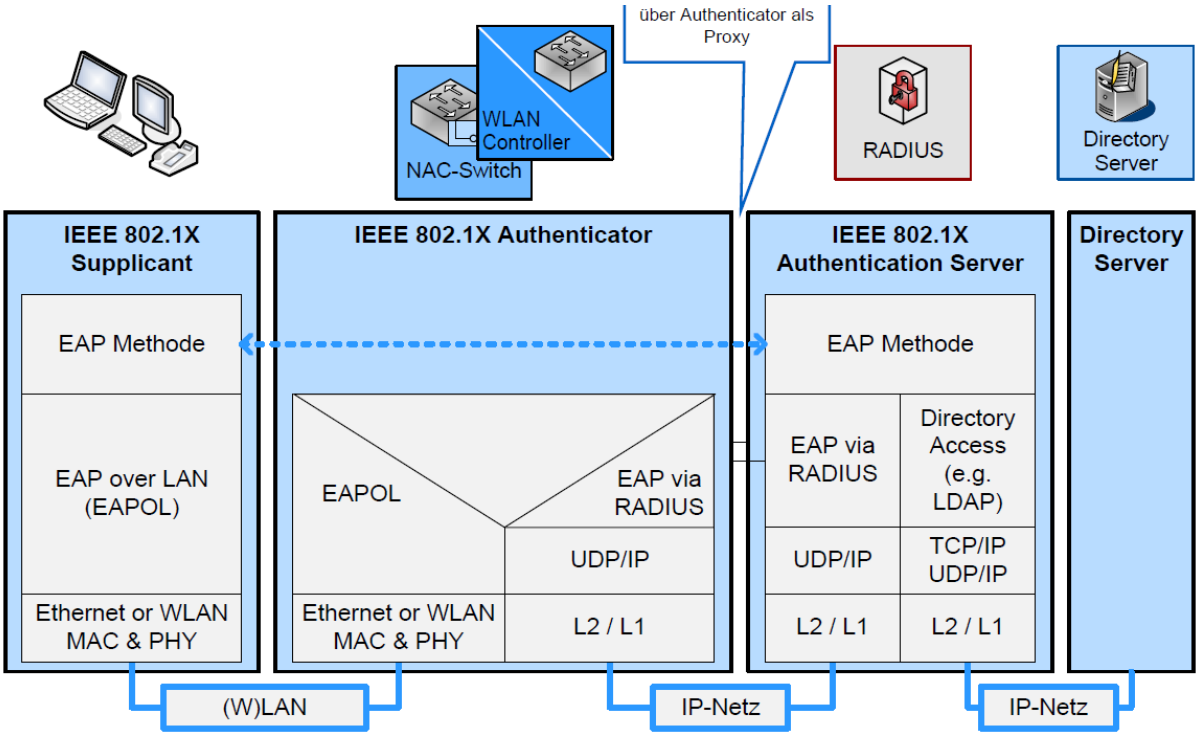
Die Anforderungen an 802.1X ist eine Unterbindung vom unkontrollierten Anschluss von unternehmensfremden Geräten. Zugriff auf das Unternehmensnetz wird nur für Unternehmensgeräte gewährt. Dieser Zugriff wird jedoch nur erlaubt, wenn die Authentisierung erfolgreich beendet wurde und weitere Konfigurationsvorgaben erfüllt

werden.

Mit der Zeit sind mehrere Versionen von 802.1X entwickelt worden. Die relevanten Funktionen sind in der Version IEEE 802.1X-2004 dazugekommen und ist daher auch die an der weitesten verbreiteten Version. Das Endgerät wird als Supplikant bezeichnet, welchem der Zugriff gewährt werden muss. Die Rolle des Authentikators übernimmt der Netzzugangspunkt, da dieser direkt mit dem Supplikanten kommuniziert und die Zugriffberechtigung umsetzt. Der Authentikator leitet die Authentifizierungsanfrage an einen zentralen Authentifikation Server weiter, welcher an weitere Systeme angeschlossen werden kann. Diese angeschlossen Systeme können benutzt werden, um unternehmensweite Credentials zu verifizieren. Die Kommunikation zwischen Supplikanten und Authentikatoren wird im lokalen LAN über EAPoL abgewickelt. Dabei werden die Daten in dem Authentikator nicht verarbeitet, sondern als Proxy mit einem anderen EAP-Paket an den Authentifikation Server weitergeleitet.

