#### 2021

Aufbau eines sicheren

Firmennetzwerks

##### Zürcher Lehrbetriebsverband ICT Abschlussprojekt

**Inhalt**

[ÄNDERUNGSTABELLE 4](#_bookmark0)

[INFORMATIONEN 4](#_bookmark1)

[Vorgaben 4](#_bookmark2)

[Ausgangslage 4](#_bookmark3)

[ZEITPLAN 5](#_bookmark4)

[Soll-Zustand 5](#_bookmark5)

[Ist-Zustand 6](#_bookmark6)

* 1. [Vorstudie 7](#_bookmark7)
  2. [Hauptstudie 7](#_bookmark8)
  3. [Detailstudie 7](#_bookmark9)
  4. [VMs aufsetzen 7](#_bookmark10)
  5. [OPNsense konfigurieren / dokumentieren 8](#_bookmark11)
  6. [Intrusion Prevention einrichten / dokumentieren 9](#_bookmark12)
  7. [ZFS Fileserver aufsetzen / dokumentieren 9](#_bookmark13)
  8. [Monitoring von OPNsense / dokumentieren 9](#_bookmark14)
  9. [Monitoring des Fileservers / dokumentieren 10](#_bookmark15)
  10. [Monitoring des Monitoring-Servers / dokumentieren 10](#_bookmark16)
  11. [WireGuard Tunnel aufbauen / dokumentieren 10](#_bookmark17)
  12. [Externer DHCP-Server aufsetzen / dokumentieren 10](#_bookmark18)
  13. [PowerPoint Folien vorbereiten 10](#_bookmark19)
  14. [Live-Demo planen 11](#_bookmark20)
  15. [/3.4 Live-Demo aufnehmen und schneiden 11](#_bookmark21)

[3.5 Abschlussprojekt präsentieren 11](#_bookmark22)

[TESTPROTOKOLL 11](#_bookmark23)

[OPNsense konfigurieren 11](#_bookmark24)

[Fileserver aufsetzen 13](#_bookmark25)

[Monitoring-Server aufsetzen 14](#_bookmark26)

[WireGuard Tunnel aufbauen 16](#_bookmark27)

[Externer DHCP-Server aufsetzen 17](#_bookmark28)

# Änderungstabelle

|  |  |
| --- | --- |
| **DATUM** | **ÄNDERUNG** |
| **14.06.2021** | Dokument erstellt |
| **14.06.2021** | Zeitplan erstellt |
| **14.06.2021** | Die Schritte des Zeitplans detailliert beschrieben |
| **16.06.2021** | Am Testprotokoll der Konfiguration von OPNsense gearbeitet |
| **21.06.2021** | Das Testprotokoll der Konfiguration von OPNsense beendet |
| **21.06.2021** | Die statischen IP-Adressen im Zeitplan ergänzt |
| **22.06.2021** | Das Testprotokoll zum Aufsetzen des Fileservers geschrieben |
| **23.06.2021** | Das Testprotokoll zum Aufsetzen des Monitoring-Servers geschrieben |
| **28.06.2021** | Das Erstellen einer passenden Netzwerktopologie in der Planung erfasst |
| **28.06.2021** | Eine passende Netzwerktopologie erstellt |
| **28.06.2021** | Anpassungen des Monitoring-Servers im Testprotokoll vorgenommen |
| **29.06.2021** | Das Testprotokoll zum Aufsetzen des externen DHCP-Servers geschrieben |
| **29.06.2021** | Das Testprotokoll zum Aufbau des WireGuard Tunnels geschrieben |
| **30.06.2021** | Die Analysen der Testfälle verfasst |
| **30.06.2021** | Ergänzungen im Zeitplan vorgenommen |
| **01.07.2021** | Die allgemeinen Informationen hinzugefügt |
| **01.07.2021** | Das Layout des Dokuments überarbeitet |
| **01.07.2021** | Das Gant-Diagramm eingefügt |

# Informationen

## Vorgaben

Ich durfte an insgesamt 12 bzw. 13 Arbeitstagen, die mir vom ZLI dafür zur Verfügung gestellt wurden, an diesem Abschlussprojekt arbeiten. Da ich durch einen Schulausfall einen Tag länger für das ZLI arbeiten durfte, hatte ich 13 statt 12 Tage Zeit. Das Thema des Projekts wurde von mir selbst gewählt, was mir die Möglichkeit gab, mich zum Abschluss des ersten Lehrjahres nochmals mit Technologien auseinanderzusetzen, die mich besonders stark interessieren.

## Ausgangslage

In meinem Abschlussprojekt gehe ich von folgender Situation aus…

Die Firma Zuko hat vor spezielle und neue Taschenlampen zu verkaufen. Da die Firma bisher nur ein Büro angemietet hat, möchte die Firmenleitung, dass ich, Leiter der IT-Abteilung dieser Firma, ein besonders sicheres Netzwerk aufbaue, damit die 7 Mitarbeiter der Firma ungestört mit ihrem persönlichen Laptop in den Büroräumlichkeiten arbeiten können. Die Sicherheit steht bei dieser Firma an oberster Stelle, denn sie hat mit ihren neuen Taschenlampen eine Weltneuheit geschaffen und alle ihre Daten sind somit streng vertraulich. Zuko will mit einem sicheren Netzwerk verhindern, dass ihre Ideen gestohlen werden. Alle ihre wichtigen Dokumente möchten sie auf einem internen Fileserver lagern, welcher auch von mir aufgesetzt und eingerichtet werden soll. Zu guter Letzt möchte der Gründer der Firma, dass das ganze Netzwerk von mir überwacht wird. Dafür baue ich eine passende Monitorumgebung auf.

Wenn ich noch genug Zeit für die optionalen Meilensteine habe, trifft auch folgendes zu…

Die Angestellten möchten auch von Zuhause aus arbeiten, also ist ein VPN-Tunnel nötig, um eine sichere Verbindung von den privaten Laptops ins Firmennetzwerk zu gewährleisten. Ausserdem ist es der Wunsch des Geschäftsführers, dass der DHCP-Server als separater Server fungiert, um der Ausfallsicherheit beizusteuern.

