Network Access Protection

mit Windows Server 2008

Ein Referat von

Marco Ullrich

Datum: **06.03.2010**

Inhaltsverzeichnis

1. Was ist Network Access Protection ?

Network Access Protection (NAP) dient der Determinierung des Zugriffgrades eines Clienten auf das LAN einer Organisation.
Die Clienten werden beim Verbindungaufbau mit dem LAN einer Intergritätsprüfung unterzogen. Clienten welche den Anforderungen nicht entsprechen werden ausgeschlossen oder im Netz isoliert.

Da die Dienste zur Integritätsprüfung Clientseitig durchgeführt werden ist NAP kein Schutz vor direkten Angriffen von Hackern, da diese die Clientseitigen Dienste manipulieren könnten. Es bietet vielmehr dem Administrator die Möglichkeit einen gewisses Level an Grundsicherheit für Clients festzulegen (z.B. das eine Firewall installiert ist und das Antivirenprogramm Up-to-date sein muss bevor ein Client Zugriff auf Netzwerkressourcen erlangt).

NAP ist ein Feature des Network Policy Services(NPS) und wird von Microsoft Windows XP (SP3), Vista, Windows 7 und Server 2008 unterstützt.

2. Konzeption

Der Client sendet einen Stautsbericht über eine Schnittstelle (Erzwingungspunkt) an einen NAP Server im Netzwerk sobald er eine Verbindung zum LAN aufbaut.

Dieser Server entscheidet anhand seiner definierten Integritätsrichtlinien wie die Schnittstelle mit dem Clienten verfahren soll.

Es beste die Möglichkeiten Clients den Zugriff auf das Netzwerk zu verbieten, sie in ein Wartungsnetzwerk zu isolieren, ihnen Vollzugriff zu gewähren oder lediglich Sie zu protokollieren.