| Version | Release | Name |
|---|---|---|
| v1 | 13.07.2001 | IEEE 802.1X-2001 |
| v2 | 13.12.2004 | IEEE 802.1X-2004 |
| v3 | 05.02.2010 | IEEE 802.1X-2010 |
| v4 | 28.02.2020 | IEEE 802.1X-2020 |

Tabelle 1: 802.1X Versionen



#### 3.1.1.1 Kontrollierte Ports

Zur Trennung von Signalisierungs- und Nutzdaten kann ein kontrollierter Port [engl. controlled Port] eingesetzt werden. Mit Hilfe dieser Art von Ports können bestimmte Protokolle als auch Ports an den Supplikanten weitergeleitet werden oder vom Supplikanten empfangen werden. Es muss durch den verwendeten Authentikator unterstützt werden. Die Namensgebung dieser Funktion ist zwischen unterschiedlichen Herstellern nicht eindeutig, jedoch wird die Funktionsweise gleich beworben. Die Forderung nach einem kontrollierten Port ist technisch bedingter Natur. Supplikanten melden sich nach dem Hochfahren am Authentikator an und erhalten nach erfolgreicher Authentisierung Netzwerkzugriff. Bevor der Supplikant sich authentisiert hat, ist er kein Teil des Netzwerkes und kann nicht aus dem Netzwerk erreicht werden. In den meisten Unternehmensnetzwerken werden automatisierte Software Verteiler eingesetzt. Damit diese ein Supplikant erreicht, muss dieser Supplikant sich an dem Netzwerk anmelden. Dieses Problem kann in einem normalen Netzwerk mit dem Wake on LAN Protokoll behoben werden. In diesem Protokoll werden die sogenannten Magic Pakete mit der MAC-Adresse des zu weckenden Endgeräts eingefügt.

Durch die Verwendung eines kontrollierten Ports können Wake on LAN Pakete an die hinter liegenden Supplikanten durchgelassen werden. Da die Wake on LAN Pakete die genaue Mac-Adresse des Endgeräts enthält, muss jedoch der Authentikator oder ein anderer Netzwerk Dienst sich merken welches Endgerät zuletzt an welchem Port angeschlossen war. Durch Magic Pakete lösen ein hochfahren des Supplikants aus.

### 3.1.2 RAIDUS

RADIUS ist ein Server-Client Protokoll, welches Autorisierung, Authentifizierung und Accounting von Geräten durchführt. Dabei wird ein Challenge Response Verfahren angewandt, welches auch mit unterschiedlichen Transportverschlüsselungsverfahren unterstützt wird. Zur Durchführung der Autorisierung und Authentifizierung wird der UDP Port 1812 benutzt. Port 1813 ist dem Accounting zugeteilt. Im RFC-2865[1] wird darauf hingewiesen, dass in alten Implementationen jeweils Port 1645 und 1646 benutzt wird, sich jedoch mit dem „datametrics“ Service überschneidet und daher nicht

genutzt werden soll. Die Transaktionen zwischen den Clients und dem Radius-Server laufen mit einem ausgetauschten Secret, welches benutzt wird um den Inhalt der Pakete, wie eventuelle Zugangsdaten, zu verschlüsseln. Mittels Attribute wird das Protokoll flexibel erweitert und ermöglicht somit eine Informationsübertragung, welcher nicht standardisiert werden muss.

Die Verwendung von UDP wurde in diesem RFC außerdem gerechtfertigt. Die Entscheidung wurde getroffen, da mehrere charakteristische Eigenschaften praktisch für RADIUS sind. Falls die Verbindung zu einem RADIUS Server im Netzwerk gestört ist, muss ein anderer angesprochen werden. Dafür muss eine Kopie der Anfrage gespeichert und zur erneuten Übertragung benutzt werden. Die in TCP eingebaute Bestätigung eines Paketes wird vom RADIUS Protokoll nicht benötigt und wird daher von dem Ersteller des RFCs als unnötiger Overhead bezeichnet. Außerdem ist das erfolgreiche Zustellen eines Paketes nach mehreren Minuten nicht nützlich, da ein anderer Server im Netzwerk innerhalb dieser Zeit die Authentifizierung erfolgreich abschließen kann. Für die Implementation ist die Einfachheit von UDP auch geeigneter, da TCP mehrere Events auslösen kann, die unterschiedlich gehandelt werden müssten.