# Zeitplan

## Soll-Zustand

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Aufbau eines sicheren Firmennetzwerks inkl. Fileserver und Monitoringumgebung**  ZLI Abschlussprojekt EINFACHES GANTT-DIAGRAMM von Vertex42.com  Mo, 6.7.2021 https://[www.vertex42.com/ExcelTemplates/simple-gantt-chart.html](http://www.vertex42.com/ExcelTemplates/simple-gantt-chart.html)  Projektanfang: | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | Woche anzeigen: | 1 |  |  | 7. Jun 2021  7 8 9 10 11 12 13 | | | | | | | 14. Jun 2021  14 15 16 17 18 19 20 | | | | | | | 21. Jun 2021  21 22 23 24 25 26 27 | | | | | | | 28. Jun 2021  28 29 30 1 2 | | | | | 3 | 4 | 5. Jul 2021 | | | | | | | 12. Jul 2021  12 13 14 15 16 17 18 | | | | | | | 19. Jul 2021  19 20 21 22 23 24 25 | | | | | | | 26. Jul 2021  26 27 28 29 30 31 1 | | | | | | |
| 5 | 6 | 7 | 8 | 9 10 11 | | |
| **AUFGABE** | **FORTSCHRITT** | **START** | **ENDE** |  | M | D | M | D | F | S | S | M | D | M | D | F | S | S | M | D | M | D | F | S | S | M | D | M | D | F | S | S | M | D | M | D | F | S | S | M | D | M | D | F | S | S | M | D | M | D | F | S | S | M | D | M | D | F | S | S |
| **Phase 1 Planung** | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.1 Vorstudie |  | 7.6.21 | 7.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.2 Hauptstudie |  | 7.6.21 | 9.6.21 |  |  | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.3 Detailstudie |  | 14.6.21 | 30.6.21 |  |  |  |  |  |  |  |  |  | | | | | | | | | | | | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Phase 2 Umsetzung** | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.1 VMs aufsetzen |  | 14.6.21 | 14.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.2 OPNsense konfigurieren |  | 15.6.21 | 15.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.3 Intrusion Prevention einrichten |  | 15.6.21 | 16.6.21 |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.4 ZFS File-Server aufsetzen |  | 21.6.21 | 22.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.5 Monitoring von OPNsense |  | 23.6.21 | 23.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.6 Monitoring des Fileservers |  | 23.6.21 | 23.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.7 Monitoring des Monitoring-Servers |  | 23.6.21 | 23.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.8 WireGuard Tunnel aufbauen |  | 28.6.21 | 28.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.9 Externer DHCP-Server aufsetzen |  | 29.6.21 | 29.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Phase 3 Dokumentation** | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.1 OPNsense dokumentieren |  | 15.6.21 | 16.6.21 |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.2 Intrusion Prevention dokumentieren |  | 16.6.21 | 16.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.3 File-Server dokumentieren |  | 22.6.21 | 22.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.4 Monitoring dokumentieren |  | 28.6.21 | 28.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.5 WireGuard Tunnel dokumentieren |  | 28.6.21 | 28.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.6 Externer DHCP-Server dokumentieren |  | 29.6.21 | 29.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Phase 4 Präsentation** | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.1 Power Point Folien vorbereiten |  | 29.6.21 | 29.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.2 Live Demo planen |  | 29.6.21 | 29.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.3 Live Demo aufnehmen |  | 30.6.21 | 30.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.4 Live Demo schneiden |  | 30.6.21 | 30.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.5 Abschlussprojekt präsentieren |  | 5.7.21 | 7.7.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

t

t

## Ist-Zustand

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Aufbau eines sicheren Firmennetzwerks inkl. Fileserver und Monitoringumgebung**  ZLI Abschlussprojekt EINFACHES GANTT-DIAGRAMM von Vertex42.com  Mo, 6.7.2021 https://[www.vertex42.com/ExcelTemplates/simple-gantt-chart.html](http://www.vertex42.com/ExcelTemplates/simple-gantt-chart.html)  Projektanfang: | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | Woche anzeigen: | | | 1 |  |  | 7. Jun 2021  7 8 9 10 11 12 13 | | | | | | | 14. Jun 2021  14 15 16 17 18 19 20 | | | | | | | 21. Jun 2021  21 22 23 24 25 26 27 | | | | | | | 28. Jun 2021  28 29 30 1 2 | | | | | 3 | 4 | 5. Jul 2021 | | | | | | | 12. Jul 2021  12 13 14 15 16 17 18 | | | | | | | 19. Jul 2021  19 20 21 22 23 24 25 | | | | | | | 26. Jul 2021  26 27 28 29 30 31 1 | | | | | | |
| 5 | 6 | 7 | 8 | 9 10 11 | | |
| **AUFGABE** | **FORTSCHRITT** | | | **START** | **ENDE** |  | M | D | M | D | F | S | S | M | D | M | D | F | S | S | M | D | M | D | F | S | S | M | D | M | D | F | S | S | M | D | M | D | F | S | S | M | D | M | D | F | S | S | M | D | M | D | F | S | S | M | D | M | D | F | S | S |
| **Phase 1 Planung** | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.1 Vorstudie | | 100% | | 7.6.21 | 7.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.2 Hauptstudie | | 100% | | 7.6.21 | 9.6.21 |  |  | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.3 Detailstudie | | 100% | | 14.6.21 | 1.7.21 |  |  |  |  |  |  |  |  |  | | | | | | | | | | | | | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Phase 2 Umsetzung** | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.1 VMs aufsetzen | | 100% | | 14.6.21 | 15.6.21 |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.2 OPNsense konfigurieren | | 100% | | 15.6.21 | 15.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.3 Intrusion Prevention einrichten | | 100% | | 15.6.21 | 16.6.21 |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.4 ZFS File-Server aufsetzen | | 100% | | 21.6.21 | 22.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.5 Monitoring von OPNsense | | 100% | | 23.6.21 | 23.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.6 Monitoring des Fileservers | | 100% | | 22.6.21 | 22.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.7 Monitoring des Monitoring-Servers | | 100% | | 22.6.21 | 22.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.8 WireGuard Tunnel aufbauen | | 66% |  | 28.6.21 | 29.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.9 Externer DHCP-Server aufsetzen | | 100% | | 28.6.21 | 28.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Phase 3 Dokumentation** | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.1 OPNsense dokumentieren | | 100% | | 15.6.21 | 16.6.21 |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.2 Intrusion Prevention dokumentieren | | 100% | | 16.6.21 | 16.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.3 File-Server dokumentieren | | 100% | | 22.6.21 | 22.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.4 Monitoring dokumentieren | | 100% | | 23.6.21 | 23.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.5 WireGuard Tunnel dokumentieren | | 100% | | 29.6.21 | 29.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.6 Externer DHCP-Server dokumentieren | | 100% | | 29.6.21 | 29.6.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Phase 4 Präsentation** | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.1 Power Point Folien vorbereiten | | 100% | | 30.6.21 | 1.7.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.2 Live Demo planen | | 100% | | 1.7.21 | 1.7.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.5 Abschlussprojekt präsentieren | 0% | | | 6.7.21 | 6.7.21 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

t

t

## Vorstudie

Die Vorstudie soll die grundsätzliche Idee des Projekts in einem oder mehreren Lösungsvorschlägen ausarbeiten. Dabei soll noch nicht ins Detail gegangen werden. Sie soll lediglich einen groben Eindruck in die Projektidee schaffen.