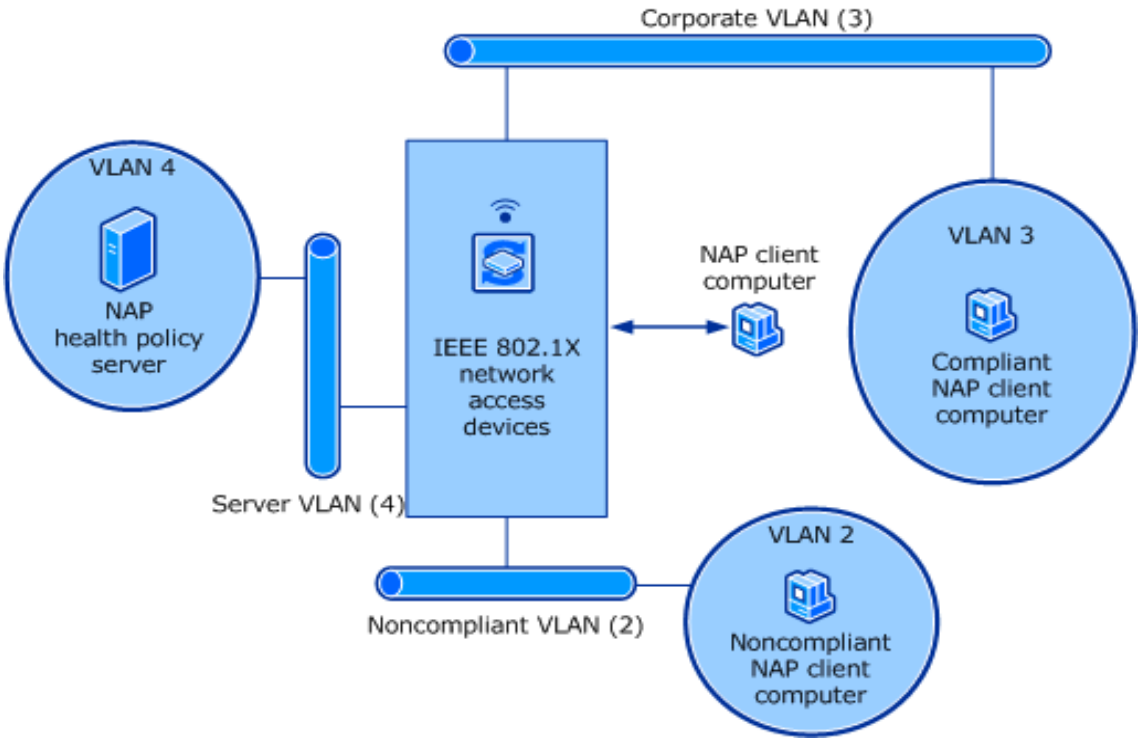
3. Varianten

3.1 802.1x

Die 802.1x Variante bietet die Möglichkeit der Selektion von Clienten anhand von Access Points und Ethernetswitches.

Man unterscheidet im Wesentlichen zwischen den Methoden:

- Zugriffslisten (ACL)
  - Ein Satz von IPv4 / IPv6 Paketfiltern
  - Separate ACL je PC.
- Virtual Local Area Network (VLAN)
  - Eine Gruppe von Ports welche ein Separates LAN bilden.
  - Infizierte Clients können hierbei untereinander kommunizieren!

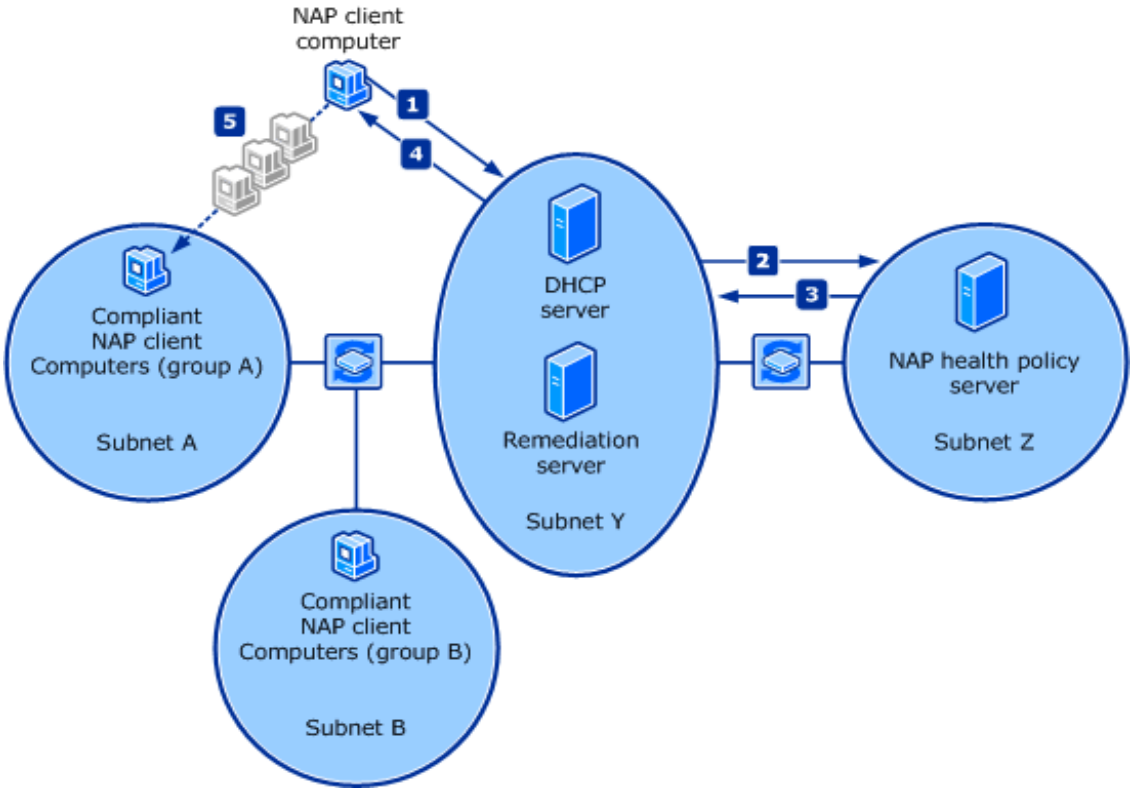


3.2 DHCP

Bei der DHCP Variante erfolgt die Selektion anhand der IP Adressvergabe.
Inkompatible Clienten bekommen ein IP-Adresse aus dem Pool des DHCP Servers zugewiesen, jedoch mit einer /32 Subnetzmaske. Desweiteren werden ihm statische Routen zum NAP Server sowie zu evtl. vorhandenen Wartungsservern zugewiesen. Der Client kann somit nur zu diesen eine Verbindung aufnehmen.

