Inventarisierung – IP-Scan

Inventarisierung von IP Systemen

TITEL	Inventarisierung – IP-Scan
AUTOR	Docusnap Consulting
DATUM	07.10.2019
VERSION	1.0 | gültig ab 07.10.2019

INHALTSVERZEICHNIS

1. Einleitung

Der IP-Scan in Docusnap liefert Ihnen die Möglichkeit, Ihr Netzwerk oder das eines Kunden umfangreich nach aktiven Systemen zu durchsuchen. Alles was Sie für diesen ersten Überblick, oder der Überprüfung auf eine vollständige Inventarisierung benötigen, sind die relevanten IP Adressbereiche. Für den IP-Scan werden keinerlei Anmeldeinformationen oder Community Strings verwendet. Auf diesem Weg können Sie ein neues Netzwerk sehr schnell und einfach inventarisieren und sich dabei einen Überblick verschaffen.

In Ihrem eigenen Netzwerk können Sie auf diesem Weg jene aktiven Komponenten erfassen, die Sie mit einem detaillierteren Scan noch nicht erfasst haben. Gründe hierfür können u.a. sein, dass das System nicht bekannt ist oder die nötigen Anmeldeinformationen fehlen.

Dieses HowTo beschreibt die Nutzung des IP-Scans und ist in folgende Kapitel unterteilt:

- In Kapitel 1 wird die Notwendigkeit und Installation des NPCAP Treibers erklärt
- In Kapitel 2 wird der eigentliche IP-Scan beschrieben
- In Kapitel 3 wird gezeigt, wie Sie NMAP Parameter testen und anschließend in Docusnap übertragen können
- In Kapitel 4 werden Anwendungsfälle und Praxisbeispiele genannt

1.1 Docusnap IP-Scan

Docusnap unterscheidet zwischen einem normalen und dem erweiterten IP-Scan. Beide IP-Scans funktionieren auf Basis von **NMAP (Network Mapper)**. Der normale IP-Scan verwendet Funktionen wie SYN-ACK, ARP-Request, ICMP Anfragen und eine Namensauflösung. Antwortende Systeme werden mit rudimentären Netzwerkinformationen erfasst.

Durch die Verwendung spezieller NMAP Parameter ist es dem erweiterten IP-Scan möglich zusätzliche Informationen, wie z. B. das Betriebssystem, zu erkennen.

Voraussetzung für den erweiterten IP-Scan ist die Installation des **NPCAP Treibers** auf dem inventarisierenden System.

1.2 Installation des NPCAP Treibers

Wichtig: Die Installation des NPCAP Treibers ist keine Voraussetzung für den erfolgreichen Abschluss der Docusnap Installation. Ein erweiterter IP-Scan ist jedoch nur mit einem installierten NPCAP Treiber möglich.

Bei einer Neuinstallation von Docusnap wird Ihnen die Installation des NPCAP Treibers während der Setup Routine angeboten. Diese ist optional und kann von Ihnen aktiviert werden.

Einen IP-Scan kann sowohl Server, Client als auch ein Docusnap Discovery Service durchführen. Dementsprechend enthält das Setup für den Docusnap Discovery Service ebenfalls die Option zur Installation des NPCAP Treibers.

Führen Sie Ihr Docusnap Update über die Update Funktion innerhalb des Programms aus, so wird keine NPCAP Installation angeboten.

1.2.1 Gefahren und Schwierigkeiten

Voraussetzung für die Installation eines zusätzlichen Netzwerkadapters und des NPCAP Treibers sind lokale Administrator Rechte.

Bei der Installation des NPCAP Treibers ist zu beachten, dass ein zusätzlicher Netzwerkadapter hinzugefügt wird. Der Eingriff in das System kann daher massiv sein. Speziell bei Systemen wie z. B. einem Domänen Controller oder ähnlichem sollte eine Installation nicht leichtfertig durchgeführt werden.

Ebenfalls gilt zu beachten, dass eine Installation des NPCAP Treibers in Konkurrenz zu ähnlichen Netzwerktreibern stehen kann. Dies kann auch andere Versionen des NPCAP Treibers betreffen. So wird bei einer Wireshark Installation ebenfalls ein NPCAP Treiber installiert. Da bei Wireshark andere Installationsoptionen gesetzt sind, können sowohl bei Wireshark als auch Docusnap fehlerhafte Resultate das Ergebnis sein.

Weitere Informationen zu den Voraussetzungen und Problematiken bei z. B. Firewall und Monitoring finden Sie in unserem **Whitepaper Docusnap Inventarisierung** im Kapitel IP-Scan.

1.2.2 NPCAP nachträglich installieren

Eine nachträgliche Installation des NPCAP Treibers ist möglich. Hierzu können Sie die im Docusnap X Installationsordner vorhandene **npcap-oem.exe** verwenden. Alternativ können Sie ebenfalls das Setup von der Herstellerseite beziehen.

Der Standardpfad dieser Datei lautet:

\Program Files\Docusnap X\MSI\npcap-oem.exe

Beachten Sie bitte bei der nachträglichen Installation, dass die entsprechenden Optionen korrekt gesetzt sind.

Bei Remote Verbindungen kann es vorkommen, dass die Verbindung kurz unterbrochen wird.

