

MS Windows Server 2008: Network Access Protection

Wirksamer Netzwerkzugriffschutz



MS Windows Server 2008 Network Access Protection

Sie operieren mit Windows-basierten Netzen? Sie legen wichtige Einstellungen zentral fest, schützen sich durch AntiVirus-Lösungen und werten den Status Ihrer Rechner regelmäßig aus? Prima – das entspricht den Empfehlungen für gemanagten Systembetrieb. Aber wie stellen Sie sicher, dass diese Rahmendaten zu jeder Zeit absolut verbindlich eingehalten werden?

HERAUSFORDERUNG: NETZWERKZUGANGSSCHUTZ

Kontrolle über das Unternehmensnetzwerk zu behalten, ist eine der wichtigsten Aufgaben von IT-Administratoren. Kein leichtes Unterfangen, insbesondere, wenn Außenstellen oder Niederlassungen am Unternehmensnetzwerk angebunden sind. Wenn dazu auch noch Gastsysteme (z.B. in Konferenzräumen) toleriert werden und/oder mobiles Arbeiten über Laptops oder gar private Heim-PCs gestattet ist, wird es auch für erfahrene Administratoren ohne den Einsatz geeigneter Tools nahezu unmöglich:

- die Kontrolle über zugriffsberechtigte Remote-PCs zu behalten
- alle Remote-PCs ausreichend zu schützen und zu warten
- Unternehmensdaten auch im WAN nur an vertrauenswürdige Rechnersysteme zu übermitteln

Gleichzeitig hat sich die IT-Administration auch mit „hausgemachten“ Problemen zu beschäftigen, weil Anwender z.B.:

- mit Sicherheitsanforderungen nicht umzugehen wissen
- Komponenten ungenehmigt ins Netzwerk hängen
- Sonderregelungen für sich beanspruchen
- Risiken nicht einschätzen können
- Konfigurationen verändern

Bisherige Lösungsansätze waren limitiert, proprietär und unflexibel. Gefragt sind daher Architekturen, die:

- professionellen Anforderungen Rechnung tragen
- schnell, einfach und zuverlässig betrieben werden können
- universell für diverse Zugangswege genutzt werden können
- Zugangsrichtlinien vor Netzwerkzugriffsfreigaben durchsetzen

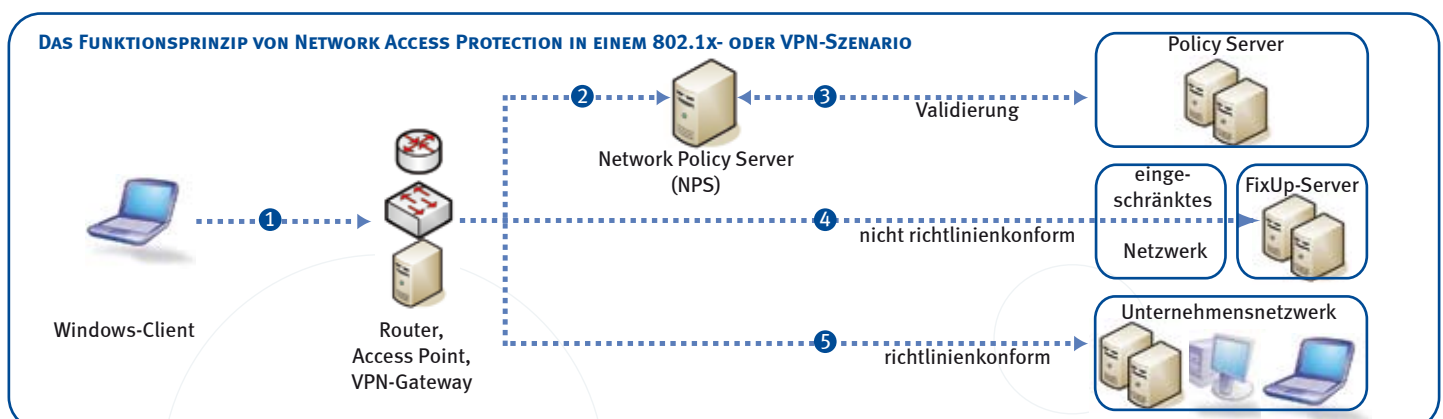
LÖSUNG: MODERNER NETZWERKSCHUTZ MIT NAP

Die NAP-Plattform (Network Access Protection) von Microsoft tritt an, einen solchen komplexen, hochwirksamen und zudem kostengünstigen Netzwerkzugriffsschutz zu ermöglichen. Als integriertes Feature des Windows Server 2008 legen Administratoren von vornherein – also proaktiv – fest, was mit einem Client geschieht, der die Richtlinien erfüllt oder auf verschiedene Arten verletzt.