Das NAP DHCP Enforcement stellt die kostengünstigste und einfachste Variante dar.

Jedoch ist zu beachten dass diese Art der Selektion sehr einfach umgangen werden kann, indem Client seitig einfach eine statische IP mit entsprechender Subnetzmaske eingetragen wird.
Einen weiteren Nachteil stellt die Inkompatibilität zu IPv6 dar.



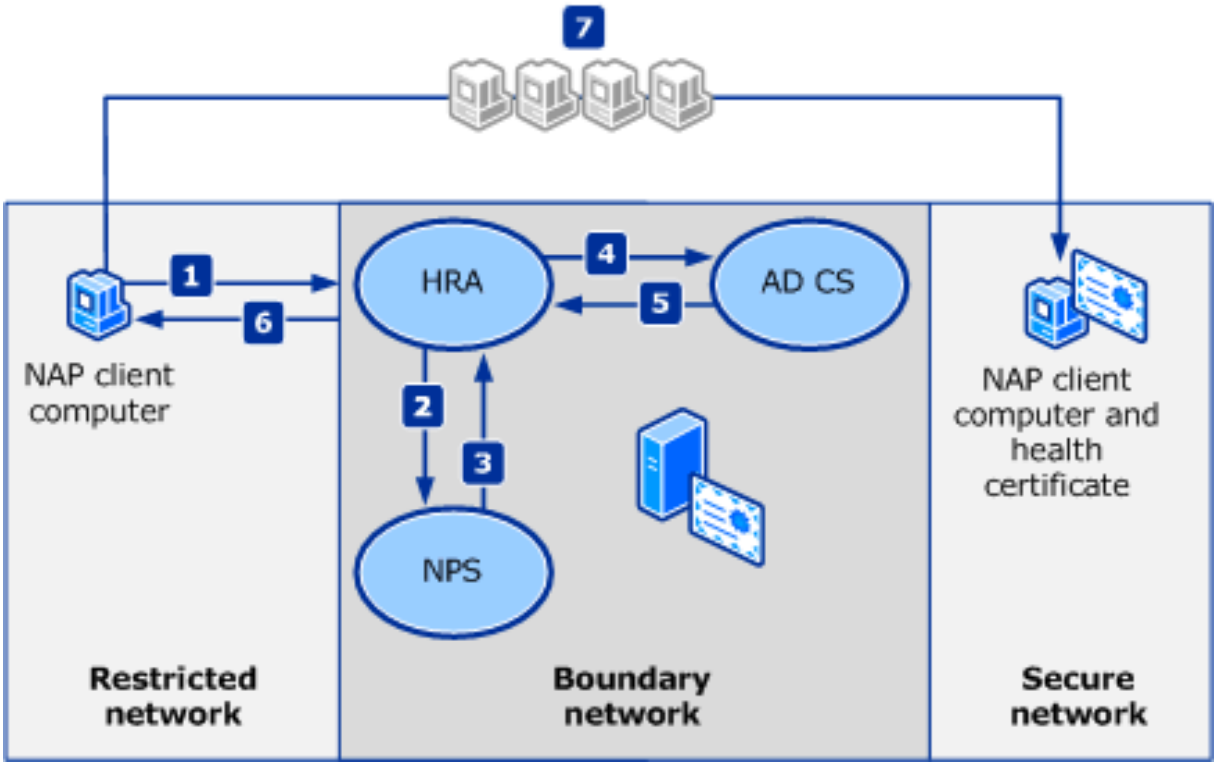
3.3 IPsec

Bei dieser Variante erhalten die Clienten, je nach Integritätsstatus unterschiedliche IPsec Zertifikate zugewiesen.