### 3.1.2.1 Aufbau

Der Aufbau des Paketes ist in Abbildung 2: Paket Format Radius dargestellt. Es beginnt mit einem Code, welcher ein Oktett lang ist und identifiziert den Typ vom Paket. Das folgende Oktett gibt den Identifier an und wird benutzt, um zu klassifizieren, auf welches Paket geantwortet wird. Der Server kann daran Duplikate von Paketen erkennen. Da ein Absender nicht innerhalb kurzer Zeit über dem gleichen Port nicht den gleichen Identifier für ein anderes Paket benutzen darf. Das Feld für die Länge ist 2 Oktette groß und beschreibt die gesamte Länge in Anzahl der Oktette des Pakets mit den Feldern für Code, Identifier, Length, Authentikator und Attribute. Sie ist mindestens 20 und maximal 4096. Der Authentikator ist 16 Oktette lang und wird abhängig von der Art des Paketes gebildet.

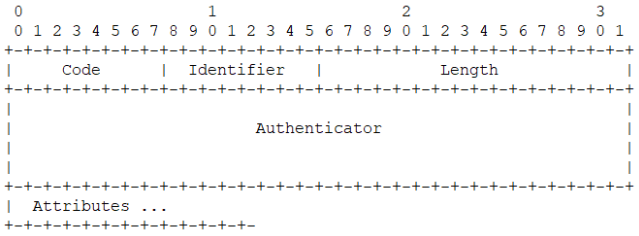



Abbildung 2: Paket Format Radius

In einem Access-Request Paket ist es eine 16 Oktett lange Nummer, welche „Request Authentikator“ im Verfahren genannt wird. Im einem Response Paket wird der Authentikator aus einem MD5-Hash berechnet, welcher über das gesamte RAIDUS Access-Request Paket gebildet wird:

MD5(Code + ID + Length + RequestAuth + Attributes + Secret)

#### 3.1.2.2 Verwendung

## 3.2 Zero Trust Prinzipien

Das nachfolgende Modell Zero-Trust basiert auf drei Sicherheitskonzepten. Es handelt es sich um den sicheren Zugriff, geringste Privilegien und Sichtbarkeit. Der sichere Zugriff muss aus einer verlässlichen starken Datenquelle kommen und muss für jeden Zugriff authentisiert werden. Dabei wird zwischen einer Nutzer Authentifizierung und Maschinen Authentifizierung unterschieden. Beide Authentifizierungsquellen sind in einer Implementierung möglich. Das Verfahren zur Authentifizierung wird nicht eingeschränkt, jedoch durch den Wortlaut „starken Datenquelle“ definiert. Nach der Authentifizierung werden die geringsten Privilegien gewährt, welche sich nach Bedarf erhöhen können. Das Sicherheitskonzept der Sichtbarkeit sieht vor, dass ein nicht authentifizierter Nutzer die Anwendung nicht sehen und erreichen kann.

## 3.3 SIEM

Ein Security Information und Event Manager System wird verwendet, um mit Hilfe von Log Daten eine Virtualisierung für eine zentrale Sicht zu generieren und durch zusätzlichen Kontext Events zu erkennen. Splunk [9], ein Hersteller für eine verbreitete SIEM Lösung, definiert es als „einzelnes Security-Management-System, das volle Sichtbarkeit und Transparenz zu Aktivitäten innerhalb Ihres Netzwerks bietet“. SIEM besteht aus den beiden Sicherheitskonzepten SIM und SEM. Ersteres ist das Security Information Management [SIM], es entspricht den Werten für ein Log Management. Die Grundlegenden Aufgaben ist das Sammeln, Übertragen, Speichern, Weiter Leitung und einfachen Analyse von Log Daten. Diese Daten stammen aus verschiedenen Netzwerk-Komponenten und werden automatisiert durch den SIM behandelt. Daraus ergeben sich laut der Computerwoche [8] die grundlegenden Funktionen für „Richtlinien-orientierte Analysen auch zu Trends, periodische Berichte

und Basisfunktionen für Alarm-Meldungen“.

SEM hingegen bezeichnet die Funktionen für Security Event Management, die Aufgabe besteht die Log Dateien zu korrelieren. Dabei folgt es definierten Richtlinien aber kann gleichzeitig auch mit festgelegten Standards automatisiert abgeglichen werden. Durch ein SIM können komplexere Logiken zur Analyse verwendet werden. Ein SIEM fast beide Konzepte zusammen und ermöglich somit eine zentrale Steuerung von beiden Aspekten, der Zusammentragung von Logdaten, als auch genaue Analyse, Auswertung und Benachrichtigungen der Nutzer.