NETWORK ACCESS PROTECTION: DAS FUNKTIONSPRINZIP

Etwas vereinfacht dargestellt, funktioniert Microsofts Network Access Protection nach folgendem Prinzip:

- 1 Ein Client meldet sich bei einem Router, Access Point oder VPN-Gateway an und präsentiert dort seinen Gesundheitszustand. Zum Beispiel kann dort überprüft werden:
 - Handelt es sich um einen autorisierten RemotePC?
 - Verfügt dieser über aktiven und aktuellen Virenschutz?
 - Ist eine Personal Firewall in Betrieb?
- 2 Router, Access Point oder VPN-Gateway leiten den Gesundheitszustand an den Microsoft Network Policy-Server weiter.
- 3 Network Policy Server (NPS) validiert den Gesundheitszustand des Clients gegen die von der Unternehmens-IT definierte Gesundheitsrichtlinie.
- 4 Falls der Client nicht der definierten Unternehmensrichtlinie entspricht, wird er in ein eingeschränktes VLAN umgeleitet und erhält Zugriff auf Ressourcen wie Patches, Konfigurationen und Signaturen.
- 5 Erfüllt der Client die Richtlinien, erhält er einen transparenten Netzwerkzugriff.





Quelle: aboutpixel.de, alarm call © mediascapes

VIelfältiger Nutzen

Microsoft Network Access Protection gewährt Unternehmen umfangreichen Nutzen auf hohem Niveau. Die wichtigsten Vorteile:

- Proaktiver, hochwirksamer, kostengünstiger Schutz
 - ✓ Policy-basierter Zugriff: Unterstützt eigene Systeme und Gastrechner
 - ✓ Läuft ohne permanente Aufsicht und Pflege durch die IT-Zentrale
 - ✓ Wirksam auch bei Anwendern mit Administratorrechten
 - ✓ Flexible, durchdachte und hochautomatisierte Lösung
 - ✓ Wirksam sofort bei Verbindung mit dem Netzwerk
 - ✓ Zentrales Rollout und zentrale Kontrolle
 - ✓ Kontrolle unabhängig vom Zugriffsweg
- Transparent für die Anwender: Keine Trainings erforderlich
- Auf Standardkomponenten basierende Technologie
 - ✓ Für kabelgebundene Zugänge, WLAN, VPN und Terminaldienste
 - ✓ Hardware-neutral: Jeder Router, jeder WLAN Access Point, jeder Switch (Layer2/Layer3, unmanaged/managed), jedes IDS
 - ✓ Offenes API mit derzeit >100 3rd-Party Lösungen (inkl. Linux!)
 - ✓ Unterstützt nativ: dynamisches IPsec, VPN, IEEE 802.1x
 - ✓ Optimale Komplementärlösung zu zertifikatsbasierter Authentisierung
- Alle Dienste sind Bestandteil der Windows-Plattform
 - ✓ Windows Server 2008 liefert die Infrastruktur
 - ✓ Sofort einsatzbereit: Windows XP ab SP3 und Windows Vista
 - ✓ Kein Updatezwang: Active Directory 2000, 2003 oder 2008
 - ✓ Keine zusätzlichen CALs
- Standortunabhängig einsetzbar

Network Access Protection mit Networkers

Die Einführung von Schutzmechanismen auf Netzwerk- und Rechnebene in einer Microsoft-lastigen Umgebung erfordert die durchgängige Betrachtung von Layer 1 bis Layer 7 der komplexen Protokoll- und Technologiewelt.

Dazu bedarf es Experten, die sich in der Netzwerk-, wie in der Betriebssystem- und Anwendungswelt gleichermaßen gut auskennen, sowie über entsprechend langjährige Erfahrung verfügen und als Team gemeinsam agieren können.

Als ein Spezialist für Planung, Aufbau und Betrieb sicherer und leistungsfähiger Applikations- und Netzwerkinfrastrukturen sowie als Microsoft Gold Certified Partner in den Kompetenzbereichen Networking Infrastructure Solutions, Information Worker Solutions und Security Solutions bietet Ihnen die Networkers AG die besten Voraussetzungen.

Microsoft
GOLD CERTIFIED
Partner

Networking Infrastructure Solutions
Advanced Infrastructure Solutions
Information Worker Solutions
Security Solutions

Professionell, routiniert und versiert etablieren wir NAP auch in Ihrem Hause und helfen Ihnen damit, Ihre Geschäftsprozesse noch effizienter und damit profitabler zu gestalten.



Networkers AG
Bandstahlstraße 2
58093 Hagen

fon: 0 23 31 . 80 95 0
fax: 0 23 31 . 80 95 499

email: info@networkers.de
web: www.networkers.de