## Hauptstudie

In der Hauptstudie entscheide ich mich ganz klar für einen Lösungsweg. Dieser wird dann ausgearbeitet, so dass er ganz einfach weitergereicht werden könnte und eine andere Person das Projekt ohne offene Fragen umsetzen kann. Dabei ist wichtig, dass ich die Komponenten und deren Beziehungen ganz genau beschreibe.

## Detailstudie

In der Detailstudie wird sowohl ein Gant-Diagramm als auch ein Testprotokoll erstellt. So kann einerseits ein detaillierter Zeitplan erstellt, und andererseits die nötigen Testfälle genau beschrieben werden.

## VMs aufsetzen

Zu Beginn des Projekts müssen zunächst alle nötigen VMs erstellt werden. Dafür werden 6 virtuelle Maschinen in VMware Workstation Pro erstellt. Die Konfiguration dieser VMs sieht wie folgt aus…

### Router

|  |  |
| --- | --- |
| *Betriebssystem* | OPNsense |
| *Prozessorkerne* | 1 |
| *Arbeitsspeicher* | 2 GB |
| *Speicher* | 20 GB |
| *Netzwerkadapter 1* | Bridged |
| *Netzwerkadapter 2* | LAN-Segment (Abschlussprojekt) |

### Ubuntu Test-Client

|  |  |
| --- | --- |
| *Betriebssystem* | Ubuntu Desktop |
| *Version* | 20.04 |
| *Prozessorkerne* | 2 |
| *Arbeitsspeicher* | 4 GB |
| *Speicher* | 60 GB |
| *Netzwerkadapter* | LAN-Segment (Abschlussprojekt) |

### Windows Test-Client

|  |  |
| --- | --- |
| *Betriebssystem* | Microsoft Windows |
| *Version* | 10 |
| *Prozessorkerne* | 2 |
| *Arbeitsspeicher* | 4 GB |
| *Speicher* | 80 GB |
| *Netzwerkadapter* | LAN-Segment (Abschlussprojekt) |

### Fileserver

|  |  |
| --- | --- |
| *Betriebssystem* | Ubuntu Server |
| *Version* | 20.04.2 |
| *Prozessorkerne* | 2 |
| *Arbeitsspeicher* | 2 GB |
| *sda* | 60 GB |
| *sdb* | 100GB |
| *sdc* | 100GB |
| *sdd* | 100GB |
| *sde* | 100GB |
| *Netzwerkadapter* | LAN-Segment (Abschlussprojekt) |

### Monitoring-Server

|  |  |
| --- | --- |
| *Betriebssystem* | Ubuntu Server |
| *Version* | 20.04.2 |
| *Prozessorkerne* | 2 |
| *Arbeitsspeicher* | 2 GB |
| *Speicher* | 60 GB |
| *Netzwerkadapter* | LAN-Segment (Abschlussprojekt) |

### DHCP-Server

|  |  |
| --- | --- |
| *Betriebssystem* | Ubuntu Server |
| *Version* | 20.04.2 |
| *Prozessorkerne* | 2 |
| *Arbeitsspeicher* | 2 GB |
| *Speicher* | 60 GB |
| *Netzwerkadapter* | LAN-Segment (Abschlussprojekt) |

## OPNsense konfigurieren / dokumentieren

Um das Firmennetzwerk aufzusetzen, muss als erstes der Router konfiguriert werden. In diesem Fall werden zusätzlich mehrere Ports blockiert und ein neuer Benutzer, der den Root-User ersetzen soll, angelegt. Ausserdem soll ein interner DHCP-Server aufgesetzt werden. Folgende Eigenschaften soll der Router am Ende der Konfiguration besitzen…

### Eigenschaften

|  |  |
| --- | --- |
| *WAN-Interface* | ens0 – DHCP |
| *LAN-Interface* | ens1 – 192.168.11.21 |
| *Netzwerkadresse* | 192.168.11.0 |
| *Subnetzmaske* | 255.255.255.224 |
| *Broadcastadresse* | 192.168.11.31 |
| *Aktive Benutzer* | hikari |
| *Blockierte TCP-Ports* | 135, 139, 455, 4444 |
| *Blockierte UDP-Ports* | 69, 135, 139, 445 |
| *DHCP-Range* | 192.168.11.1 – 192.168.11.20 |

## Intrusion Prevention einrichten / dokumentieren

Auf dem Router soll nach der Konfiguration auch noch **Intrusion Prevention** eingerichtet werden. Dies soll nach Angriffen auf das Netzwerk suchen und diese Angriffe auch gerade blockieren. Dafür müssen Regeln installiert werden, auf die geachtet werden soll. Im Web-Interface von OPNsense werden solche Regeln bereits vorgeschlagen. In diesem Fall werden **alle vorgeschlagenen Regeln** installiert, um einen möglichst grossen Bereich abzudecken.

## ZFS Fileserver aufsetzen / dokumentieren

Nachdem der Router so weit konfiguriert ist, kann der erste Server aufgesetzt werden. Dieser besitzt die statische IP-Adresse **192.168.11.22** und ist der Fileserver des Netzwerks. Falls die Ubuntu Server VM nicht bereits mit dem **ZFS** installiert wurde, muss dies zunächst gemacht werden. Danach kann ein sogenannter **zpool** mit den vier 100GB grossen Festplatten erstellt werden. Dieser soll auf **RAIDZ- II** basieren. Sobald dieser erstellt ist, können darauf die Verzeichnisse aus der untenstehenden Berechtigungsmatrix erstellt werden. Zudem müssen die neuen Benutzer angelegt werden, die auch darin zu finden sind. Für Zuko Hoshino wird als Beispiel der Benutzer **zuko-hoshino** mit dem Passwort **1\*Licht\*** erstellt. Somit wäre das Login für Fritz Huber **fritz-huber** mit dem Passwort **3\*Licht\***. Das Passwort muss später selbstverständlich vom Nutzer geändert werden.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Freigabe | Verzeichnis | Zuko Hoshino | Peter Muster | Fritz Huber | Anna Mueller | Max Suter | Philip Meister | Alexandra Berger |
| Administration | /zuko/administration | rwx | --- | --- | --- | --- | --- | --- |
| Vertrieb | /zuko/sales | r-x | rwx | rwx | r-x | --- | --- | r-x |
| Marketing | /zuko/marketing | r-x | --- | --- | rwx | --- | --- | r-x |
| Entwicklung | /zuko/development | r-x | --- | --- | --- | rwx | rwx | --- |
| Buchhaltung | /zuko/accounting | r-x | --- | --- | --- | --- | --- | rwx |

Gemäss der obenstehenden Berechtigungsmatrix sollen nachher auch die Freigaben mit **SAMBA**

erstellt und an die richtigen Personen freigegeben werden.