Der große Vorteil des IPsec Zugriffsverfahrens liegt darin, dass der Zugriff nicht nur auf bestimmte IP-Adressen, sondern auch auf Ports beschränkt werden kann. Zum Beispiel kann so einem Clienten Zugriff auf den Update-Dienst, jedoch nicht auf den FTP Dienst eines Servers gewährt werden.

Das NAP IPsec Enforcement stellt die sicherste und vielseitigste

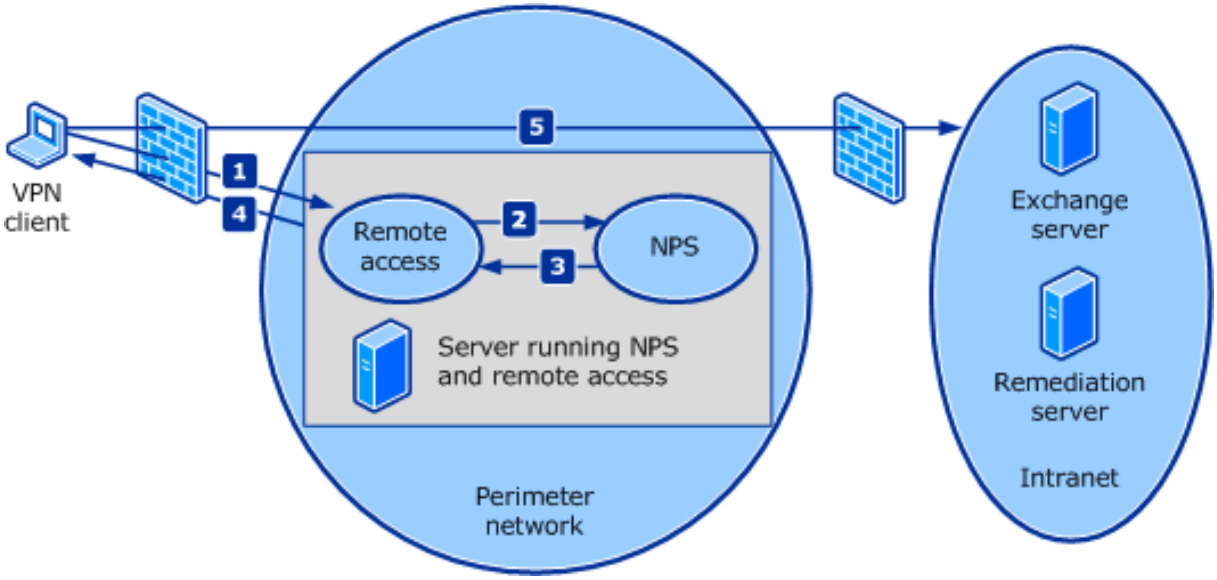
Implementierungsform dar. Ein Nachteil ist jedoch der größere administrative Aufwand, da eine Certification Authority für die Verwaltung und Vergabe der IPsec Zertifikate benötigt wird.



3.4 VPN

Hierbei baut der Client über Remote eine Verbindung zu einem VPN Server auf, welcher als Erzwingungspunkt dient.

Der VPN Server leitet den Clienten, entsprechend des Ergebnisses der Authentifizierung durch den NAP bzw. NPS in das entsprechende Netzwerk weiter.



4. Komponenten

4.1 System Health Agent

Die Erstellung des Integritätsberichtes des Clienten erfolgt durch den System Health Agent, kurz SHA.
Auf einem Clienten können ein, oder mehrere SHA installiert sein und parallel betrieben werden. Jeder dieser Agents ist für „einen Bereich“ zuständig.

Standardmäßig sind die Windows System Healt Agents (WSHA) installiert, diese überprüfen u.a. den Status des Sicherheitscenters (Firewall, Antivirensoftware u.v.m), so wie die Windows Updates. Momentan sind nur die WSHA`s verfügbar.

