Best Practice

Secure Client

Automatische Hotspot-Anmeldung

Automatische Hotspot-Anmeldung zum Aufbau eines VPN Tunnels ab Client Version 10.10

Funktionalität der integrierten, dynamischen NCP Personal Firewall-Lösung

Stand August 2016
Version 10.10

Haftungsausschluss

Die in diesem Dokument enthaltenen Informationen können ohne Vorankündigung geändert werden und stellen keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten.

Warenzeichen

Alle genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber.

Inhaltsverzeichnis

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave. · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

1. Unsicheres Mobile Computing in WLANs (Hotspots)

Mobiles Business ist heute eine etablierte Arbeitsmethode in modern organisierten Unternehmen. Der Einsatz von Notebooks und Handhelds steigert die Produktivität sowie Flexibilität mobiler Mitarbeiter und damit den geschäftlichen Erfolg im globalen Wettbewerb.
Als Übertragungsmedien dienen neben ISDN, dem analogen Fernsprechnetz und xDSL insbesondere öffentliche Funknetze (GSM, UMTS) und Nahbereichs-Funknetze wie Wireless LAN (WLAN) an öffentlichen Plätzen, sog. Hotspots in Bahnhöfen, Flughäfen, Messehallen, Hotels etc. mit Anbindung an das Internet.
WLANs stellen aufgrund der „Luftschnittstelle“ eine besondere Gefahrenquelle dar, da sie sehr leicht angreifbar sind. Mobile Teleworker befinden sich an Hotspots in einem höchst unsicheren Umfeld, in dem sie sich selbst um das Thema Sicherheit kümmern müssen. Dabei geht es nicht nur darum, eine bestehende Datenverbindung in das Firmennetz zu schützen, sondern bereits vor und während des Verbindungsaufbaus keine Sicherheitslücken entstehen zu lassen.

1.1. Grundfunktionalitäten von Hotspots

An Hotspots betreiben Provider WLANs, die sie für die allgemeine Nutzung gegen Entgelt zur Verfügung stellen. Öffentliche WLANs dienen als breitbandige Zugangsnetze zum Internet bzw. in das Firmennetz.
Will nun ein mobiler Mitarbeiter eine VPN-Verbindung zur Firmenzentrale herstellen, muss er sich zunächst beim Hotspot-Betreiber registrieren. Dies erfolgt üblicherweise über einen Web-Browser. Hier gibt der Anwender seine Kennung ein, die ihm den Zugang freischaltet und aufgrund derer letztlich die Bezahlung bzw. Rechnungsstellung erfolgt.

1.2. Risiken und Problemstellung

Auf öffentliche WLANs kann grundsätzlich jeder Anwender mit entsprechend ausgestattetem PC zugreifen. Hierfür erhält er eine IP-Adresse, sofern er die SSID (Service Set Identifier) des WLAN kennt. Die Sicherheit der Daten oder ein Schutz seines Arbeitsgerätes vor Attacken ist vom WLAN-Betreiber nicht abgedeckt. Hierum muss sich jeder Anwender selbst kümmern.
Konkret geht es um folgende Sicherheitsaspekte:

1. Schutz der Vertraulichkeit
   Sensitive Informationen dürfen während der Übertragung für Dritte nicht zugänglich sein.
2. Schutz des PCs am Hotspot
   Der PC-Arbeitsplatz muss gegenüber Attacken aus dem WLAN (andere WLAN-Teilnehmer) und dem Internet zu jeder Zeit abgeschottet sein.

Zum Schutz der Vertraulichkeit dienen die bewährten Sicherheitsmechanismen: VPN-Tunneling und Datenverschlüsselung. Für die Sicherheit des PC wird zusätzlich eine Personal Firewall benötigt. Den erforderlichen Schutz bietet „Stateful Packet Inspection“. Sollte diese Funktion nicht gegeben sein, ist von Mobile Computing an einem Hotspot grundsätzlich Abstand zu nehmen.
Das eigentliche Sicherheits-Risiko besteht darin, dass die Registrierung beim Hotspot-Betreiber außerhalb des geschützten Bereichs eines VPN mittels Browser erfolgen muss. Das bedeutet: während dieses Zeitraums ist das Endgerät ungeschützt.
Dies steht normalerweise im Widerspruch zur Unternehmens-Policy, die direktes Surfen im Internet untersagt und nur bestimmte Protokolle zulässt. Eine Firewall-Lösung im Endgerät, die wirklich umfassenden Schutz bietet, muss also auch die kritischen Phasen während des An- und Abmeldevorganges am Hotspot absichern.