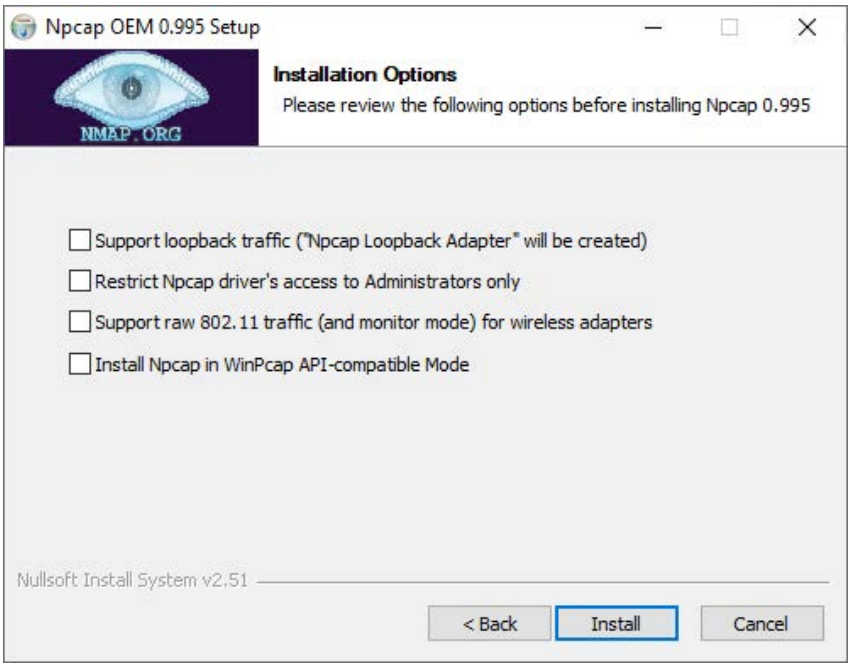


Abbildung 1 - NPCAP Setup

2. IP-Scan in Docusnap

2.1 IP-Scan-Assistent

Der IP-Scan ist ein eigenständiger Inventarisierungsassistent in Docusnap. Unterschieden wird zwischen dem **Einfachen IP-Scan** und dem **Erweiterten IP-Scan**. Die Auswahl kann im Verlauf des Assistenten mittels einer Checkbox getroffen werden.

IP-Scan

Der IP-Scan prüft mittels ICMP Anfragen die Adressen. Antwortet das angefragte System wird es als IP-System erfasst und mit zusätzlichen Informationen in der Datenbank gespeichert (Scandatum, IP-Adresse und Subnetzmaske). Zusätzlich versucht der IP-Scan den zugehörigen DNS Namen aufzulösen. Ist dies erfolgreich, wird das System mit dem DNS Namen erfasst.

Erweiterter IP-Scan

Mit Hilfe des Erweiterten Modus werden zusätzlich MAC-Vendor, Informationen zum Betriebssystem, Betriebszeit und der letzte Systemstart erfasst. Eine Genauigkeitsangabe der erfassten Informationen wird in Prozent angegeben. Dies kommt daher, dass NMAP das Betriebssystem etc. nicht immer zu 100% bestimmen kann. Anhand der Reaktion auf abgesetzte Anfragen schätzt NMAP diese Informationen ab.

Wird der Erweiterte IP-Scan aktiviert, so sucht Docusnap nach dem benötigten NPCAP Treiber. Ist dieser nicht vorhanden, kann der Erweiterte IP-Scan nicht verwendet werden.

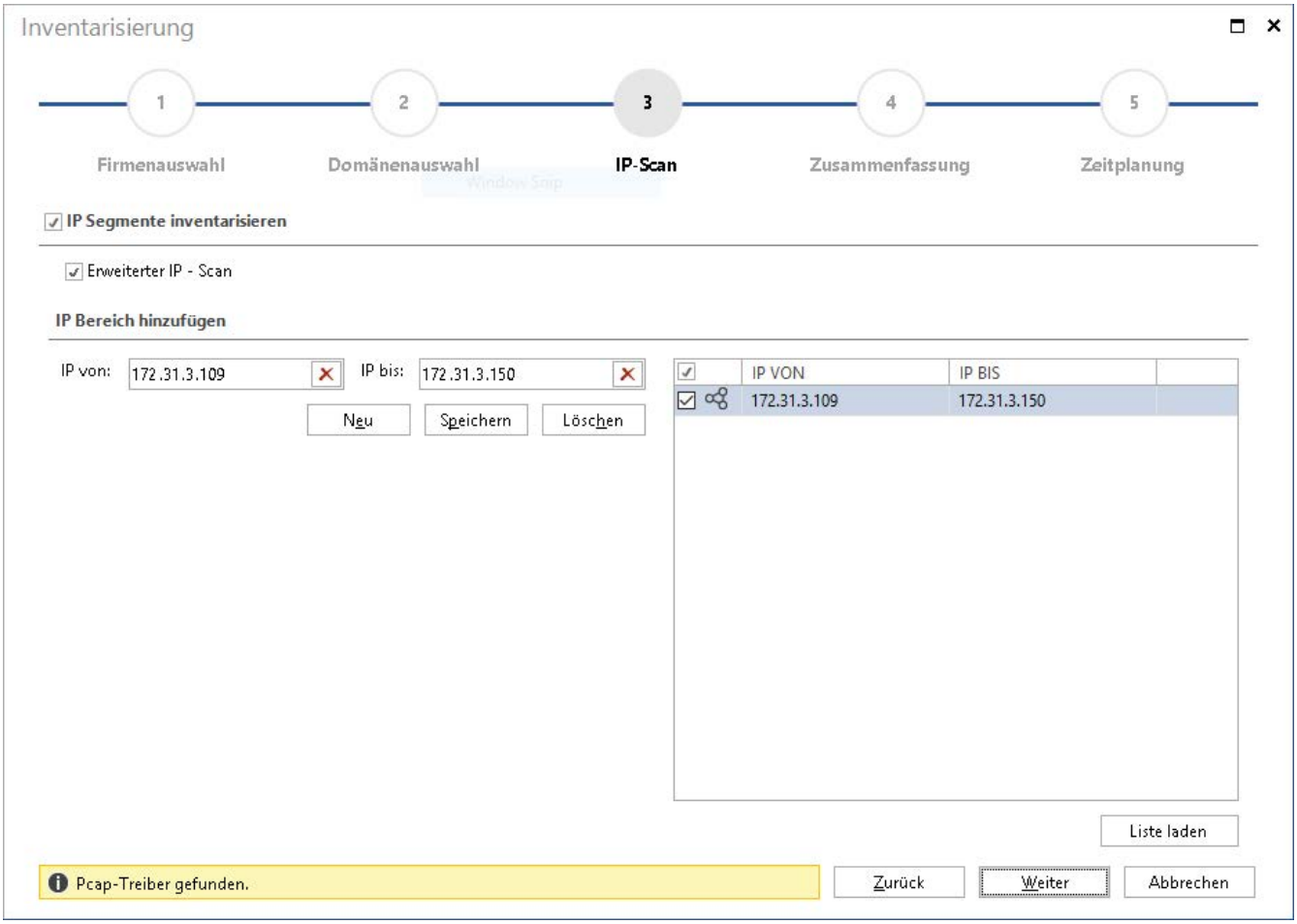


Abbildung 2 - IP-Scan Assistent

Möchten Sie mehrere Netze zur Inventarisierung angeben empfiehlt sich die Verwendung des CSV Imports. Diesen können Sie über **Liste laden** aufrufen. In nachfolgender Abbildung wird der Aufbau der CSV Datei beschrieben.