Das Whitepaper von Bosch [10] bewertet die Lösung eines SIEM-Systems als On-Premise Server positiv, da es über umfangreiche Anwendungsfälle genutzt werden kann und nicht nur als reine Angriffserkennung dient. Diese Funktion wird meistens von externen Firmen vorgeschrieben, welches die Individuelle Entscheidungen innerhalb des Unternehmens einschränkt. Als Nachteil wird das erhöhte Knowhow genannt, da keine Experten als Dienstleiter das SIEM betreuen und Regeln erstellen, sondern Mitarbeiter des Unternehmens für dieses System geschult werden müssen. Auch wird somit der Bedarf an Experten für das einmalige Anlernen erhöht, welcher in der Anfangsphase eines Systems Schwierigkeiten aufklären kann und somit zu einer höheren Produktivität führt.

# 4 Methoden

## 4.1 Network Access Control

Bei Network Access Control

## 4.2 Software-Defined Perimeter

Software-Defined Parameter ist ein Sicherheitskonzept welches von der Cloud Security Alliance [CSA] April 2014 in der Spezifikation 1.0 veröffentlicht wurde[11]. Die aktuelle Spezifikation 2.0 wurde März 2022 veröffentlicht[12]. CSA ist eine Non Profit Organisation, welche 2008 gerändet wurde um die Sicherheit von Cloud-Umgebungen und Cloudservices zu fördern. SDP stellt Sicherheit für die angebundenen Netze, Cloud-Umgebungen und andere Systeme her, indem es die netztechnische Anbindung der Systeme verborgen werden. Dabei verwendet es nur einen reinen Softwareeinsatz und keine physische Abtrennung der Hardware und Netzwerktechnik. Auf Grund der Arbeitsweise von SDP wird auch der Begriff Black Cloud genutzt.

### 4.2.1 Modelle

Bei der Implementierung von SDP unterscheidet man in der zweiten Spezifikation in sechs unterschiedliche Modelle, welche verwendet werden um unterschiedliche Netzwerktopologien abzusichern. Bei der Beschreibung der Modelle werden drei verbreiterte tiefer erklärt und weitere Schematisch dargestellt.

#### 4.2.1.1 Client - Gateway Modell

Das erste Modell eignet sich, wenn ein oder mehrere Server hinter einer SDP-Infrastruktur geschützt werden müssen. Der Client baut eine Verbindung zu dem Gateway auf

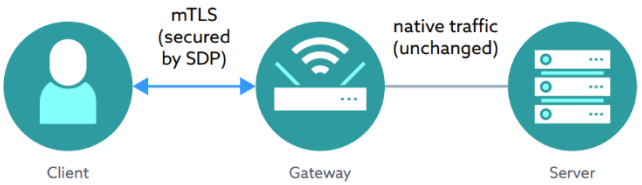



Abbildung 3: Darstellung Client - Gateway Modell [11]

mit der Absicht den Server zu erreichen. Das Gateway prüft diesen Client und stellt eine Verbindung zu dem Server auf, welcher Dieses Modell hat den Vorteil, dass keine Änderungen an den zu schützenden Servern und Infrastruktur vorgenommen werden müssen, da das Gateway als Mittelmann in der Verbindung steht und sich somit nur etwas für den betroffenen Client ändert.

### 4.2.1.2 Client - Server Modell

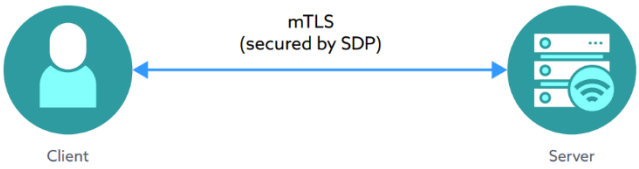



Abbildung 4: Darstellung Client - Server Modell [11]

Ein Nachteil des Client - Gateway Modells ist, dass das Gateway als Mittelmann zwischen dem Client und Server agiert. Wenn eine Ende-zu-Ende Verbindung zwischen Client und Server mit SDP gefordert ist, muss eine Software auf dem Server benutzt werden, welche den Secure Perimeter auf dem Server laufen lässt und den bereitzustellenden Service damit verbindet. Über diese Software werden die Verbindungen aufgebaut und Endgeräte überprüft. Ein Nachteil von diesem Modell ist die Änderung am und höhere Belastung des Servers, welcher den Service bereitstellt. Vorteil dabei ist die Erreichbarkeit über eine Ende-zu-Ende Verbindung und keiner Bereitstellung eines weiteren Servers.