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave. · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

1.3. **Alternative Lösungsansätze mit Restrisiken**

Die Firewall-Regeln für http bzw. https werden vom Administrator fest voreingestellt, um die Funktionalität an beliebigen Hotspots zu gewährleisten. Alternativ kann die Konfiguration derart sein, dass die Ports für http bzw. https bei Bedarf für ein bestimmtes Zeitfenster (z.B. 2 Minuten) geöffnet werden.
Das Sicherheitsrisiko besteht in beiden Fällen darin, dass der Benutzer unabhängig von einem VPN-Tunnel, ungesichert im Internet surft und sich Schadsoftware einfangen kann. Bei der temporären Öffnung der Firewall besteht die Gefahr vorsätzlichen Missbrauchs durch mehrfaches Auslösen des Zeitfensters durch den Anwender.
Bei einer anderen Variante verändert der User vor Ort die Firewall-Regeln. Diese bedarfsabhängige Öffnung der Personal Firewall birgt das Risiko von Fehlkonfigurationen. Denn der Anwender muss genau wissen, welche Änderungen an welcher Stelle vorzunehmen sind.
Sein Sicherheitsbewusstsein und technisches Know-How alleine bestimmen die Qualität des aktuellen Sicherheitsniveaus.

2. Die Lösung von NCP – Automatische Hotspot-Anmeldung

Damit der remote Client in jeder Phase des Verbindungsaufbaus auch im WLAN- und Hotspot-Umfeld ohne Zutun des Anwenders gegenüber jeglichen Attacken geschützt ist, hat NCP die Personal Firewall fest in die Secure Client Software integriert. Sie verfügt über intelligente Automatismen für eine sichere Hotspot-Anmeldung. Administratoren und Anwender können sich jederzeit auf die Sicherheit ihrer Endgeräte und Daten verlassen.

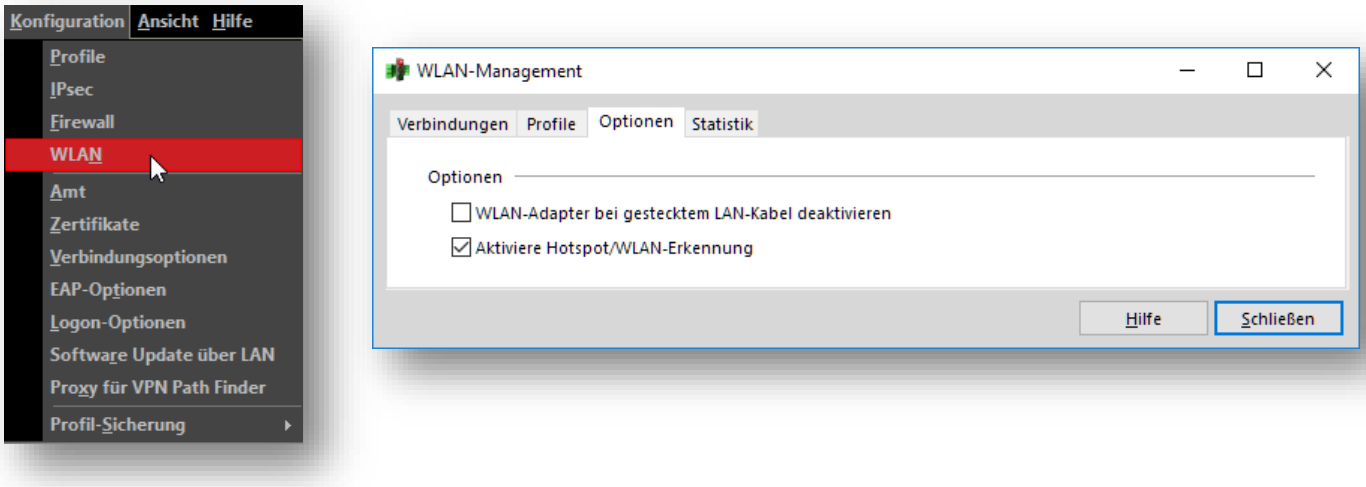
Es werden zwei grundlegende Techniken für die Anmeldung am Hotspot unterschieden:

- Nutzung eines Browsers zur interaktiven Anmeldung durch den Anwender mit automatischer, dynamischer Anpassung von Firewall-Regeln im Hintergrund
- Script-basierte Anmeldung ohne Interkation durch den Anwender

In diesem Dokument wird ausschließlich auf die erste Variante mit Interaktion des Benutzers eingegangen, weitere Informationen zur script-basierten Hotspot-Anmeldung befinden sich im Handbuch des NCP Secure Client.