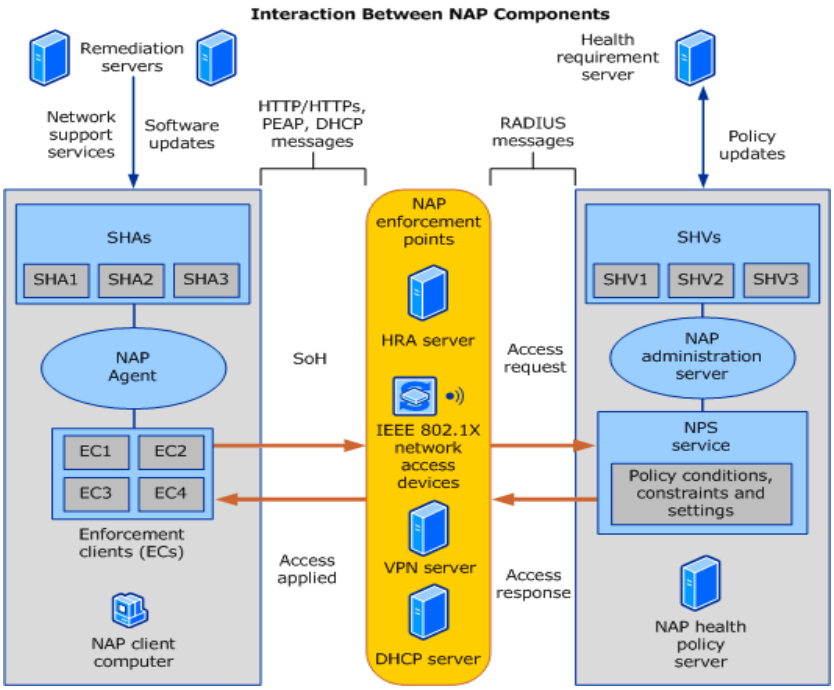
Ein SHA erstellt einen Statement of Health (SoH), welcher Informationen über den Status des Bereiches des SHA enthält.

4.2. System Health Validator

Der System Health Validator, kurz SHV, dient der Serverseitigen Analyse der Statement of Health des Clienten.

Jeder SHV wertet den SoH eines bestimmten System health Agents aus. Es können also, wie beim Clienten, mehrere SHV parallel agieren.

Nach der Auswertung des SoH erstellt jeder SHV einen Statement of Health Response (SoHR). Anhand dieses Berichtes stuft der NPS den Clienten entsprechend ein.



NAP-Agent: Dienst & Konfigurations-Schnittstelle der Clientseitigen NAP Komponenten.

EC: Enforcement Client. Schnittstelle zu den Erzwingungspunkten.

NAP enforcement points: NAP Erzwingungspunkte. Diese sind von der verwendeten NAP Varianten abhängig. Sie führen die Selektion des Clienten aus.

NPS: Network Policy Server. Wendet die Zugriffsrichtlinien an und verwaltet diese.

NAP administration Server: Network Access Protection Dienst & Konfigurationsschnittstelle.

Health requirement server: Updatet Richtlinien des NPS (z.B. wenn eine neue Antivirensignatur verfügbar ist).

Remediation Server: Wartungsserver für Updates.

5. Verbindungsprozess

a. Ein Client stellt eine Verbindung zu einem LAN her.

b. Jeder SHA überprüft das System und erstellt einen SoH, alle SoH werden zum System Statement of Health (SSoH) kombiniert.

c. Der SSoH wird über den Erzwingungspunkt an den NAP Server übermittelt.

d. Der NAP Server wertet den SSoH anhand seiner SHV aus.

e. Jeder SHV erstellt einen Statement of Health Response (SoHR) mit evtl. Wartungsanweisungen.

f. Die SoHR werden zu einem System Statement of Health Response (SSoHR) zusammengefasst.