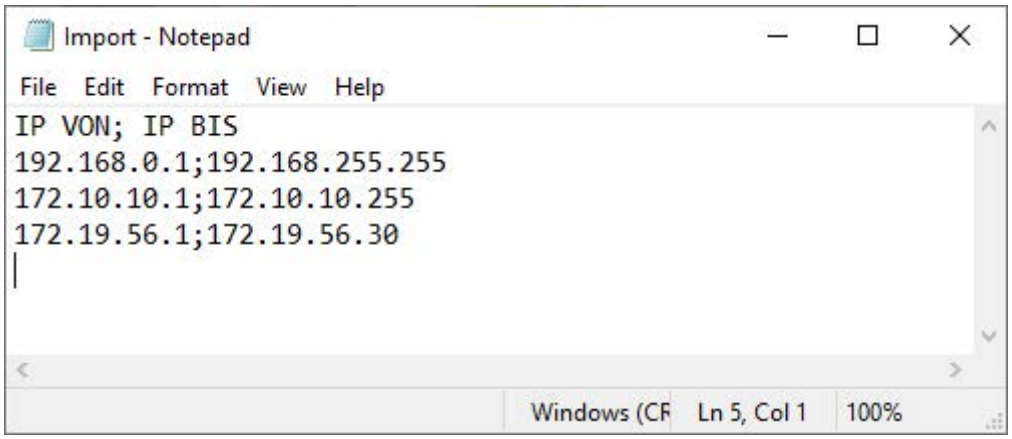


Abbildung 3 – IP-Bereiche - CSV Import

Die maximale Größe eines Netzsegments ist auf Class B (192.168.1.1 – 192.168. 255.255) beschränkt.

2.2 Analyse und Ergebnis

Die Ergebnisse Ihres IP-Scans finden Sie im Datenbaum von Docusnap unter Firma – Infrastruktur – Domäne – IP Systeme

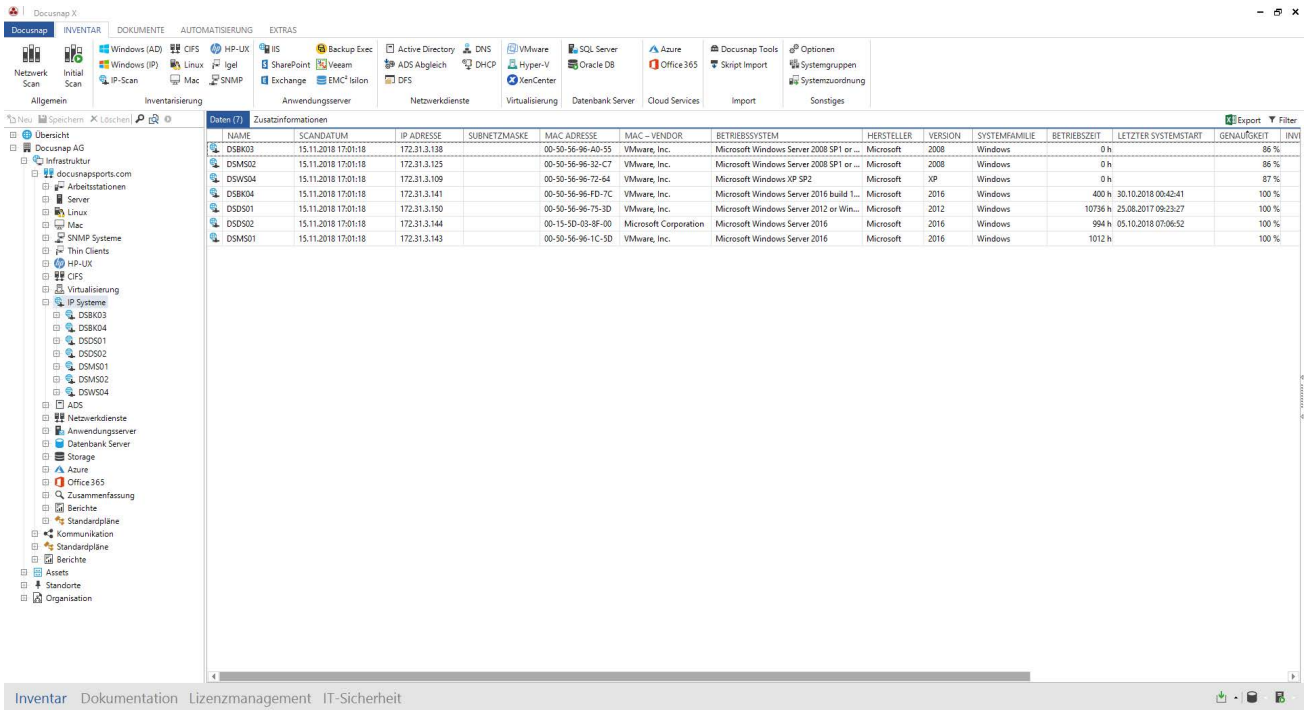


Abbildung 4 - Ergebnisse des Erweiterten IP-Scans

Überblick der Informationen die erfasst werden können:

- Name: Name des Systems. Wenn ein DNS Eintrag vorhanden ist, wird dieser als Name verwendet, ansonsten die IP-Adresse.
- Scandatum: Zeitpunkt, wann das System das letzte Mal per IP-Scan erfasst wurde
- IP-Adresse: IP-Adresse des Systems
- Subnetzmaske: Subnetzmaske des Systems
- MAC Adresse: MAC Adresse des Systems
- MAC-Vendor: Hersteller – Ergibt sich aus der erfassten MAC Adresse
- Betriebssystem: Information zu dem verwendeten Betriebssystem
- Hersteller: Hersteller des Betriebssystems
- Version: Versionsnummer des Betriebssystems
- Systemfamilie: Familie, z. B. Windows oder Linux
- Betriebszeit: Zeitangabe in Stunden
- Letzter Systemstart: Datum, wann das System das letzte Mal neu gestartet wurde
- Genauigkeit: Angabe zur Genauigkeit der erweiterten Informationen in Prozent

Mit Hilfe der erweiterten Informationen wie z. B. dem MAC-Vendor und Informationen zum Betriebssystem kann sich ein allgemeiner Überblick über das Netzwerk verschafft werden. Anschließend können die Systeme einem Assistenten für die weitere Inventarisierung zugeordnet werden.

IP-Systeme werden sowohl in Berichten, als auch im Netzwerk- und Topologie Plan berücksichtigt.

2.3 MAC Filter für IP-Systeme

Manche Systeme können nur via IP-Scan erfasst werden, da keine andere Standard Schnittstelle, z. B. SNMP unterstützt wird. Damit diese Systeme im Topologie Plan als z. B. Telefone dargestellt werden können, steht Ihnen ein MAC Filter zur Verfügung. Dadurch wird Ihnen die Unterscheidung der IP-Systeme im Topologie Plan erleichtert.