2.1. **Hotspot-Anmeldung mit dynamischer Anpassung von Firewall-Regeln**

Die Einstellungen, um die integrierte, sichere Hotspot-Anmeldung nutzen zu können, erfolgen im Menü „Konfiguration“ unter dem Punkt „WLAN“. Die Aktivierung wird im Reiter „Optionen“ vorgenommen (sieh unten).

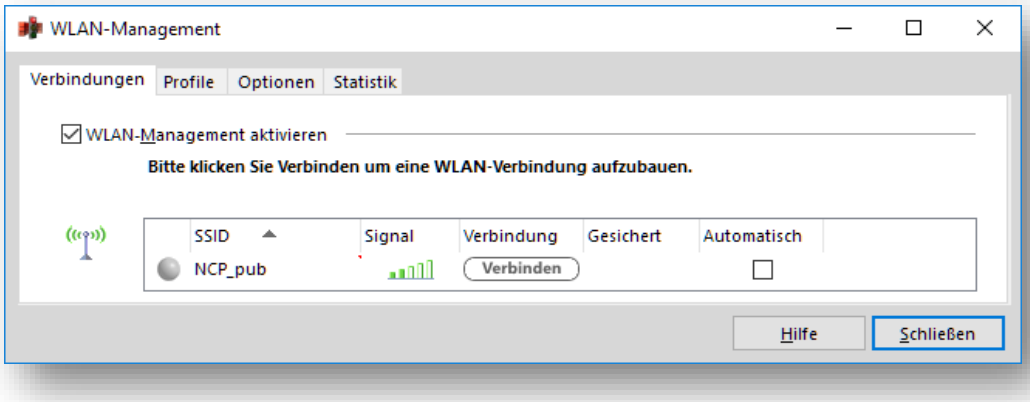


Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave. · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Die somit aktivierte Hotspot-Anmeldung kann nun auf zwei Arten genutzt werden, welche im weiteren Verlauf jeweils noch genauer beschrieben werden. Ideal ist die Nutzung mit aktiviertem WLAN-Management des NCP Secure Clients. Dabei führt der Client den Anwender intuitiv durch die einzelnen Schritte bis zum erfolgreichen Logon am WLAN. Soll das WLAN-Management nicht eingesetzt werden, muss der Anwender selbst ein paar Zwischenschritte auf dem Weg ins WLAN nehmen. Doch dazu später mehr.

2.1.1. Die elegante Variante – Anmeldung mit aktivem NCP WLAN-Manager

Das WLAN-Management des NCP Secure Clients erlaubt die Konfiguration und Verbindung zu drahtlosen Netzwerken direkt im Client. Dies bietet verschiedene Vorteile im Zusammenspiel mit der VPN-Verbindungskontrolle im Allgemeinen, insbesondere jedoch bei der geführten Anmeldung für den sicheren Zugriff auf öffentliche Hotspots (in gleicher Weise auch am (firmen-)eigenen WLAN/Hostspot). Aktiviert wird das WLAN-Management über die entsprechende Option im Reiter „Verbindungen“ wie unten abgebildet.

