SecurITy made in Germany
Trust Seal
www.teletrust.de/itsmig

NCP
SECURE COMMUNICATIONS

Whitepaper

Friendly Net Detection

Friendly Net Detection Stand März 2022

1. 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.

2. Warenzeichen

Alle genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber.

Friendly Net Detection - Begriff und Inhalt

Bei der Friendly Net Detection (FND) handelt es sich um eine Technik zur automatischen Erkennung von so genannten „Bekannten Netzen“, auch „Friendly Networks“ genannt. Ziel ist es, einerseits in Remote Access VPNs (Virtual Private Networks) ein Maximum an Sicherheit für das zentrale Datennetz zu garantieren und andererseits dem Anwender ein transparentes Arbeiten im Firmennetz bzw. in vertrauenswürdigen Umgebungen zu ermöglichen. Es gilt eine Lösung zu finden, die das Ende-zu-EndeSicherheitsprinzip umsetzt – also die Abschottung des entfernten Endgerätes – und gleichzeitig über die Intelligenz verfügt, in Friendly Networks ungehindertes Arbeiten zu erlauben. Im Folgenden werden Anforderungen und Funktionsweise der Friendly Net Detection ausführlich beschrieben.

Friendly Networks – Ausgangssituation

Die integrierte Personal Firewall der NCP Secure Clients ermöglicht eine sehr flexible Gestaltung von Firewall-Regeln. So besteht die Möglichkeit, Regeln zu definieren, die sowohl von einer gesperrten Grundeinstellung (es ist alles verboten, was nicht erlaubt ist) ausgehen. Abhängig davon werden Netzwerkpakete nach bestimmten Kriterien gefiltert.

Beispielhaft seien hier genannt:

- Absender/Empfänger Adresse
- Protokoll (IP, UDP, ICMP, usw.)
- Anwendungsprogramm

Diese Kriterien, die in der Security Policy festgeschrieben sind, definieren sehr genau, was ein Anwender von seinem Rechner aus in einem Netzwerk (z.B. Intranet, zentrales Datennetz (Firmen-Netzwerk), Internet usw.) darf und was nicht. Die Security Policy wird i.d.R. vom Netzwerkadministrator erstellt und gepflegt.

Damit ein Anwender diese Security Policy nicht umgehen, d.h. Firewall-Regeln deaktivieren löschen oder ändern kann, ermöglicht der NCP Secure Client ein Sperren des Zugriffs auf diese Konfigurationsparameter. Dies gilt auch für Benutzer mit Administrator-Berechtigungen, d.h. unabhängig von den Rechten der Systemumgebung.

Hieraus entsteht jedoch ein Problem für mobile Anwender, die sich in unterschiedlichsten Netzwerken, z.B. Flughafen, Hotel, zuhause aber auch im Lokal Area Network (LAN) der Firma (Zentrale oder Filiale), befinden. Der Administrator muss ein Firewall-Regelwerk definieren, das den Sicherheits-anforderungen dieser unterschiedlichen Standorte gerecht wird. Die Anforderung könnte so aussehen, dass einem mobilen Anwender nur erlaubt ist, seine E-Mails vom Firmen-Server herunterzuladen, wobei ihm das Surfen im Internet aus sicherheitstechnischen Gründen untersagt ist.

Was geschieht jedoch, wenn dieser Anwender seinen Rechner z.B. im zentralen Datennetz anschließt? Er befindet sich in einer durch zentrale Sicherheitseinrichtungen (Firewall, Virenscanner etc.) geschützten Umgebung. Vielleicht existieren auch spezielle Client-/Serveranwendungen, welche die Kommunikation über definierte TCP/IP bzw. UDP Ports erfordern, die er verwenden möchte. Eine Personal Firewall ist hier überflüssig, d.h. bestimmte Firewall-Regeln müssen außer Kraft gesetzt werden, um im Firmennetz transparent arbeiten zu können. Im Falle statischer Firewalls, wo Regeln nur „aktiviert" bzw. „deaktiviert" sein können, hat er keinen Netzwerk-Zugriff. Der Benutzer müsste in Abhängigkeit von seinem jeweiligen Standort die Regeln manuell umschalten. Das widerspricht aber der Security Policy und dem Ende-zu-Ende-Sicherheitsprinzip.

Um dieses Problem zu lösen, werden Netzwerke in zwei Gruppen eingeteilt:

1. Friendly Networks, welche das Firmen-Netzwerk beinhalten und alle weiteren Netzwerke, denen der Administrator vertraut.
2. Alle anderen Netzwerke, man spricht auch von „Unfriendly Networks" oder „Unbekannten Netzen".