## Monitoring von OPNsense / dokumentieren

Um mit dem Monitoring zu beginnen, muss zunächst Check\_MK auf dem Monitoring-Server installiert werden. Auch soll danach das automatisch generierte Passwort durch das Passwort **2\*Licht\*3** ersetzt werden. Nach dem dies geschehen ist und man über das Web-GUI auf Check\_MK zugreifen kann, kann auf dem Router der erste Agent installiert werden. Dieser sollte beim Einbinden als neuer Host in Check\_MK automatisch erkennen, was vom Netzwerk alles überwacht werden kann. Davon sollten sicher Paket- und Fehlerrate, Bandbreite des Netzwerks, Zustand der Ports und CPU-Auslastung überwacht werden.

## Monitoring des Fileservers / dokumentieren

Als nächstes kann ein Agent im Fileserver installiert werden. Dort soll wiederum die Auslastung der CPU gemessen werden. Ausserdem sollten noch das Dateisystem und die mit SAMBA geteilten Ordner überwacht werden.

## Monitoring des Monitoring-Servers / dokumentieren

Zum Schluss soll auch noch ein Agent im Monitoring-Server selbst installiert werden. So überprüft er sich selbst und erkennt sofort allfällige Fehler. Dabei soll der Fokus auf die Überwachung des Monitoring Diensts und dessen Hardwarekomponenten gelegt werden.

## WireGuard Tunnel aufbauen / dokumentieren

Dies ist der erste optionale Meilenstein in meiner Planung. Hierbei wird ein VPN Tunnel mit WireGuard von den Test-Clients zum Firmennetzwerke aufgebaut. Dafür muss auf beiden Clients **WireGuard installiert** werden. Auch benötigt OPNsense den **WireGuard Plugin**. Sobald alles installiert ist, können die Grundkonfigurationen vorgenommen und die generierten PublicKeys ausgetauscht werden. So kann dann nach einer Anpassung in den Firewall-Rules des Routers von den Clients auf das Firmennetzwerk direkt zugegriffen werden. Wichtig dabei ist auch, dass sich die Clients beim Ausprobieren **ausserhalb der Firmennetzwerks** befinden.

## Externer DHCP-Server aufsetzen / dokumentieren

Der externe DHCP-Server lässt sich mit dem Programm **isc-dhcp-server** ziemlich leicht konfigurieren. Die Eigenschaften des Netzwerks müssen dabei einfach in der **Konfiguration** des Servers eingetragen werden. Nach dem nächsten Neustart des Diensts sind diese neuen Konfigurationen aktiv. Es folgen die Eigenschaften des einzurichtenden DHCP-Servers…

### Eigenschaften

|  |  |
| --- | --- |
| *Statische IP-Adresse* | 192.168.11.1 |
| *Netzwerkadresse* | 192.168.11.0 |
| *Subnetzmaske* | 255.255.255.224 |
| *Broadcastadresse* | 192.168.11.31 |
| *Gateway* | 192.168.11.21 |
| *DHCP-Range* | 192.168.11.1 – 192.168.11.20 |
| *Domain Name* | dhcp.zuko |
| *Domain Name Servers* | 8.8.8.8 |
| *DLT* | 600 |
| *MLT* | 7200 |

## PowerPoint Folien vorbereiten

Um mich gut auf meine Präsentation vorzubereiten, erstelle ich ein paar PowerPoint Folien. Diese sollen meinen Vortrag so gut wie möglich unterstützen. Beginnen soll das Ganze mit dem Erläutern des Projektablaufs. Danach will ich die Funktionalität meines Systems aufzeigen. Anschliessend folgt die Sicht aus der Administration und eine fünfminütige Demonstration. Zum Schluss nehme ich mir noch kurz Zeit, mein Fazit zu erläutern.

## Live-Demo planen

Um die Demonstration meines Systems reibungslos durchzuführen, benötige ich ein wenig Vorbereitung. Dazu muss ich mir nochmals das komplette Firmennetzwerk ansehen und genau planen, wie ich bei der Demonstration vorgehe.

## /3.4 Live-Demo aufnehmen und schneiden

Wenn ich bis zum letzten Tag mit allem soweit fertiggeworden bin, möchte ich die Demonstration in Form eines Videos abhalten, welches ich im Voraus aufnehme und schneide. Dabei soll es gleich abgehalten werden, wie ich die Live-Demo geplant habe. Der Vorteil dabei ist, ich kann es ansprechender gestalten und Fehler vermeiden.

## 3.5 Abschlussprojekt präsentieren

Mit allen bisherigen Tätigkeiten in diesem Abschlussprojekt habe ich auf diese Präsentation hingearbeitet. Nun werde ich das Umgesetzte und neu Gelernte präsentieren.