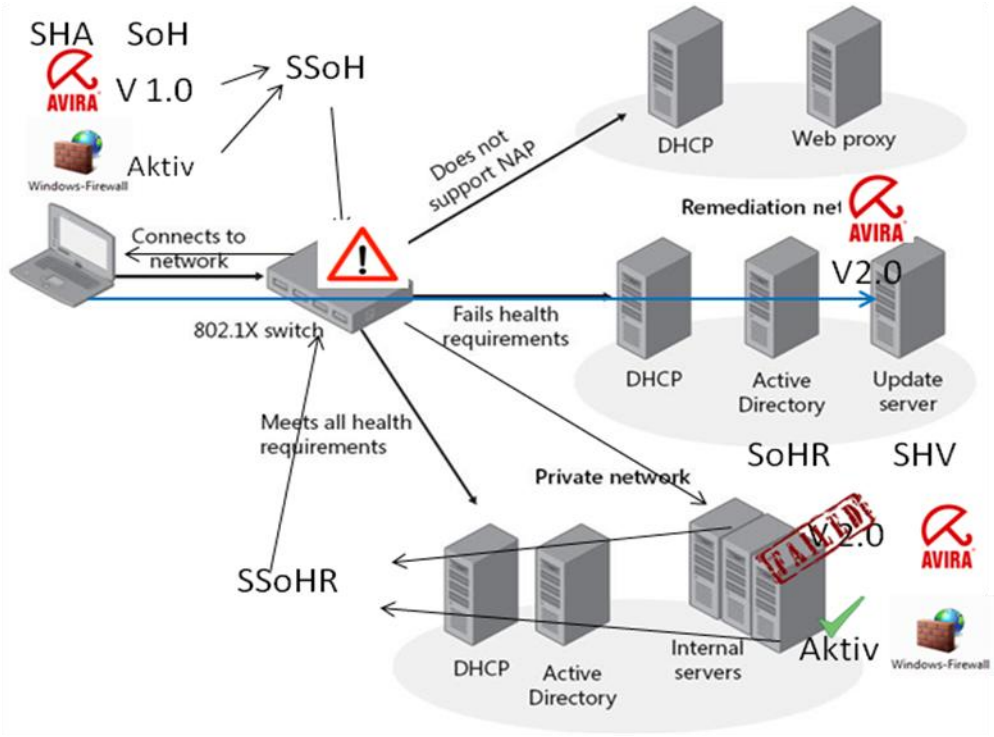
g. Der Server sendet den SSoHR über den Erzwingungspunkt an den Client zurück.

h. Anhand des Ergebnisses wird der Client vom Erzwingungspunkt mit dem LAN bzw. dem Wartungsnetzwerk verbunden.

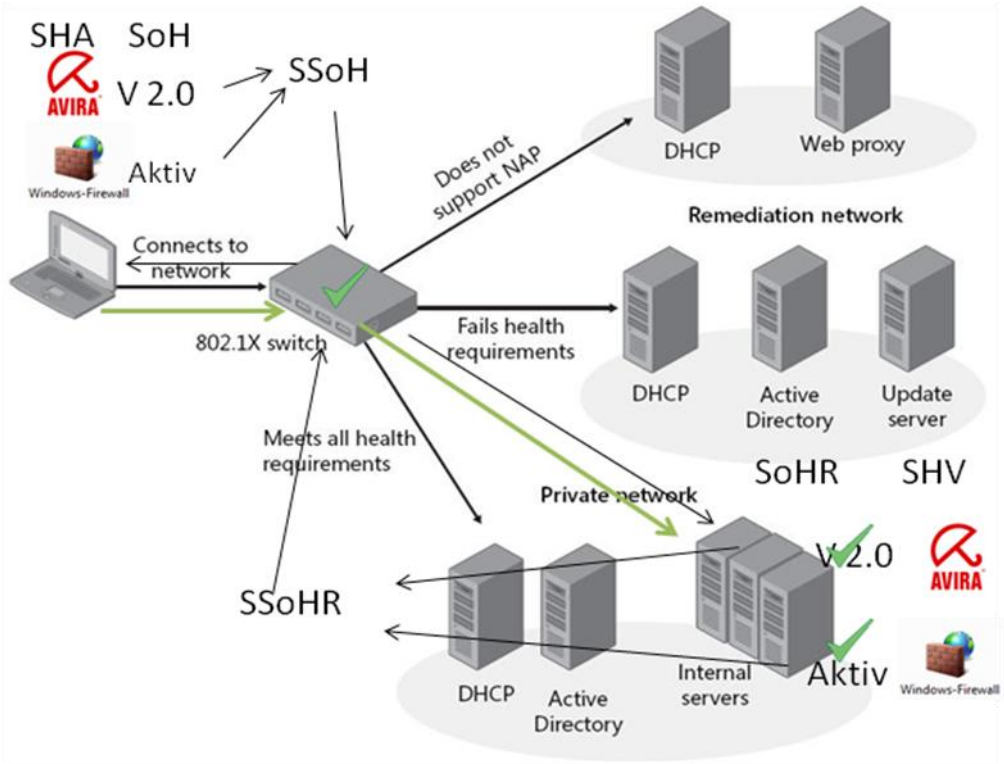
i. Die SHA verarbeiten den SoHR.