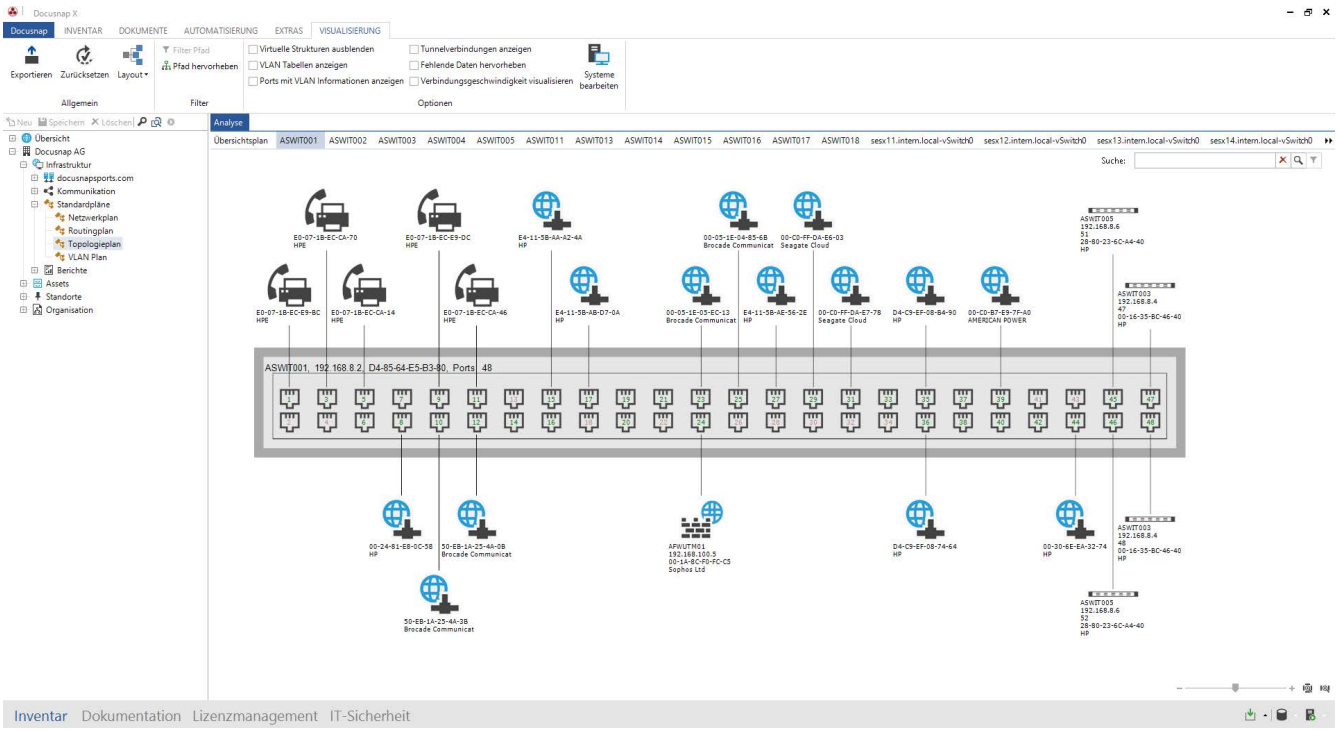


Abbildung 5 - MAC Filter bei IP-Systemen

Vorgehensweise:

- Identifizieren sie den kleinsten gemeinsamen Nenner bei der MAC Adresse. Bei zwei IP-Telefonen mit jeweils einer MAC Adressen **E0-07-1B-EC-CA-70** und **E0-07-1B-EC-E9-DC** wäre der kleinste gemeinsame Nenner **E0-07-1B-**.
- Wechseln Sie in die Docusnap **Administration** – Reiter **Inventar** – **MAC Filter**
- Hinterlegen Sie dort die MAC Adresse – **E0-07-1B-**
- Unterstützte Wildcard Zeichen sind ***** um mehrere beliebige Zeichen und **?** um genau ein beliebiges Zeichen anzugeben.

MAC Adressen vom Typ Ignorieren und Virtuell werden im Topologie Plan anschließend nicht mehr dargestellt.

Weitere Informationen zum MAC Filter finden Sie im Docusnap Handbuch im Bereich MAC Filter. (F1 Taste im entsprechenden Bereich innerhalb der Docusnap Administration) oder im HowTo **Inventarisierung und Auswertung von SNMP** in der **Docusnap Knowledge Base**.

3. Optional: IP-Scan Analyse-Tool

Das IP-Scan Analyse-Tool erhalten Sie auf Anfrage beim Docusnap Support.

3.1 Verwendungszweck

Jedes Netzwerk ist anders. Somit kann es vorkommen, dass der IP-Scan in seltenen Fällen keine bzw. mangelhafte Ergebnisse liefert. Ursache kann hierfür der Virenscanner, die Konfiguration der Firewall oder auch ein Proxy sein. Verschiedenste Netzwerkkomponenten können sich auf die Ergebnisse des IP-Scans auswirken. Der Docusnap IP-Scan verwendet im Standard Parameter, welche bei einem Großteil der Netzwerke erfolgreich Daten inventarisiert. Damit Sie auch in Ihrem Netzwerk die besten Ergebnisse mit dem IP-Scan erhalten, haben Sie die Möglichkeit mit Hilfe des IP-Scan Analyse-Tools die für Sie richtigen NMAP Parameter herauszufinden. Anschließend können Sie diese an Docusnap übergeben.

Das IP-Scan Analyse-Tool ist eine eigenständige Applikation. Es wird keine Docusnap Installation vorausgesetzt. Voraussetzung ist die Installation des NPAC Treibers.

Für eine bestmögliche Analyse sollten Sie das IP-Scan Analyse-Tool auf demselben System ausführen, auf dem der Docusnap IP-Scan ebenfalls ausgeführt wird, z. B. Docusnap Server oder Docusnap Discovery Service.

Standard Parameter des Docusnap IP-Scans, Docusnap Version 10.0.1472.2:

```
-F -T3 -O --osscan-guess --script smb-os-discovery.nse
```

3.2 Anwendung des Test-Programms

Wenn Sie das IP-Scan Analyse-Tool mit einem Doppelklick starten, öffnet sich ein neues Fenster. Innerhalb dieser GUI können Sie einen IP-Scan durchführen, Parameter beeinflussen und anschließend die Ergebnisse analysieren.