# Testprotokoll

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| OPNsense konfigurieren | | | | | |
| **#** | **Ziel** | **Beschreibung** | **Erwartetes**  **Ergebnis** | **Tatsächliches**  **Ergebnis** | **OK** |
| 1 | Der Router ist mit statisch gesetzter IP in der vorgegebenen IP-Range erreichbar. Mit einer IP ausserhalb dieser Range ist dies nicht der Fall. | Es wird versucht mit einer statisch gesetzten IP- Adresse zwischen **192.168.11.1** und  **192.168.11.30** auf das Web-GUI des Routers mit der IP **192.168.11.21**  zuzugreifen. Dasselbe wird mit einer IP ausserhalb dieser Range versucht. | Wenn die IP in der vorgegebenen Range ist, wird eine Warnung des Browsers angezeigt. Nach dem Ignorieren der Warnung gelangt man auf den Anmelde- Bildschirm. | Wenn die IP in der vorgegebenen Range ist, wird eine Warnung des Browsers angezeigt. Nach dem Ignorieren der Warnung gelangt man auf den Anmelde- Bildschirm. |  |
|  |  |  | Wenn sie ausserhalb der Range ist, wird die Seite nicht geladen. | Wenn sie ausserhalb der Range ist, wird die Seite nicht geladen. |  |
|  | Die Ausführung des Tests hat tadellos funktioniert. Dadurch, dass ich die Netzwerkadresse (192.168.11.0) und Subnetzmaske (255.255.255.224) korrekt eingestellt habe, wurde das vorgesehene Netzwerk erschaffen. | | | | |
| 2 | Ein Client, der mit dem | Ein Client wird mit dem | Beim Ausführen | Beim Ausführen |  |
|  | Router verbunden wird, | Router verbunden. | des Commands ***ip*** | des Commands ***ip*** |  |
|  | erhält dynamisch eine IP- | Danach wird mit dem | ***a*** ist ersichtlich das | ***a*** ist ersichtlich das |  |
|  | Adresse in der | Command ***ip a*** die | die IPv4-Adresse | die IPv4-Adresse |  |
|  | vorgegebenen Range. | aktuelle IP-Konfiguration | des Clients | des Clients |  |
|  |  | eingesehen. | zwischen | zwischen |  |
|  |  |  | **192.168.11.1** und | **192.168.11.1** und |  |
|  |  |  | **192.168.11.20** | **192.168.11.20** |  |
|  |  |  | liegt. | liegt. |  |
|  | Auch diesen Testfall konnte ich ohne Probleme ausführen. Da ich bei den Diensten unter OPNsense für | | | | |
|  | das LAN-Interface DHCPv4 eingerichtet habe erhält jedes Gerät, welches sich mit dem LAN-Interface | | | | |
|  | verbindet, dynamisch eine IPv4 Adresse der vorgegebenen Range (192.168.11.1 – 192.168.11.20). | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3 | Die Interfaces sind korrekt konfiguriert und von einem Client im Netzwerk kann man ins Internet gelangen. | Mit dem Client wird die IP-Adresse **216.58.215.227** von  google.ch angepingt. | Der Client erhält eine Antwort vom Absender mit der IP-Adresse **216.58.215.227**. | Der Client erhält eine Antwort vom Absender mit der IP-Adresse **216.58.215.227**. |  |
| Dieser Testfall wiederum verlief ohne Probleme, denn dafür sind die Firewall-Regeln zuständig welche automatisch auf dem LAN-Interface konfiguriert werden. Diese ermöglichen grundsätzlich allen Datenverkehr der von einem Gerät, dass sich im LAN-Netzwerk befindet, ausgeht. | | | | |
| 4 | Der neue und aktive Nutzer des Routers ist der neu konfigurierte **hikari**. Mit dem root-user lässt es sich nicht mehr einloggen. | Es wird mit beiden Benutzern versuch sich im Web-Interface des OPNsense Routers anzumelden. | Es ist möglich sich mit dem Nutzer **hikari** anzumelden, aber die Anmeldung mit dem root-user wird abgelehnt. | Es ist möglich sich mit dem Nutzer **hikari** anzumelden, aber die Anmeldung mit dem root-user wird abgelehnt. |  |
| Das Ausführen dieses Testfalls hat ebenfalls tadellos funktioniert. Zuvor wurde von mir der root-user deaktiviert und ein neuer Benutzer namens hikari mit Administrationsrechten angelegt. Dies setzt einem potenziellen Angreifer voraus, dass er nicht nur das Passwort, sondern auch den Benutzernamen kennen muss, um sich beim Router einloggen zu können. Ausserdem schränkt es keinerlei weitere Arbeiten ein. | | | | |
| 5 | Die **TCP-Ports 135, 139,** | Es wird der Windows Test- | Bei dem Versuch | Bei dem Versuch |  |
|  | **455, 4444** werden von der | Client, dessen Firewall | Verbindungen auf | Verbindungen auf |  |
|  | Firewall ausgehend | ausgeschaltet ist, an | die blockierten | die blockierten |  |
|  | blockiert. | einem zusätzlichen LAN- | Ports herzustellen, | Ports herzustellen, |  |
|  |  | Interface angeschlossen. | erhält der Ubuntu | erhält der Ubuntu |  |
|  |  | Dieses Interface soll ein | Test-Client gar | Test-Client gar |  |
|  |  | WAN-Interface simulieren | keine Antwort. | keine Antwort. |  |
|  |  | und wird später auch für | Beim Versuch eine | Beim Versuch eine |  |
|  |  | die VPN-Verbindung | Verbindung auf | Verbindung auf |  |
|  |  | verwendet. Dann wird mit | andere Ports | andere Ports |  |
|  |  | dem Ubuntu Test-Client, | herzustellen, | herzustellen, |  |
|  |  | der am normalen WAN- | erhält der Test- | erhält der Test- |  |
|  |  | Angeschlossen ist, eine | Client die Antwort: | Client die Antwort: |  |
|  |  | Telnet Verbindung auf die | ***Unable to connect*** | ***Unable to connect*** |  |
|  |  | blockierten Ports des | ***to remote host:*** | ***to remote host:*** |  |
|  |  | Windows Test-Clients | ***Connection*** | ***Connection*** |  |
|  |  | versucht herzustellen. | ***refused*** | ***refused*** |  |
|  |  | Auch wird versucht |  |  |  |
|  |  | Verbindungen über |  |  |  |
|  |  | andere Ports herzustellen. |  |  |  |
|  | Auch die Ausführung dieses Testfalls verlief problemlos. Der Windows Test-Client lehnt trotz der | | | | |
|  | ausgeschalteten Firewall die Verbindung über Telnet ab. Dennoch erhält der Ubuntu Test-Client eine | | | | |
|  | Antwort, und zwar das die Verbindung vom Windows Test-Client abgelehnt wird. Da die Firewall die Ports | | | | |
|  | nur blockiert und keine Rückmeldung sendet erhält der Test-Client bei der Verbindung auf diese Ports gar | | | | |
|  | keine Antwort. | | | | |
| 6 | Die **UDP-Ports 69, 135,** | - | - | - |  |
|  | **139, 445** werden von der |  |  |  |  |
|  | Firewall ausgehend |  |  |  |  |
|  | blockiert. |  |  |  |  |
|  | Ich konnte leider keine Möglichkeit finden in dieser virtuellen Umgebung die blockierten UDP-Ports zu | | | | |