j. Falls es möglich ist versuchen inkompatible SHA die Integritätsanforderungen zu erfüllen.

k. Erneuter Authentifizierungsversuch.



Beispiel 1: Der Client besteht die Authentifizierung nicht und wird in einem Wartungsnetzwerk zugeteilt um sich zu aktualisieren.



Beispiel 2: Der Client erfüllt die Anforderungen.

6. Logs

Serverseitig befinden sich die Logfiles unter:

Ereignisanzeige -> Windows-Protokolle -> Sicherheit

Beispiel Log einer erfolgreichen Authentifizierung.

Clientseitig sind die Logfiles unter folgendem Pfad zu finden:

Ereignisanzeige -> Anwendungs- und Dienstprotokolle -> Microsoft -> Windows -> Network Access Protection -> Operational

7. How-To:

Integration des DHCP NAP Enforcement in eine bestehende Umgebung

(Es wird die installierte und konfigurierte Rolle „DHCP“ vorausgesetzt).

1. Installation des Netzwerkrichtlinienservers
(Folgende Schritte werden auf dem DHCP Server ausgeführt!)

1. Starten Sie den Server Manager.
2. Im Menüpunkt „Rollen“, wählen Sie „Rolle hinzufügen“.
3. Wählen Sie die Rolle „Netzwerkrichtlinien und Zugriffsdienst“ aus.
4. Im Menüpunkt „Rollendienste“, wählen Sie den „Netzwerkrichtlinienserver“.
5. Klicken Sie auf Installieren.

2. Konfiguration des NPS Server für Network Access Protection

1. Klicken Sie Star -> Verwaltung -> Netzwerkrichtlinienserver
   (Alternativ: WINDOWS+R -> nps.msc)
2. Wählen Sie „NPS (Lokal)“.
3. In der Detailansicht wählen Sie aus dem Drop-Down-Menü „Netzwerkzugriffsschutz (NAP)“ aus und klicken auf „NAP konfigurieren“.
4. Auf dem Anzeigefenster „Auswählen der Netzwerkverbindungsmethode zur Verwendung mit NAP“ wählen Sie aus dem Drop-Down-Menü „Dynamic Host Configuration-Protokoll (DHCP).
5. Auf der folgenden Seite muss kein Radius Client gewählt werden, da der DHCP Dienst auf diesem Server verwendet wird.
6. Auf der Seite „DHCP-Bereiche angeben“ müssen ebenfalls keine Einstellungen vorgenommen werden. Wollten Sie NAP nur auf bestimmte IP-Scopes eines DHCP Servers anwenden, so könnten Sie diese hier eintragen. Wir möchten NAP aber auf alle Scopes anwenden.
7. Im Installationspunkt „Benutzer- und Computergruppen konfigurieren“ werden ebenfalls keine Einstellungen vorgenommen. Hier könnte man die Anwendung von NAP auf bestimmte Computer oder Benutzergruppen einschränken.
8. Im nächsten Schritt werden Wartungsserver festgelegt. Diese Server ermöglichen es NAP Clients, welche die Integritätsprüfung nicht bestanden haben, sich zu aktualisieren um die Anforderungen zu erfüllen.
   - Klicken Sie auf „Neue Gruppe…“.
   - Vergeben Sie einen Namen für die Gruppe.
   - Klicken Sie auf Hinzufügen
   - Geben Sie die IP-Adresse oder den Namen der Server ein.