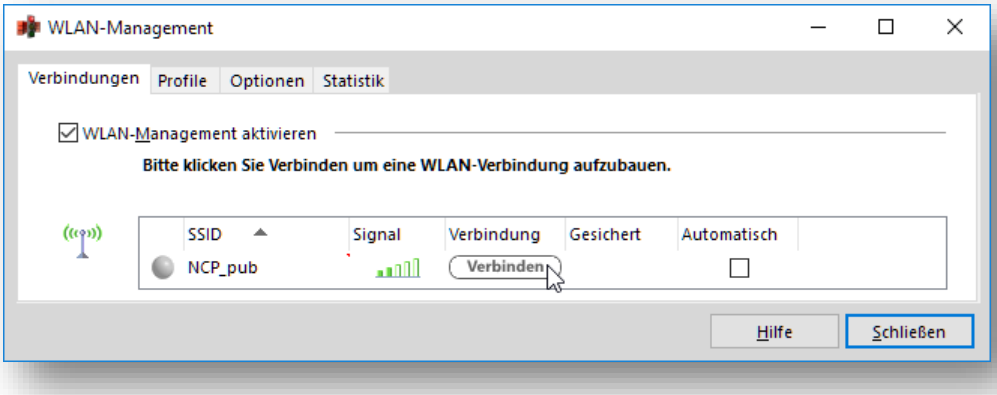


Befindet sich ein Benutzer mit seinem Endgerät im Empfangsbereich eines (öffentlichen) WLAN, prüft der NCP Secure Client automatisch ob für eines der verfügbaren drahtlosen Netzwerke bereits eine Konfiguration mit automatischer Verbindung vorliegt. Falls ja, wird hierzu automatisch eine Verbindung hergestellt

Ist dies nicht der Fall wird im Monitor auf die Verfügbarkeit dieser Netze hingewiesen (siehe folgende Abbildung).
Befindet sich ein Benutzer mit seinem Endgerät im Empfangsbereich eines (öffentlichen) WLAN, prüft der NCP Secure Client automatisch ob für eines der verfügbaren drahtlosen Netzwerke bereits eine Konfiguration mit automatischer Verbindung vorliegt. Ist dies nicht der Fall wird im Monitor auf die Verfügbarkeit dieser Netze hingewiesen (siehe folgende Abbildung).

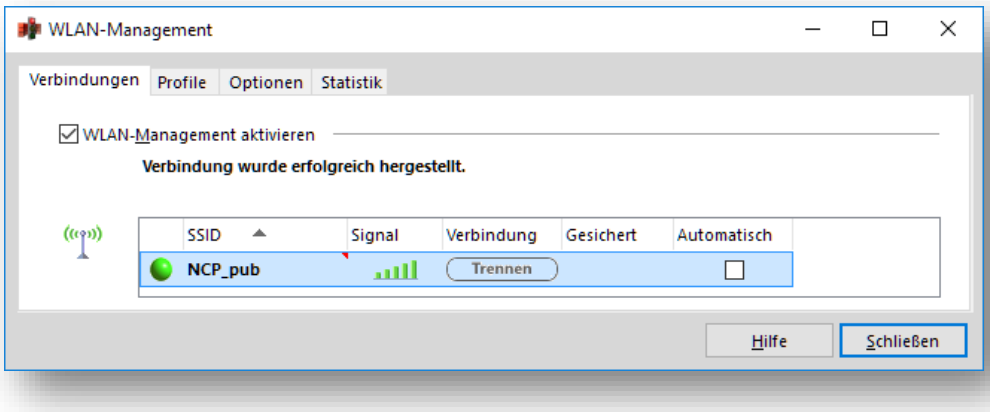
Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave. · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Durch einen Mausklick auf die blaue Textzeile „Klicken Sie hier um sich zu verbinden“ im Monitor bzw. den auf gleicher Höhe befindlichen Auswahl-Button wird die Übersicht der verfügbaren drahtlosen Netzwerke angezeigt.

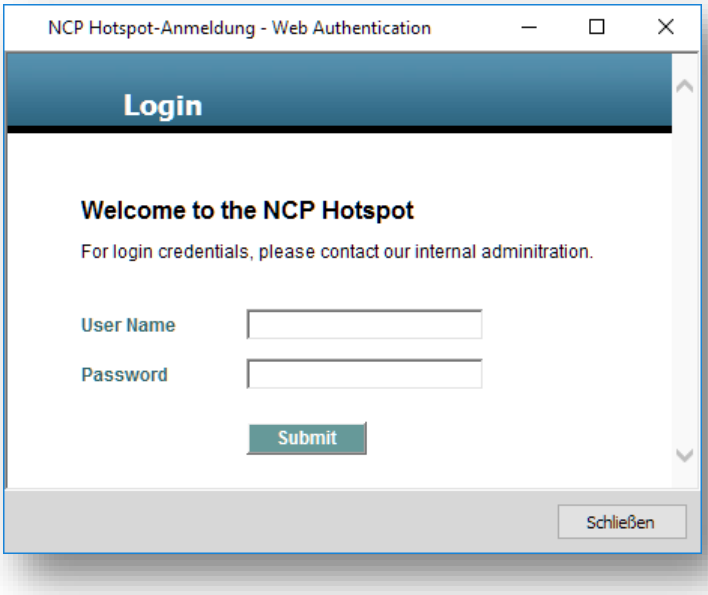


Wiederum ein Klick auf den „Verbinden“-Button der gewünschten SSID (im Beispiel „NCP_pub“) stellt die Verbindung zum Access Point her und im Hintergrund führt der NCP Secure Client die Internet-Verbindungsprüfung durch.