|  | testen. Wenn ich versuche, die Offenen Ports des Routers von einem Client aus zu scannen erscheinen | | | | |
|  | gar keine offenen Ports. | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 7 | **Intrusion Prevention** funktioniert so wie vorgesehen und wehrt allfällige Attacken auf das Netzwerk ab. | Die Alerts unter der Administration vom **IDS** werden inspiziert. | Unter dem Tab Alerts in der Administration von **Intrusion Detection** werden Aktivitäten notiert, die von den Regeln erfasst und blockiert wurden. | Unter dem Tab Alerts in der Administration von **Intrusion Detection** werden Aktivitäten notiert, die von den Regeln erfasst, aber trotzdem erlaubt wurden. | ~ |
| Das Ausführen des Testfalls hat nicht so funktioniert wie erwartet, denn ich habe lediglich ein **Intrusion Detection System** aufgebaut. In mehreren Artikeln, die ich gelesen habe, stand das es mit dem IPS in Kombination mit VMware Probleme gibt, da dieses direkt auf die Netzwerkkarte zugreifen muss. So habe ich mich dagegen entschieden dies einzusetzen. Das Aufsetzen des IDS hingegen hat reibungslos funktioniert. Auf der Webseite <https://doc.emergingthreats.net/bin/view/Main/EmergingFAQ#What_is_the_general_intent_of_ea> habe ich mich über die verschiedenen Rule-Sets informiert und folgende ausgewählt…   * botcc * drop * attack\_response * dos * exploit * malware * policy   Ausserdem habe ich noch alle Rule-Sets von abuse.ch aktiviert. | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Fileserver aufsetzen | | | | | |
| **#** | **Ziel** | **Beschreibung** | **Erwartetes**  **Ergebnis** | **Tatsächliches**  **Ergebnis** | **OK** |
| 1 | Der Fileserver ist über die | Es wird ein ping Befehl | Beide Sender | Beide Sender |  |
|  | statische IP-Adresse | von beiden Test-Clients | erhalten vom Host | erhalten vom Host |  |
|  | **192.168.11.22** erreichbar. | auf die IP-Adresse | mit der IP-Adresse | mit der IP-Adresse |  |
|  |  | **192.168.11.22** ausgeführt. | **192.168.11.22** | **192.168.11.22** |  |
|  |  |  | (Fileserver) eine | (Fileserver) eine |  |
|  |  |  | Antwort. | Antwort. |  |
|  | Auch dieser Testfall verlief reibungslos. Durch den Eintrag in der netplan-Konfigurationsdatei wurde die | | | | |
|  | IP-Adresse des Servers auf 192.168.11.22 gelegt. Diese IP befindet sich im konfigurierten Netzwerk, wird | | | | |
|  | vom DHCP-Server aber nicht vergeben, was besonders wichtig ist, denn ansonsten könnten IP-Konflikte | | | | |
|  | entstehen. | | | | |
| 2 | Aus allen vier Festplatten | Der Befehl «zpool status» | Es wird ein zpool | Es wird ein zpool |  |
|  | zusammen wurde ein | wird ausgeführt. Dieser | mit RaidZ-II | mit RaidZ-II |  |
|  | zpool mit RaidZ-II namens | zeigt alle mit ZFS | namens **zuko** | namens **zuko** |  |
|  | **zuko** erstellt. | erstellten Pools an und | angezeigt, welcher | angezeigt, welcher |  |
|  |  | informiert den Betrachter | aus den | aus den |  |
|  |  | über das Raid-Level und | Festplatten sdb, | Festplatten sdb, |  |
|  |  | die beteiligten | sdc, sdd, sde | sdc, sdd, sde |  |
|  |  | Festplatten. | besteht. | besteht. |  |
|  | Dieser Testfall wiederum verlief problemlos. Gemäss dieser Anleitung: | | | | |
|  | <https://linuxconfig.org/configuring-zfs-on-ubuntu-20-04>konnte ich ZFS installieren und mit dem | | | | |
|  | Command «***sudo zpool create zuko raidz2 /dev/sdb /dev/sdc /dev/sdd /dev/sde***» den zpool erstellen. | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3 | Das Filesystem ist gemäss | Es wird mit allen | Alle mit Vollzugriff | Alle mit Vollzugriff |  |
|  | Berechtigungsmatrix | angelegten Benutzern | auf das Verzeichnis | auf das Verzeichnis |  |
|  | korrekt aufgebaut. Alle | versucht auf alle | konnten ein | konnten ein |  |
|  | Mitarbeiter haben nur auf | Verzeichnisse zuzugreifen | Verzeichnis | Verzeichnis |  |
|  | bestimmte Bereiche | und ein Verzeichnis mit | erstellen und diese | erstellen und diese |  |
|  | Zugriff. | ihrem Benutzernahmen zu | mit Lese- | mit Lese- |  |
|  |  | erstellen. | Berechtigungen | Berechtigungen |  |
|  |  |  | konnten lediglich | konnten lediglich |  |
|  |  |  | diese Ordner | diese Ordner |  |
|  |  |  | einsehen. | einsehen. |  |
|  | Das Erarbeiten dieses Testfalls wies ein paar Schwierigkeiten auf, aber dennoch konnte ich am Ende alles | | | | |
|  | so wie geplant umsetzen. Die Installation und Konfiguration konnte ich nach von mir selbst | | | | |
|  | dokumentierten Arbeitsschritten ausführen. Um aber später allen die vorgesehenen Berechtigungen zu | | | | |
|  | verteilen, musste ich mich auf der Webseite [https://www.samba.org/samba/docs/current/man-](https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html) | | | | |
|  | [html/smb.conf.5.html](https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html) über die «write list» informieren. | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Monitoring-Server aufsetzen | | | | | |
| **#** | **Ziel** | **Beschreibung** | **Erwartetes**  **Ergebnis** | **Tatsächliches**  **Ergebnis** | **OK** |
| 1 | Check MK wurde korrekt | Auf den Clients wird im | Der | Der |  |
|  | installiert und dessen | Browser die IP-Adresse | Anmeldebildschirm | Anmeldebildschirm |  |
|  | Web-Interface ist über die | **192.168.11.23** | von Check MK | von Check MK |  |
|  | statische IP-Adresse | eingegeben. Hinter dieser | erscheint. | erscheint. |  |
|  | **192.168.11.23** erreichbar. | IP und einem Schrägstrich |  |  |  |
|  |  | wird noch der Name der |  |  |  |
|  |  | zuvor konfigurierten |  |  |  |
|  |  | Instanz angegeben. |  |  |  |
|  | Das Ausführen dieses Testfalls hat sehr gut funktioniert. Da ich zuvor Check MK gemäss dem | | | | |
|  | Erklärungsvideo von Check MK selbst [(https://checkmk.com/de/videos/ep-1-installing-checkmk)](https://checkmk.com/de/videos/ep-1-installing-checkmk) | | | | |
|  | installiert habe und des Servers IP in der netplan-Konfigurationsdatei festgelegt habe, konnte das Web- | | | | |
|  | Interface von CheckMK über die IP 192.168.11.23 erreicht werden. | | | | |