9. Auf der Seite „NAP- Integritätsrichtlinie definieren“ können Sie die durchzuführenden Überprüfungen (SHV) auswählen.
   Gehen Sie sicher, dass die „Windows-Sicherheitsintegritätsverifizierung“ ausgewählt ist.
   Der Punkt „Automatische Wartung von Clientcomputern“ sollte ebenfalls aktiviert sein.
   Definieren Sie zum Schluss noch wie mit nicht NAP-Kompatiblen Clienten verfahren werden soll und klicken Sie anschließend auf „Weiter“ und „Fertigstellen“.
   Der Network Access Protection Service auf dem Network Policy Server ist eingerichtet.

3. Konfigurieren der System Health Validators (SHV)

1. Klicken Sie Star -> Verwaltung -> Netzwerkrichtlinienserver
   (Alternativ: WINDOWS+R -> nps.msc)
2. Unter dem Menüpunkt „Netzwerkzugriffsschutz“ wählen Sie „Systemintegritätsprüfung“.
3. In der Detailansicht klicken Sie auf den zu konfigurierenden SHV.
   (Anfangs ist nur der „Windows- Sicherheitsintegritätsverifizierung“ SHV vorhanden).
4. Klicken Sie auf „Konfigurieren“
5. Hier können Sie die durchzuführenden Überprüfungen des SHV auswählen.
6. Deaktivieren Sie für unseren Test alle bis auf „Für alle Netzwerkverbindungen ist eine Firewall aktiv“.
7. Bestätigen Sie mit OK.

4. Konfigurieren des DHCP-Servers zur Unterstützung von NAP

1. Klicken Sie Start -> Verwaltung -> DHCP
2. Klicken Sie rechts auf den DHCP Scope auf den Sie NAP anwenden wollen und wählen Sie „Eigenschaften“ (Wählen Sie anstelle des Scopes „IPv4“ aus um NAP auf alle Scopes anzuwenden).
3. Klicken Sie auf den Reiter „Netzwerkzugriffsschutz“.
4. Wählen Sie „Für diesen Bereich aktivieren“ und „Netzwerkzugriffsschutz-Standardprofil verwenden“.
5. Bestätigen Sie mit OK.

5. **NAP Clientkomponenten konfigurieren**
   (Alle Clientseitigen Einstellungen sind auch über Gruppenrichtlinien realisierbar)

   1. Klicken Sie rechts auf „Computer“, wählen Sie „Verwalten“.
   2. Im Menüpunkt „Dienste“ rechts klicken Sie auf den „NAP Agenten“ und wählen „Eigenschaften“.
   3. Legen Sie den Starttyp auf „Automatisch“ und klicken Sie anschließend auf „Start“ und „OK“.
   4. Starten Sie auf dem Client eine Konsole mit Administrator Rechten.
   5. Tippen Sie „netsh nap client show state“ ein.
   6. In der Rubrik „Clientstatus“ sollte im Punkt „Status“ nun „Aktiviert“ stehen.
   7. In der Rubrik „Erzwingungsclientstatus“ sollte im Punkt „DHCP-Quarantäneerzwingungsclient“ „Initialisiert = Nein“ zu lesen sein.
      Der NAP- Client weiß noch nicht gegen welchen Erzwingungspunkt er sich authentifizieren soll.
   8. Notieren Sie sich die ID des „DHCP-Quarantäneerzwingungsclient“.
   9. Geben Sie „netsh nap client set enforcement ID = <Notierte ID> Admin = „Enable“ “ein.
   10. Mittels „netsh nap client set userinterface title=“<Titel>“ text = „<Text>““ können Sie das Benachrichtigungsfenster, welches im Fehlerfall erscheint, anpassen (optional).
   11. Die Konfiguration des NAP Client ist abgeschlossen, die SHA können sich nun gegen den NAP Server authentifizieren.

8. Quellen:

Internet:
http://technet.microsoft.com/en-us/network/bb545879.aspx

Bücher:
„Konfigurieren einer Windows Server 2008 Netzwerkinfrastruktur“
von Tony Northrup & J.C. Macki | ISBN: 978-3-86645-942-7

„Windows Server 2008 R2 - Das umfassende Handbuch“
von Ulrich B. Boddenberg | ISBN: 978-3836215282