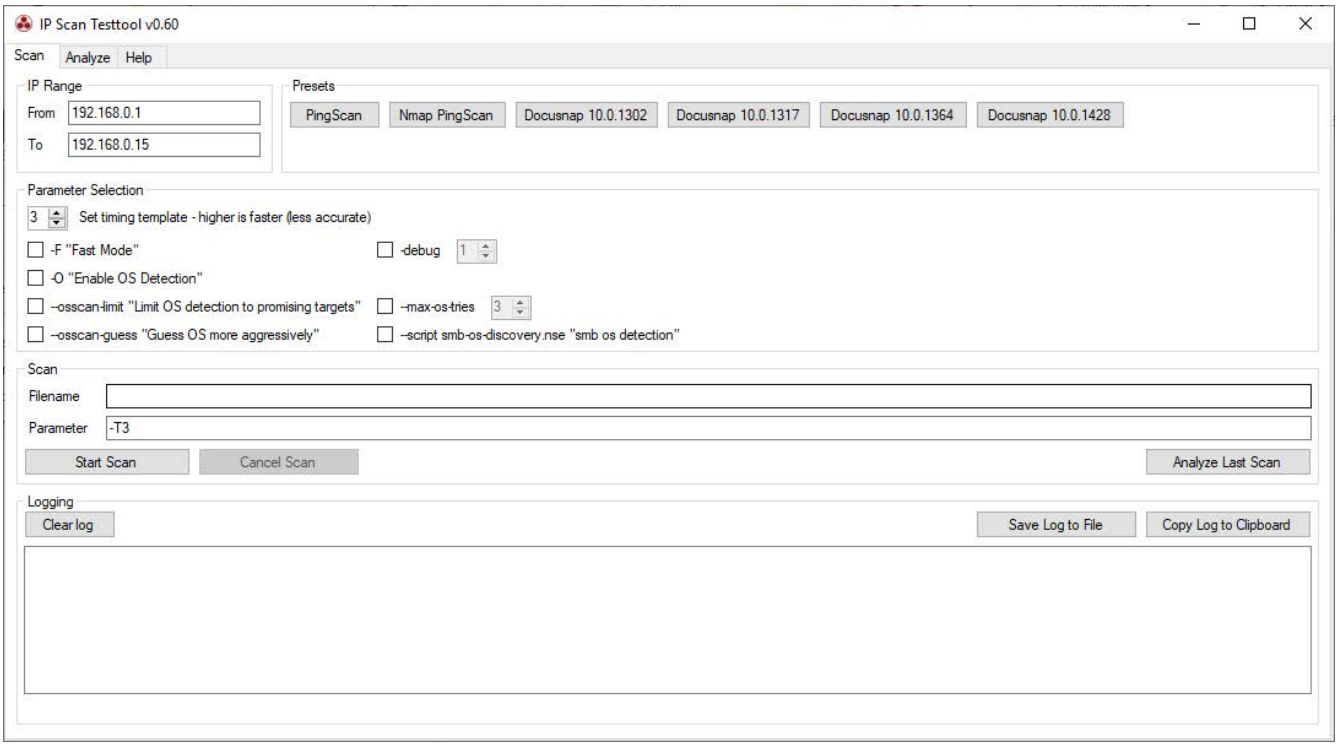


Abbildung 6 - IP-Scan Analyse-Tool GUI

Das Analyse-Tool ist in drei Bereiche unterteilt. **Scan**, **Analyse** und **Help**.

3.2.1 Scan

Innerhalb des **Scan** Bereichs ist es Ihnen möglich die Parameter Ihrem Netzwerk entsprechend anzupassen. Dabei können Sie ebenfalls auf **Presets** zurückgreifen. Die vorgegebenen Presets unterscheiden sich in den verwendeten Parametern. Dabei stehen Ihnen folgende Presets zur Verfügung:

- PingScan: Parameter –PE – Ping. (Echo-Reply wird erwartet)
- Nmap PingScan: Parameter –sP – einfacher IP-Scan in Docusnap
- Docusnap Version: Verwendet NMAP Parameter der jeweiligen Docusnap Version

Eine Anpassung der zu verwendenden Parameter können Sie unter **Parameter Section** durchführen. Parameter können mittels der Checkboxen ausgewählt oder über eine Texteingabe im Feld **Parameter** hinzugefügt werden. Eine detaillierte Übersicht aller verfügbaren NMAP Parameter finden Sie unter https://nmap.org/.

Im nachfolgenden Beispiel wird der Scan mit dem Preset der letzten Docusnap Version durchgeführt. Die Parameter werden automatisch mit einem Klick auf das jeweilige Preset gesetzt. Mit dem Button **Start Scan** wird dieser mit den angegebenen Parametern gestartet.

Die verwendeten Parameter sowie Pfadangabe der Logdatei finden Sie in den jeweiligen Textboxen. Logfiles werden in einem automatisch angelegten Ordner auf Ihrem Desktop gespeichert. Im Logging sehen Sie Informationen zum aktuellen Status des Scans.

Beispiel:
Um die Durchführung des IP-Scans zu beschleunigen wird die Geschwindigkeit erhöht, sowie die Maßnahmen zur Betriebssystemerkennung minimiert.

Beachten Sie, dass eine Erhöhung der Geschwindigkeit die Qualität der Ergebnisse beeinflussen kann.