| 2 | Das automatisch | Es wird auf dem | Die Anmeldung ist | Die Anmeldung ist |  |
|  | generierte Passwort | Anmeldebildschirm | erfolgreich und | erfolgreich und |  |
|  | wurde durch das | versucht sich mit dem | man gelangt auf | man gelangt auf |  |
|  | Passwort **2\*Licht\*3** | Benutzer **cmkadmin** und | das Dashboard von | das Dashboard von |  |
|  | ersetzt. | dem Passwort **2\*Licht\*3** | Check MK. | Check MK. |  |
|  |  | anzumelden. |  |  |  |
|  | Auch die Ausführung dieses Testfalls verlief tadellos. Das Passwort wurde nach der Installation gleich auf | | | | |
|  | **2\*Licht\*3** geändert. Dieses Vorgehen ist ebenfalls im zuvor erwähnten [Video](https://checkmk.com/de/videos/ep-1-installing-checkmk) erwähnt. | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3 | Der Router wurde dem Monitoring-Server als Host hinzugefügt, dessen **Auslastung**, **Paket- und Fehlerrate**, **Bandbreite** und **Zustand der Ports** überwacht werden. | Im Web-Interface werden alle Services des Hosts Router betrachtet. Daraus kann ermittelt werden, was überwacht wird und was nicht. | Die Auslastung des Routers sowie dessen Paket- und Fehlerraten, dessen Bandbreite und der Zustand dessen Ports werden von Check MK überwacht und unter den Services  angezeigt. | Die Auslastung des Routers sowie dessen Paket- und Fehlerraten, dessen Bandbreite und der Zustand dessen Ports werden von Check MK überwacht und unter den Services  angezeigt. |  |
| Dieser Testfall verlief nicht ganz so wie erwartet. Nachdem der Host per **SNMP** statt Check MK-Agent dem Monitoring hinzugefügt wurde, waren aber dennoch unter allen Diensten, die überwacht werden können, die erwarteten Punkte aufgelistet. Der Versuch den Check MK-Agent nach folgender Anleitung <https://forum.opnsense.org/index.php?topic=11828.0>auf dem OPNsense Router zu installieren war erfolglos, denn dieser wurde von Check MK beim hinzufügen des Hosts nicht erkannt. Stattdessen wurde von mir der SNMP Plugin auf den Router installiert und dieser schlussendlich per SNMPv2 Check MK hinzugefügt. | | | | |
| 4 | Der Fileserver wurde dem Monitoring-Server als Host hinzugefügt, dessen **Auslastung** und **Filesysteme** überwacht werden. Auch werden die **Shares** einzeln überwacht. | Im Web-Interface werden alle Services des Hosts Fileserver betrachtet.  Daraus kann ermittelt werden, was überwacht wird und was nicht. | Die Auslastung des Fileservers sowie dessen Filesysteme und SAMBA-Shares werden von Check MK überwacht und unter den Services angezeigt. | Die Auslastung des Fileservers sowie dessen Filesysteme werden von Check MK überwacht und unter den Services angezeigt. Die SAMBA-Shares werden nicht einzeln überwacht. | ~ |
| Bei diesem Testfall konnte das Ziel leider nicht ganz erreicht werden. Nachdem der Host per Check MK- Agent dem Monitoring hinzugefügt wurde, war es nicht möglich die SAMBA-Shares einzeln zu überwachen. Der Check MK-Agent wurde ebenfalls gemäss dem zuvor erwähnten [Video](https://checkmk.com/de/videos/ep-1-installing-checkmk) installiert. | | | | |
| 5 | Der Monitoring-Server wurde dem Monitoring- Server als Host hinzugefügt, dessen **Auslastung** und **Zustand der eingerichteten Instanz** überwacht werden. | Im Web-Interface werden alle Services des Hosts Monitoring-Servers betrachtet. Daraus kann ermittelt werden, was überwacht wird und was nicht. | Die Auslastung des Monitoring-Servers sowie der Zustand der eingerichteten Instanz werden von Check MK überwacht und unter den Services angezeigt. | Die Auslastung des Monitoring-Servers sowie der Zustand der eingerichteten Instanz werden von Check MK überwacht und unter den Services angezeigt. |  |
| Dieser Testfall lief genau so wie erwartet. Nachdem ich den neuen Host per Check MK-Agent hinzugefügt habe, konnte ich alle erwarteten Punkte auswählen und dem Monitoring hinzufügen. Den Check MK- Agent konnte ich auf demselben Weg installieren, wie ich dies beim Fileserver gemacht habe. | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 6 | Die **Netzwerktopologie** | Bei allen überwachten | In der automatisch | In der automatisch |  |
|  | zeigt den Aufbau des | Servern wurde der | generierten | generierten |  |
|  | Netzwerkes gemäss der | OPNsense Router als | Netzwerktopologie | Netzwerktopologie |  |
|  | Realität dar. Die Parnets | Parent angegeben. | sind alle Server | sind alle Server |  |
|  | sind allesamt richtig |  | direkt mit dem | direkt mit dem |  |
|  | gesetzt. |  | Router verbunden. | Router verbunden. |  |
|  |  |  | Dieser wiederum | Dieser wiederum |  |
|  |  |  | hat als einziger | hat als einziger |  |
|  |  |  | Zugang nach | Zugang nach |  |
|  |  |  | draussen. | draussen. |  |
|  | Auch dieser Testfall verlief problemlos. Indem ich bei der Konfiguration der Hosts ihren Parent angegeben | | | | |
|  | habe, erstellte sich die Netzwerktopologie von selbst. | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| WireGuard Tunnel aufbauen | | | | | |
| **#** | **Ziel** | **Beschreibung** | **Erwartetes**  **Ergebnis** | **Tatsächliches**  **Ergebnis** | **OK** |
| 1 | Der Router ist vom per VPN-Tunnel angeschlossenen | Es wird ein ping Befehl von beiden Test-Clients auf die IP-Adresse | Beide Clients erhalten eine Antwort vom | Der Ubuntu Test- Client erhält eine Antwort vom | ~ |
|  | Windows Test-Client und | **192.168.22.1** ausgeführt. | Router mit der IP | Router mit der IP |  |
|  | Ubuntu Test-Client | Dies ist die IP des Routers | **192.168.22.1**. | **192.168.22.1**. |  |
|  | erreichbar. | im VPN-Netzwerk |  |  |  |
|  |  | **192.168.22.0/27**. |  |  |  |
|  | Dieser Testfall konnte nicht wie geplant ausgeführt werden. Ich konnte den Aufbau des WireGuard | | | | |
|  | Tunnels mit dem Ubuntu Test-Client beenden, doch aus zeitlichen Gründen konnte ich dies nicht auch | | | | |
|  | noch mit dem Windows Test-Client umsetzen. Dennoch gehe ich davon aus, dass es auch mit Windows | | | | |
|  | funktioniert. | | | | |
|  | Ich habe zunächst die Konfiguration des OPNsense Routers gemäss folgender Anleitung vorgenommen… | | | | |
|  | [https://www.thomas-](https://www.thomas-krenn.com/de/wiki/OPNsense_WireGuard_VPN_f%C3%BCr_Road_Warrior_einrichten) | | | | |