### 4.2.1.3 Gateway - Gateway Modell

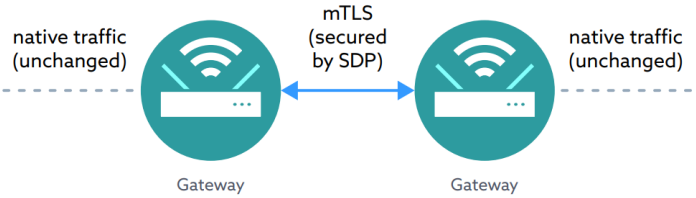
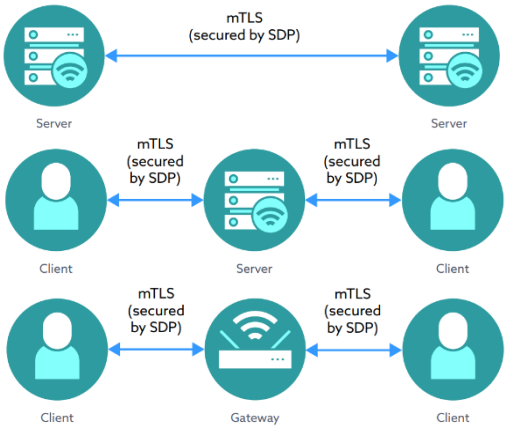



Abbildung 5: Darstellung Gateway - Gateway Modell

Um zwei getrennte Netze mittels SDP zu verbinden werden in beiden Netzen Gateways bereitgestellt. Dadurch können nicht verbundene Cloudsysteme Services bereitstellen, die vom jeweils anderen genutzt werden. Dieses Modell ist in der Spezifikation SPD 2.0 definiert und konnte jedoch in einer Infrastruktur der Spezifikation 1.0 kompliziert umgesetzt werden. Der Vorteil des Modells ist die unveränderte native Verbindung, welche mit SDP zwischen den Gateways getunnelt ist.

### 4.2.1.4 Weitere Modelle




Die Cloud Security Alliance definierte weitere Modelle um SDP für ein Großteil der Anwendungsfälle unkompliziert und genormt bereitstellen zu können. Diese sind das Server – Server Modell, welches zwei Server mit dem defined Perimeter von außen absichert. Das Client-Server-Client Modell, stellt den Anwendungsfall einer Kommunikation über einen Server zwischen Clients dar. Das Client-Gateway-Client Modell ist eine Variation des Client-Server-Client Modells, bei dem die Clients eine direkte Verbindung zueinander aufbauen müssen und kein Service benötigt wird

## 4.3 Zero Trust Network Access

Zero Trust Network Access oder auch kurz ZTNA ist ein Konzept um eine Anwendung sicher mit einem steuerbaren Zugriff vom Internet zugriffsfähig zu machen. Dabei wird die Interaktion eines Service von dem Netzwerk Zugriff isoliert betrachtet. Diese Isolierung erlaubt es wie SDP das Gerät von außen nicht sichtbar machen zu lassen.

Unterscheidung in drei ZTNA-Typen, welche Unterschiedliche Bereiche eines Netzwerkes schützen. Dabei handelt es sich um ZTNA zum Schützen von Endnutzern, Schützen der Arbeitslast und Schützen eines Geräts. Beim Schutz eines Endnutzers wird durch die ZTNA versichert, dass der Nutzer nur den Zugang zu einer Anwendung erlangt und keinen Kontakt mit anderen (Internet-)Services bekommt. Der Arbeitslastschutz wird erlangt in dem keine

## 4.4 Vergleich der Methoden

Die Methoden haben durch unterschiedliche Anwendungsgebiete und Eingriffe in die Architektur, verschiedene Vor und Nachteile. Da sie aber alle verwendet können, um ein Netz sicherer zu machen, werden diese hier zusammengetragen. NAC greift beim Verbinden eines Clients mit der Netzwerkschnittstelle ein und kann direkt eine Hardwareanbindung an das Netzwerk unterbrechen. Bei SDP und ZTNA werden Software Produkte benutzt, welche auf Endnutzer, Service oder drittbeteiligte Geräte angewandt wird und eine Überprüfung der Verbindungen erlaubt.