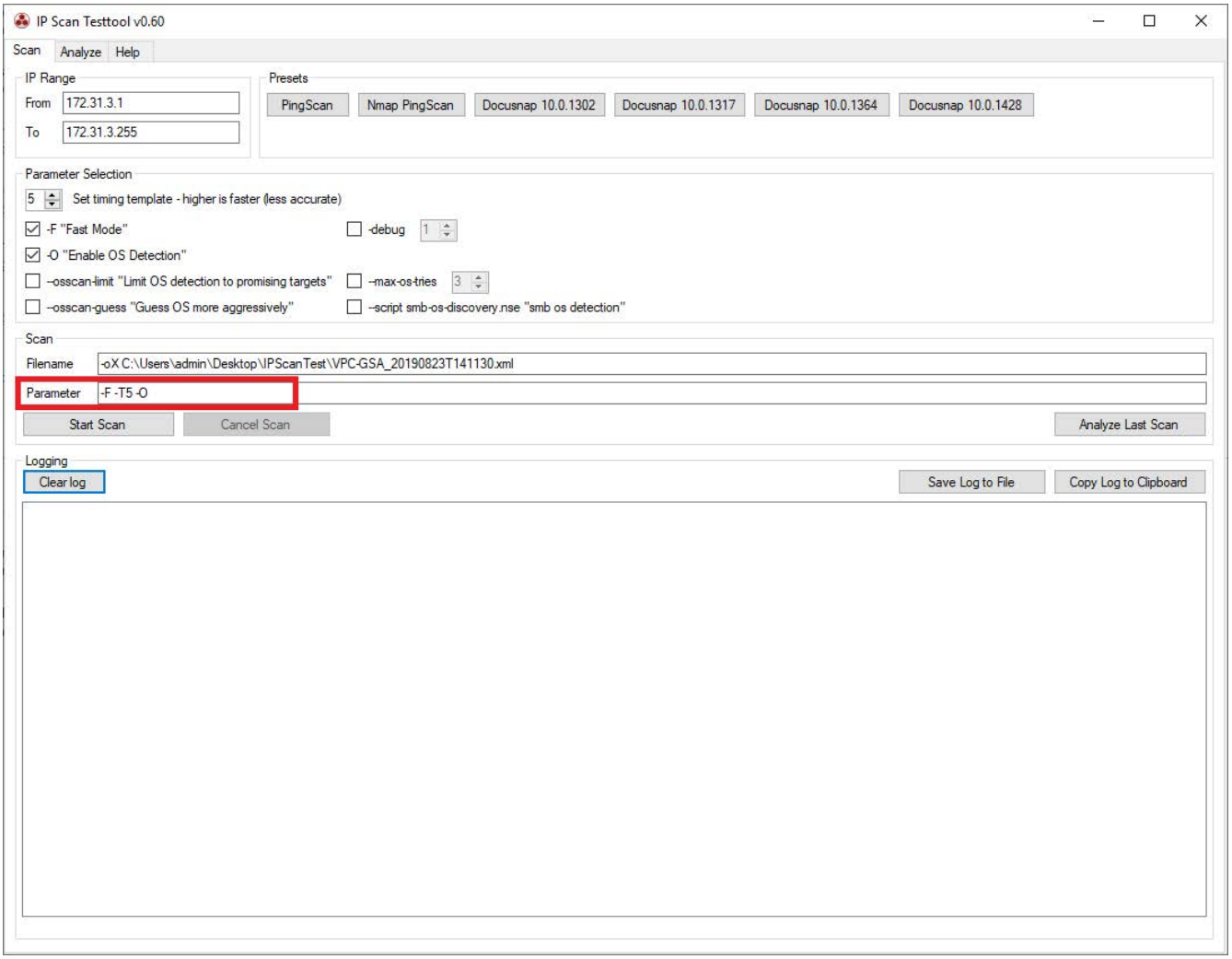


Abbildung 7 - IP-Scan Analyse-Tool Parameter anpassen

3.2.2 Analyse

Im **Analyse** Bereich können Sie die Ergebnisse Ihres letzten, oder von vorherigen Scans auswerten. Genauere Informationen zur Analyse finden Sie im nachfolgenden Kapitel Ergebnisse analysieren

3.2.3 Hilfe

Innerhalb des **Help** Tabs finden Sie weitere Informationen zu den **Timing-Einstellungen** sowie zur **Analyse**.

3.3 Übertragung in Docusnap

3.3.1 Ergebnisse analysieren

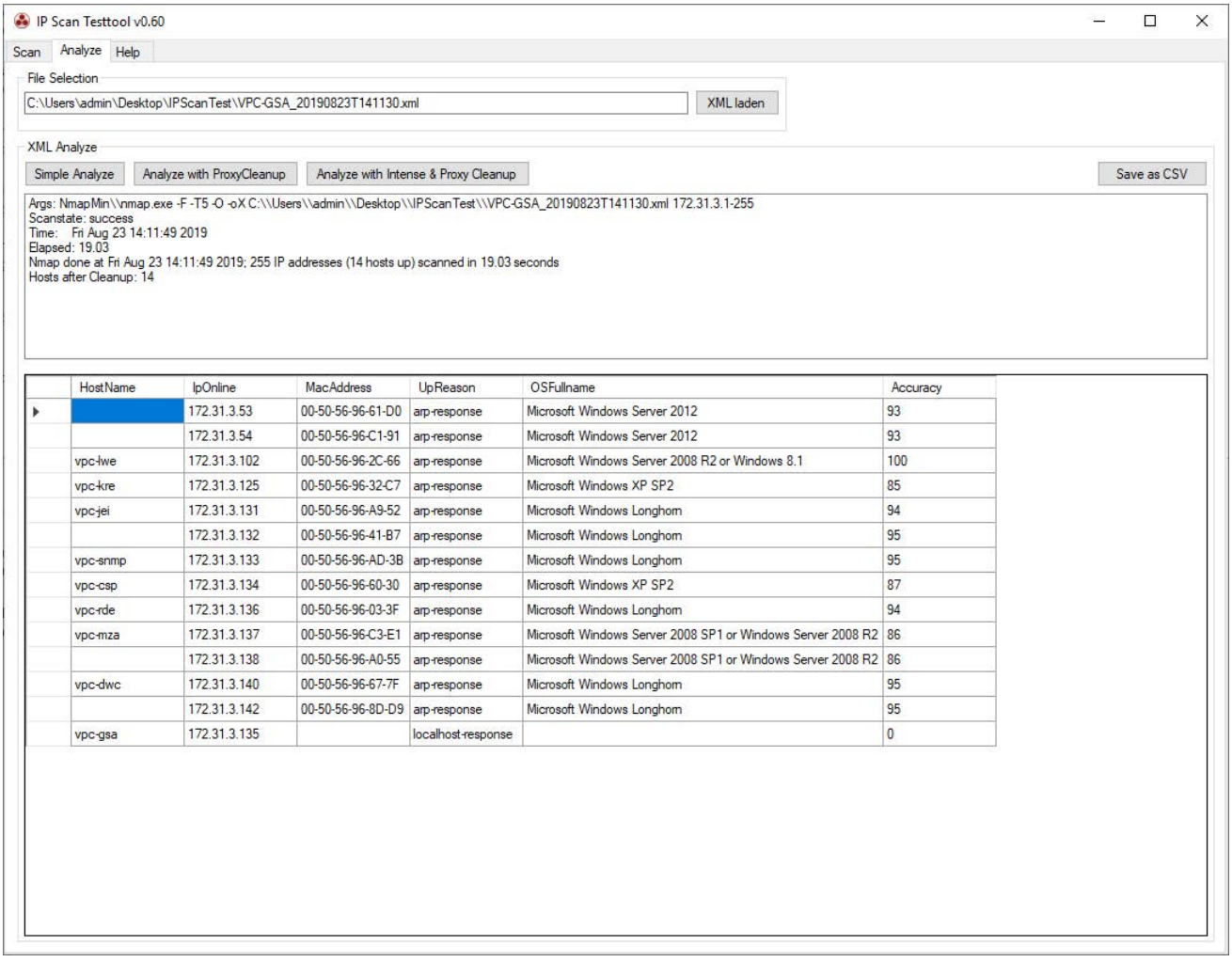
Im Analyse-Bereich können Sie die Ergebnisse Ihrer Scans anschließend auswerten. Im Standard öffnet das IP-Scan Analyse-Tool den letzten durchgeführten Scan. Möchten Sie einen bestimmten Scan auswerten, können Sie über **File Selection** die gewünschte .xml Datei in das Analyse-Fenster laden.