|  | [krenn.com/de/wiki/OPNsense\_WireGuard\_VPN\_f%C3%BCr\_Road\_Warrior\_einrichten.](https://www.thomas-krenn.com/de/wiki/OPNsense_WireGuard_VPN_f%C3%BCr_Road_Warrior_einrichten) Dabei ist zu | | | | |
|  | beachten, dass ich dies nicht über das WAN-Interface, sondern ein zusätzliches LAN-Interface aufgesetzt | | | | |
|  | habe. Dieses wurde aber ähnlich zum WAN-Interface konfiguriert. Danach habe ich gemäss einer | | | | |
|  | weiteren Anleitung [(https://schroederdennis.de/tutorial-howto/wireguard-vpn-server-installieren-client-](https://schroederdennis.de/tutorial-howto/wireguard-vpn-server-installieren-client-to-server/) | | | | |
|  | [to-server/)](https://schroederdennis.de/tutorial-howto/wireguard-vpn-server-installieren-client-to-server/) WireGuard auf dem Ubuntu Test-Client konfiguriert und den verwendeten Port angepasst. So | | | | |
|  | konnte nach dem Start von WireGuard auf beiden Seiten eine Verbindung über den VPN-Tunnel | | | | |
|  | hergestellt werden. | | | | |
| 2 | Die Server, die sich im Firmennetzwerk befinden und über das LAN- Interface zugänglich sind, sind von einem per VPN- Tunnel angeschlossenen Client erreichbar. Kurz gesagt ein Externer Client hat Zugriff zum Firmennetzwerk **192.168.11.0/27**. | Es wird ein ping Befehl von beiden Test-Clients auf die IP-Adressen **192.168.11.22**,   * + - 1. und       2. ausgeführt. | Beide Clients erhalten eine Antwort von jedem der 3 Server. | Der Ubuntu Test- Client erhält eine Antwort von jedem der 3 Server. | ~ |
|  | Auch hier konnte der Testfall nicht wie geplant umgesetzt werden. Dies lag auch daran, dass ich aus zeitlichen Gründen nicht dazu gekommen bin den VPN-Tunnel mit dem Windows Test-Client aufzubauen. Um den Zugriff auf das Netzwerk zu ermöglichen habe ich in der Konfigurationsdatei die beiden Zeilen… | | | | |
|  | ***PostUp = ip route add 192.168.11.0/27 via 192.168.22.1 PreDown = ip route delete 192.168.11.0/27*** | | | | |
|  | hinzugefügt. So hatte auch der per VPN-Tunnel angeschlossene Host vollen Zugriff auf das LAN-Netzwerk. | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3 | Die TCP-Ports **445** und | Es wird versucht auf den | Es wird eine | Es wird eine |  |
|  | **139** sind für die VPN- | Fileserver zuzugreifen und | Verbindung zum | Verbindung zum |  |
|  | Clients offen. | ein Verzeichnis zu öffnen, | Fileserver | Fileserver |  |
|  |  | denn SMP erfolgt über die | hergestellt. | hergestellt. |  |
|  |  | Ports **139** oder **445**. | Darüber lassen | Darüber lassen |  |
|  |  |  | sich die darauf | sich die darauf |  |
|  |  |  | befindenden | befindenden |  |
|  |  |  | Verzeichnisse | Verzeichnisse |  |
|  |  |  | öffnen. | öffnen. |  |
|  | Dieser Testfall verlief reibungslos. Durch die zuvor gesetzten Firewall-Regeln von WireGuard in folgender | | | | |
|  | Anleitung [https://www.thomas-](https://www.thomas-krenn.com/de/wiki/OPNsense_WireGuard_VPN_f%C3%BCr_Road_Warrior_einrichten) | | | | |
|  | [krenn.com/de/wiki/OPNsense\_WireGuard\_VPN\_f%C3%BCr\_Road\_Warrior\_einrichten](https://www.thomas-krenn.com/de/wiki/OPNsense_WireGuard_VPN_f%C3%BCr_Road_Warrior_einrichten) sind für diese | | | | |
|  | Clients, die sich per VPN-Tunnel mit dem Netzwerk verbinden, alle Ports zugänglich. | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Externer DHCP-Server aufsetzen | | | | | |
| **#** | **Ziel** | **Beschreibung** | **Erwartetes**  **Ergebnis** | **Tatsächliches**  **Ergebnis** | **OK** |
| 1 | Der DHCP-Server ist von | Es wird mit einem Ping | Die Clients | Die Clients |  |
|  | den Clients aus über die | versucht von den Clients | erhalten eine | erhalten eine |  |
|  | IP-Adresse **192.168.11.24** | den Server zu erreichen. | Antwort vom | Antwort vom |  |
|  | erreichbar. |  | DHCP-Server mit | DHCP-Server mit |  |
|  |  |  | der IP | der IP |  |
|  |  |  | **192.168.11.24**. | **192.168.11.24**. |  |
|  | Das Ausführen dieses Testfalls hat tadellos funktioniert. Durch den Eintrag in der netplan- | | | | |
|  | Konfigurationsdatei wurde die IP-Adresse des Servers auf 192.168.11.23 gelegt. Diese IP befindet sich im | | | | |
|  | konfigurierten Netzwerk, wird vom DHCP-Server aber nicht vergeben, was besonders wichtig ist, denn | | | | |
|  | ansonsten könnten IP-Konflikte entstehen. | | | | |
| 2 | Die Clients beziehen ihre | WireShark wird auf dem | Der Client erhält | Der Client erhält |  |
|  | dynamische IP-Adresse | Client gestartet, wobei | den **DHCP-Offer** | den **DHCP-Offer** |  |
|  | vom neuen DHCP-Server | der Filter nur nach DHCP- | und den **DHCP-** | und den **DHCP-** |  |
|  | mit der IP-Adresse | Paketen suchen soll. | **Acknowledge** von | **Acknowledge** von |  |
|  | **192.168.11.24**. | Danach wird der Befehl | der IP-Adresse | der IP-Adresse |  |
|  |  | «**dhclient -v**» ausgeführt. | **192.168.11.24**. | **192.168.11.24**. |  |
|  | Auch diesen Testfall konnte ich problemlos ausführen. Ich konnte gemäss meiner eigenen Dokumentation | | | | |
|  | den isc-dhcp-server installieren und konfigurieren. Diese Konfiguration habe ich danach an die hier | | | | |
|  | gewünschte angepasst. | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3 | Ein Client, der per DHCP | Ein Client bezieht seine IP- | Beim Ausführen | Beim Ausführen |  |
|  | seine IP-Adresse bezieht, | Adresse vom DHCP- | des Commands «ip | des Commands «ip |  |
|  | erhält dynamisch eine IP- | Server. Danach wird mit | a» ist ersichtlich | a» ist ersichtlich |  |
|  | Adresse in der | dem Command ***ip a*** die | das die IPv4- | das die IPv4- |  |
|  | vorgegebenen Range. | aktuelle IP-Konfiguration | Adresse des | Adresse des |  |
|  |  | eingesehen. | Clients zwischen | Clients zwischen |  |
|  |  |  | **192.168.11.1** und | **192.168.11.1** und |  |
|  |  |  | **192.168.11.20** | **192.168.11.20** |  |
|  |  |  | liegt. | liegt. |  |
|  | Auch hier konnte ich den Testfall wie geplant umsetzen. Dafür musste ich lediglich die korrekte IP-Range | | | | |
|  | in der Konfigurationsdaten vom DHCP-Server angeben, welche 192.168.11.1 – 192.168.11.20 beträgt. | | | | |