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave. · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

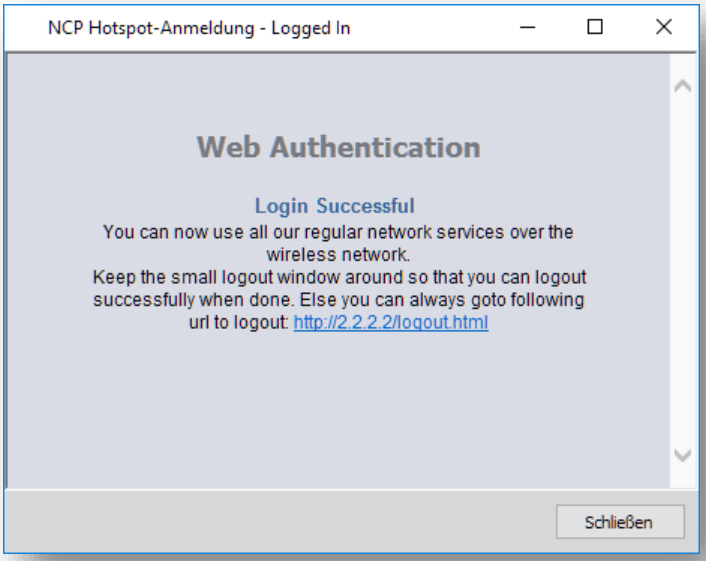


Erfolgt die Umleitung zu einem Captive Portal also einer vorgeschalteten Web-Seite, welche die Eingabe von Zugangsdaten für den Internet-Zugriff erforderlich macht, wird die WLAN-Übersicht geschlossen und der der NCP Secure Client öffnet automatisch einen eingeschränkten Browser, basierend auf der Windows Internet Explorer API.



Dieser Browser erlaubt keine Eingabe von Web-Seiten (URLs) durch den Benutzer, sodass kein „freies Surfen“ ermöglicht wird. Die integrierte Personal Firewall des NCP Secure Clients gestattet ausschließlich diesem Browser-Prozess, der im Kontext des Secure Client Monitors (ncpmon.exe) läuft, den Zugriff auf die Anmeldeseite des Hotspots. Die Kommunikation des Browser-Prozesses wird über Stateful Packet Inspection abgesichert, sodass kein aktiver Datenverkehr von außen gestattet wird sondern nur Antwortpakete auf gesendete Anfragen akzeptiert werden. Darüber hinaus unterliegt dieser Browser keiner übergeordneten Proxy Server-Konfiguration, welche möglicherweise für den Standard-Browser eingerichtet wurde.

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave. · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com



Nach erfolgreicher Eingabe der Zugangsdaten und Freischaltung durch den Hotspot-Betreiber, baut der NCP Secure Client mit aktiven Konfigurationsprofil selbstständig die VPN-Verbindung z.B. zur Firmenzentrale auf.

Ab nun kann wieder sicher wie an einem Büroarbeitsplatz kommuniziert werden kann.

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave. · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Zusammengefasst bietet die überarbeitete Hotspot-Anmeldung des NCP Secure Clients folgende Vorteile:

- Mehr Transparenz für Administrator und Benutzer durch integrierte Browser-Ansatz und intuitive Abfolge der Anmeldungsschritte.
- Limitierte Funktion des genutzten Browsers, der Benutzer kann keine Web-Adressen eingeben oder sonstige Einstellungen vornehmen
- Exakte Firewall-Überwachung des Browser-Prozesses mit Stateful Packet Inspection. Andere Browser werden durch die Firewall geblockt.
- Keine Beschränkung innerhalb der Hotspot-Anmeldung hinsichtlich Zeit und Anzahl der kontaktierten IP-Adressen/Server/Ports ohne Sicherheitsbeeinträchtigung (durch explizite Prozessüberwachung).
- Flexible Anmeldung an beliebigen Hotspot-Umgebungen ohne Manipulation der Proxy Server-Konfiguration.