Unterschieden wird zwischen der **einfachen Analyse** und der **Analyse mit Cleanup.**

Bei der **einfachen Analyse** werden lediglich die Ergebnisse aus dem Scan ausgewertet. Falsch erkannte Hosts, z. B. ausgelöst durch einen transparenten Proxy, werden hierbei nicht gefiltert.

Bei einer **Analyse mit Cleanup** werden die erkannten Hosts anschließend auf dieselbe Weise wie in Docusnap gefiltert. Damit wird versucht fälschlicherweise als positiv erkannte Hosts herauszufiltern. Bei Netzwerken mit einem transparenten Proxy kann es vorkommen, dass dieser auf jede Anfrage des IP-Scans antwortet. Somit werden alle Adressen als positiv erkannt. Mit Hilfe der Cleanup Funktion werden die falsch erkannten Systeme herausgefiltert. Die Ergebnisse Ihres Scans können Sie anschließend im Analyse-Fenster sehen und z. B. in eine CSV Datei exportieren.

Entsprechen die Resultate des Scans den Systemen Ihres Netzwerks, können Sie anschließend die von Ihnen gesetzten Parameter an Docusnap übergeben.



HostName	IpOnline	MacAddress	UpReason	OSFullname	Accuracy
	172.31.3.53	00-50-56-96-61-D0	arp-response	Microsoft Windows Server 2012	93
	172.31.3.54	00-50-56-96-C1-91	arp-response	Microsoft Windows Server 2012	93
vpc-lwe	172.31.3.102	00-50-56-96-2C-66	arp-response	Microsoft Windows Server 2008 R2 or Windows 8.1	100
vpc-kre	172.31.3.125	00-50-56-96-32-C7	arp-response	Microsoft Windows XP SP2	85
vpc-jei	172.31.3.131	00-50-56-96-A9-52	arp-response	Microsoft Windows Longhorn	94
	172.31.3.132	00-50-56-96-41-B7	arp-response	Microsoft Windows Longhorn	95
vpc-snmp	172.31.3.133	00-50-56-96-AD-3B	arp-response	Microsoft Windows Longhorn	95
vpc-csp	172.31.3.134	00-50-56-96-60-30	arp-response	Microsoft Windows XP SP2	87
vpc-rde	172.31.3.136	00-50-56-96-03-3F	arp-response	Microsoft Windows Longhorn	94
vpc-mza	172.31.3.137	00-50-56-96-C3-E1	arp-response	Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2	86
	172.31.3.138	00-50-56-96-A0-55	arp-response	Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2	86
vpc-dwc	172.31.3.140	00-50-56-96-67-7F	arp-response	Microsoft Windows Longhorn	95
	172.31.3.142	00-50-56-96-8D-D9	arp-response	Microsoft Windows Longhorn	95
vpc-gsa	172.31.3.135		localhost-response		0

Abbildung 8 - Ergebnisse des IP-Scan Analyse-Tools

3.3.2 Anpassung der Docusnap IP-Scan Konfiguration

Die NMAP Parameter für den IP-Scan werden in der **DocusnapSettings.xml** durchgeführt. Zu beachten ist, dass diese Anpassung auf jedem System durchgeführt werden muss. Haben Sie z. B. mehrere Docusnap Discovery Services im Einsatz, muss auf dem jeweiligen System die DocusnapSettings.xml angepasst werden.

Sind keine Parameter gesetzt, verwendet der Docusnap IP-Scan automatisch die Parameter der jeweiligen Docusnap Version.

Im Standard finden Sie die DocusnapSettings.xml auf dem Docusnap-/ bzw. Docusnap Discovery Service Hostsystem in folgendem Verzeichnis:

C:\ProgramData\Docusnap\DocusnapSettings.xml

Mit einem Texteditor, z. B. Notepad, können Sie die DocusnapSettings.xml bearbeiten.

Innerhalb der <ApplicationSettings> Tags werden die neuen Tags eingefügt. Zwischen den <ExtendedScan> Tags können Sie anschließend Ihre Parameter hinterlegen.

NMAP Parameter Tags für DocusanpSettings.xml:

```
<NmapSettings>
   <ExtendedScan></ExtendedScan>
</NmapSettings>
```