# 5 Mögliche Lösungen

## 5.1 Cisco ISE

Der Hersteller Cisco bietet für die Funktion der Netzwerkzugangskontrolle das Produkt Cisco Identity Services Engine [ISE] an.

## 5.2 Macmon

Macmon bietet mehrere Lösungen für die Netzwerksicherheit an. Dabei handelt es sich um die momentan verwende Network Access Control Lösung macmon NAC. Außerdem wird eine zentrale ZTNA Lösung unter dem Namen „macmon SDP Suite“ wird angeboten. Dabei steht das SDP für Software Defined Perimeter, welches im Kapitel 4.2 erklärt wird. Diese Lösung steht nur als Cloudbasierte Anwendung auf Servern von Macmon zur Verfügung. Da diese Server noch nicht alle benötigten Zertifikate des Bundesamtes für Sicherheit in der Informationstechnik erlangt hat, kann es nicht als Lösung innerhalb der BAW genutzt werden.

Die ZTNA Lösung ist in dem macmon Network Paket enthalten. Dabei werden durch die konfigurierte Netzwerkhardware alle Endgeräte in einer Datenbank gespeichert, auf diese dann ein Regelwerk angewendet werden kann. Dabei stehen mehrere Auswahlmöglichkeiten zur Verfügung. Es wird unterschieden in einem nachgelagerten Prüfprozess und erstmalige Freischaltung eines Geräts, welches somit kurzzeitig Zugriff auf das Netzwerk erlangt. Der Gegensatz dazu ist das direkte Prüfen durch das Regelwerk und freischalten, sobald es als autorisiertes Gerät identifiziert wurde. Als nachgelegter Prüfmethoden wird das Auslesen und Prüfen des lokalen Zertifikatsspeichers, abrufbare Einstellungen des konfigurierten WMI Profils angeboten.

## 5.3 Fortinet

## 5.4 Software Dockingstation

Die verwendete Dockingstation besitzt eine Software, welche es erlaubt, dass diese die Mac-Adresse des Geräts annehmen zu können.

# 6 Vergleich der Lösungen

# 7 Fazit

Um Network Access Control im Netz umzusetzen, eignen sich verschiedene Herangehensweisen, welche Unterschiedliche Schwierigkeiten bei der Implementierung darstellen. Für die Implementierung wird eine zentrale SIEM Lösung zur Fehlererkennung empfohlen, da Endnutzer und Services betroffen sind. Diese erlaubt es bei Problemen verschiedene Logdaten der Netzwerkhardware, Authentisierungsmechaniken zu analysieren, sodass die Eskalationsstufe beim technischen Support geringgehalten, werden kann.

## Literaturverzeichnis

[1] Remote Authentication Dial In User Service (RADIUS) [online] https://www.rfc-editor.org/rfc/rfc2865 Abgerufen am: 06.06.2023

[2] Aurand, Andreas LAN-Sicherheit dpunkt.verlag Heidelberg, 1. Auflage 2005

[3] RADIUS Types – iana [online] https://www.iana.org/assignments/radius-types/radius-types.xhtml Abgerufen am: 15.06.2023

[4] Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions [online] https://www.rfc-editor.org/rfc/rfc6929 Abgerufen am: 15.06.2023

[5] Private Enterprise Numbers – iana [online] https://www.iana.org/assignments/enterprise-numbers/ Abgerufen am: 15.06.2023

[6] Secure Network Access - What is Zero Trust [online] https://www.appgate.com/blog/what-is-zero-trust Abgerufen am: 19.06.2023

[7] What Is Zero Trust Network Access [online] https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust-network-access Abgerufen am: 03.07.2023

[8] Was SIM und SEM von SIEM unterscheidet [online] https://www.computerwoche.de/a/was-sim-und-sem-von-siem-unterscheidet,2511108 Abgerufen am: 12.07.23

[9] Was ist ein SIEM? [online] https://www.splunk.com/de_de/data-insider/what-is-siem.html Abgerufen am: 12.07.23

[10] SIEM-Einsatz im Managed Security Operations Center [online] https://business-services.heise.de/security/security-management/beitrag/siem-einsatz-im-managed-security-operations-center-4520 Abgerufen am 21.08.23

[11] SDP Specification 1.0 [online] https://cloudsecurityalliance.org/artifacts/sdp-specification-v1-0/ Abgerufen am 03.08.23

[12] Software-Defined Perimeter (SDP) Specification v2.0 [online] https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-zero-

trust-specification-v2/ Abgerufen am 04.08.23

[13]