Automatische Firewall-Regeln im Detail:

Folgende Stateful-Regeln werden beim Start der Hotspot-Anmeldung dynamisch angelegt und mit dem Ende des Anmeldevorgangs (Schließen des Browser-Fensters) wieder gelöscht.:

Für Internet-Verfügbarkeitsprüfung (Internet-Online-Test):

- Namensauflösung über DNS (Source Port: 1024-65535; Destination Port: 53)
- IP-Adresse des NCP bzw. Microsoft Web Servers, deren URLs für die Prüfung aufgerufen werden (NCP-Seite: „http://hotspot.ncp-e.com/“; Microsoft-Seite: „http://www.msftncsi.com/ncsi.txt“)

Für Hotspot-Anmeldung mit eingeschränktem Browser:

- Namensauflösung über DNS (Source Port: 1024-65535; Destination Port: 53)
- Beliebige Zieladressen und –Ports ausschließlich ausgehend vom Browser-Prozess (Source Ports: 1024-65535)

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave. · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

3. Weitere Informationen zur NCP Personal Firewall

Die Personal Firewall ist integrativer Bestandteil der NCP Secure Clients. Alle Firewall-Mechanismen sind optimiert für Remote Access-Anwendungen und werden bereits beim Start des Rechners aktiviert. D.h. im Gegensatz zu VPN-Lösungen mit eigenständiger Firewall ist der Telearbeitsplatz bereits vor der eigentlichen VPN-Nutzung gegen Angriffe geschützt. Die Firewall bietet auch im Fall einer Deaktivierung der Client-Software vollen Schutz des Endgerätes. Alle Firewall-Regeln können zentral vom Administrator vorgegeben und deren Einhaltung erzwungen werden. Voraussetzung hierfür ist das zentrale NCP Secure Enterprise Management, mit dessen Hilfe die Konfiguration des Secure Enterprise Clients fest, für den Anwender nicht änderbar vorgegeben werden kann.

3.1. Die Funktionalitäten der integrierten NCP Personal Firewall im Überblick

IP-Network Address Translation (IP-NAT)
IP-NAT verbirgt die interne Client-Adresse, damit diese von außen nicht angreifbar ist.

Stateful Packet Inspection
Es werden Regeln (s.u) für den Datentransfer festgelegt, d.h. alle ausgehenden und ankommenden Datenpakete müssen den vorher festgelegten Filterregeln entsprechen. Auf Basis der definierten Eigenschaften wird jedes kommende Datenpaket überprüft und bei Nichtübereinstimmung abgewiesen. Das bedeutet: Der jeweilige Rechner wird entsprechend dem erstellten Regelwerk abgeschirmt und der Aufbau unerwünschter Verbindungen verhindert.

Applikationsabhängige Firewall-Regeln
Es können Firewall-Regeln definiert werden, die nur aus einer bestimmten Anwendung verwendet werden können. Ein klassisches Beispiel wäre eine Regel, welche nur vom Internet Explorer verwendet wird und das Surfen über Port 80 erlaubt.

Protokoll-, port- und adressenbezogene Firewall-Regeln
Standardmäßig werden Firewall-Regeln über IP-Adressen und Ports definiert. Jedoch besteht zusätzlich die Möglichkeit nach Protokollen zu filtern.

Friendly Net Detection (FND)
Definierte Firewall-Regeln werden in Abhängigkeit von der Netzwerkumgebung, in der sich ein Teleworker befindet, automatisch aktiviert z.B. Standort LAN im Unternehmen oder WLAN an Hotspots. In bekannten Netzen gelten andere Bedingungen als in öffentlichen, unbekannten Übertragungsnetzen. Die automatische Erkennung des Netzwerkes erfolgt durch Auswertung eines oder mehrerer Faktoren:

- Automatisch mittels FND-Server (siehe FND-Whitepaper) oder
- Statisch
  - aktueller Netzwerkadresse
  - IP-Adresse des DHCP Servers

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave. · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Automatische Hotspot-Anmeldung

Intelligenter Mechanismus für die sichere Freischaltung des Netzzuganges über den Browser an öffentlichen WLANs. Jeder weiterer Datentransfer bleibt gesperrt, d.h. der Anwender ist auch in dieser Phase vor einem VPN-Verbindungsaufbau zum Firmennetz nicht angreifbar.

Verbindungsabhängige Firewall-Regeln

Logging-Optionen

- Protokollierung aus/ein
- Abgelehnter Datenverkehr
- Zugelassener Datenverkehr

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 678 Georgia Ave. · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com