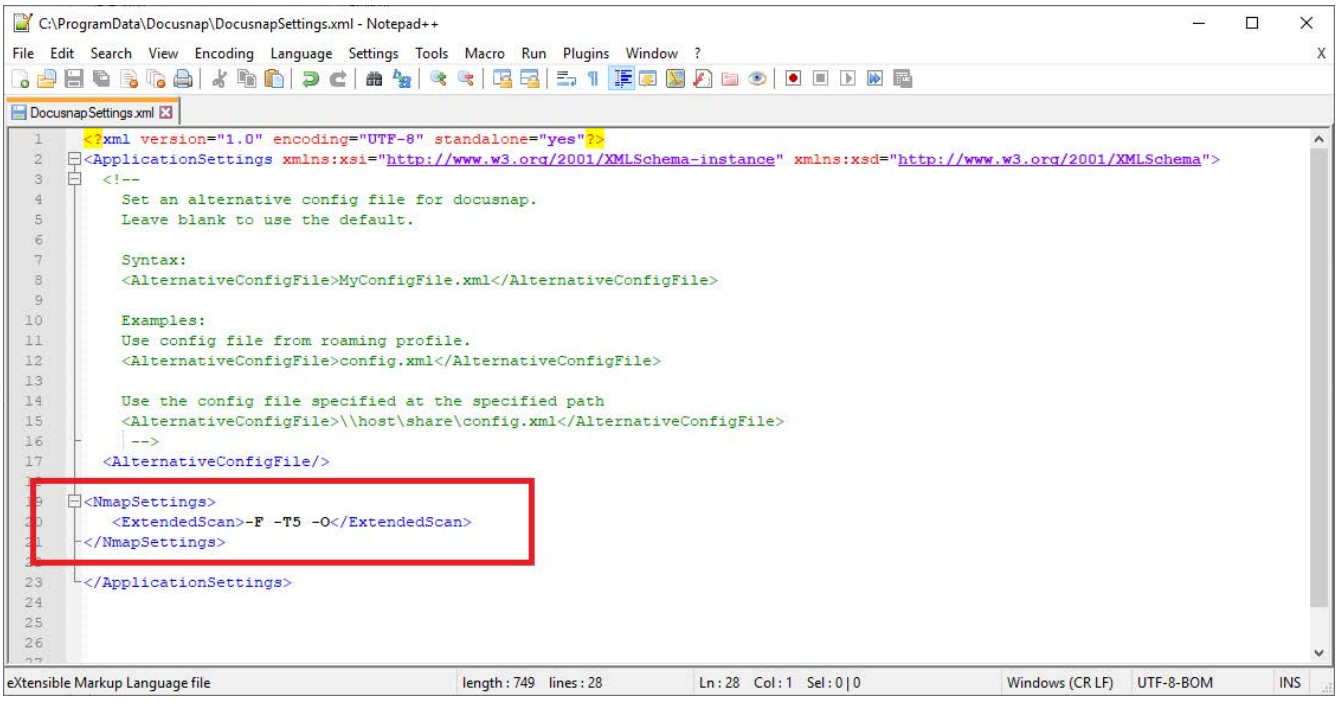


Abbildung 9 - NMAP Parameter in Docusnap - DocusanpSettings.xml

4. Anwendungsfälle und Praxisbeispiele

4.1 Erstinventarisierung

Eine vollständige und detaillierte Inventarisierung einer Netzwerkumgebung ist nur mit ausreichend privilegierten Benutzern möglich. Oftmals hat die inventarisierende Person bei einem neuen Kunden weder einen root Zugang zu Linux Systemen noch einen administrativen Zugang zu den Windows Systemen zur Verfügung. Trotzdem wird von dem Netzwerk ein erster Überblick benötigt.

Mit Hilfe des erweiterten IP-Scans können Sie die gewünschten Netzwerke analysieren, ohne dass administrative Rechte benötigt werden. Dabei können Sie herausfinden, wie viele Systeme vorhanden sind. Mit Hilfe der Betriebssysteminformationen ist anschließend eine Unterteilung in entsprechende Kategorien möglich.

- ➔ Anzahl der Windows Systeme
- ➔ Anzahl der Linux Systeme
- ➔ Anzahl der möglichen SNMP Systeme
- ➔ Etc.

4.2 Erhöhen der Datenqualität

Voraussetzung für eine qualitativ hochwertige Dokumentation ist eine gute Datenqualität in Docusnap. Da oftmals keine Übersicht der bestehenden Systeme vorhanden ist, ist ein Gegenprüfen der inventarisierten Systeme nicht möglich. Mit Hilfe des IP-Scans ist es Ihnen möglich eine Übersicht mit noch unbekannten Systemen zu erstellen und gezielt zu erfassen.

Ausgangssituation:
Alle Drucker des Unternehmens befinden sich im Netz XYZ. Dieses Netz wird bereits regelmäßig per SNMP inventarisiert. Um sicher zu gehen, dass wirklich alle Systeme innerhalb des Netzes erfasst werden, wird zusätzlich noch regelmäßig der IP-Scan eingesetzt.

Sind in diesem Fall Geräte noch nicht in Docusnap erfasst, werden diese nun zu den IP-Systemen hinzugefügt.

Anschließend sollten Sie die erfassten IP-Systeme bezüglich der SNMP Schnittstelle prüfen.

Werden diese Systeme zukünftig als SNMP Systeme erfasst, wird der Eintrag unterhalb der IP-Systeme verschoben. Eine Herabstufung hingegen ist nicht möglich – z. B. SNMP zu IP-System.

4.3 Sicherheitslücken erkennen

Bring your own Device, alte Netzwerkkomponenten und Internet of Things. Oftmals werden diese Systeme in Verbindung mit Sicherheitslücken gebracht. Nachfolgend wird Ihnen beschrieben, wie Sie mittels des Docusnap IP-Scans Sicherheitslücken erfassen, dokumentieren und darauf reagieren können.

Alte Netzwerkkomponenten erkennen:

In einem wachsenden Netzwerk kommt es im Laufe der Zeit vor, dass immer mehr alte Systeme vorhanden sind. Je nach Funktion kann dadurch eine Sicherheitslücke entstehen. Unterstützen diese Systeme als Schnittstelle nicht mindestens das SNMP Protokoll wird es schwierig diese zu erfassen, dokumentieren und entsprechend zu reagieren.

Mit Hilfe des IP-Scans können Sie einen regelmäßigen Scan Ihres Netzwerks durchführen. Ist z. B. noch ein alter Switch im Einsatz, wird dieser durch den IP-Scan erfasst. Dadurch vermeiden Sie z. B. den Ausfall Ihres Netzwerks aufgrund veralteter Hardware.

Bring your own Device / Internet of Thins

Die Aussage „Jeder neue Kühlschrank hat eine IP-Adresse" entspricht nicht ganz der Realität, trifft den Nagel jedoch auf den Kopf. Mit den Netzwerken eines Unternehmens sind verschiedenste Systeme verbunden. Von Arbeitsplatzrechnern, Servern, privaten Mobiltelefonen bis hin zu Systemen des Alltags ist alles dabei. Aufgrund der Sicherheit des Netzes werden diese oftmals in verschiedene Bereiche eingeteilt. Zu Sicherheitslücken kann es kommen, wenn die Kaffeemaschine plötzlich im selben VLAN wie die Switche verfügbar ist.

Um eine solche Fehlkonfiguration zu erkennen, bietet sich der IP-Scan an. Da alle aktiven Systeme im Netzwerk erfasst werden, finden Sie auch die Systeme des Alltags sowie die sonstigen Geräte und können deren Netzwerkkonfiguration prüfen.

ABBILDUNGSVERZEICHNIS

VERSIONSHISTORIE

Datum	Beschreibung
07.10.2019	Version 1.0 – Beschreibung des IP-Scans