Um nun Firewall-Regeln zu definieren, die abhängig vom Standort bzw. aktuellen Netzwerk des Anwenders sind, bieten die NCP Secure Clients die Möglichkeit, einer dieser Gruppen eine Firewall-Regel zuzuordnen. Das hat zur Folge, dass sie nur dann aktiv ist, wenn sich der Anwender in einem der Gruppe zugeordneten Netzwerk befindet.

Friendly Net Detection – Problembeschreibung

Der Vorteil von FNs ist, dass der Administrator Firewall-Regeln nur einmal für die gesamte System-Landschaft definiert und die Personal Firewall in der Client-Software entsprechend konfiguriert. Voraussetzung ist ein Netzwerk mit einer statischen Struktur. Intranets oder Extranets von Unternehmen und Organisationen sind aber wie oben beschrieben von permanenten Veränderungen geprägt, die u.a. in den unterschiedlichen Kommunikationsumgebungen mobiler Mitarbeiter und ggf. Geschäftspartner begründet sind.

Der Administrator steht vor der Aufgabe, die Liste der Friendly Networks permanent aktuell zu halten und die Einhaltung der Firewall-Regeln sicherzustellen. Das ist Inhalt der Friendly Net Detection – einem Feature der dynamischen Personal Firewall des NCP Secure Clients. Sie ermöglicht dem remote Client automatisch zu erkennen, ob er sich in einem FN befindet, völlig transparent und ohne das Einspielen einer neuen Konfiguration. Vor der detaillierten Funktionsbeschreibung ist noch auf ein anderes Problem mit Friendly Networks einzugehen. Nicht jede Firma besitzt einen IP-Adressenbereich aus dem öffentlichen IP-Adressraum. Viele verwenden private IP-Adressen, wie 10.x.x.x/8, 172.16.x.x/16 oder 192.168.x.x/24, und setzen dann auf NAT-Devices (Network Address Translation) bzw. Proxy-Server. Das Problem besteht darin, dass in fest konfigurierten FNs beispielsweise ein Mitarbeiter in seinem Heimnetzwerk mit den gleichen Netzwerk-Adressen arbeitet wie im Friendly Net. Ein anderes denkbares

Szenarium ist, wenn ein Außendienstmitarbeiter sein Notebook in einem anderen Netzwerk z.B. bei einem Kunden anschließt, das den gleichen IP-Adressraum verwendet wie das Firmen Netzwerk

Das Ergebnis ist in jedem Fall das gleiche, die Security Policy wird aufgehoben bzw. aufgeweicht, d.h. Firewall-Regeln, welche den Client schützen sollen und deshalb nur in „Friendly Networks“ angewendet werden, sind nun aktiviert. Damit weder der Benutzer noch der Administrator mit dem Pflegen einer FN-Liste beschäftigt ist, empfiehlt sich der Einsatz einer Friendly Net Detection.

Aufbau und Funktionsweise der NCP Friendly Net Detection.

Die FND ist eine klassische Client-/Server-Anwendung. Da es sich bei dem Server (FNDS) um einen separat zu installierenden Dienst handelt, der vollkommen unabhängig vom VPNGateway ist, kann er auf einem beliebigen Rechner innerhalb des bekannten Firmennetzwerks installiert werden. Der Client (FNDC) ist Bestandteil der NCP Secure Client Suite und kann innerhalb deren Firewall-Einstellungen konfiguriert werden. Die Funktionsweise der FND basiert auf EAP (Extensible Authentication Protocol) über UDP (User Datagram Protocol) in verschiedenen Modifikationen oder TLS (Transport Layer Security).

Dies gewährleistet die Sicherheit des Systems und schützt vor Fehlern, wie sie bei proprietären Lösungen häufiger vorkommen. Voraussetzung für die Nutzung von FND ist die Installation des FNDS in einem Netzwerk, welches als FN deklariert wurde. Dieser Dienst muss dann von allen Anschlüssen des Netzwerks erreichbar sein, d.h. es müssen gegebenenfalls Änderungen an den Router Einstellungen vorgenommen werden. Betreibt ein Mitarbeiter sein Endgerät direkt am Firmennetzwerk, so versucht der FNDC, den konfigurierten FNDS zu kontaktieren. Wird dieser erreicht und authentifiziert, so ist bestätigt, dass sich der Rechner in einem FN befindet und die Firewall-Regeln des NCP Secure Clients werden entsprechend für „internen Betrieb“ umgeschaltet.

Der Authentifizierungs-Vorgang läuft wie folgt ab: Basis sind die standardisierten Authentifizierungs-Protokolle EAP (RFC2284) und EAP-TLS (RFC2716) bzw. TLS (RFC5246), wobei nur der Server vom Client authentifiziert wird.

Im Falle von EAP wird am Server ein Benutzername und Passwort hinterlegt, welches gleichzeitig auch im Client hinterlegt werden muss. Diese Vorgehensweise ermöglicht auch eine Gruppierung von Clients (Definition gruppenspezifischer FNs).

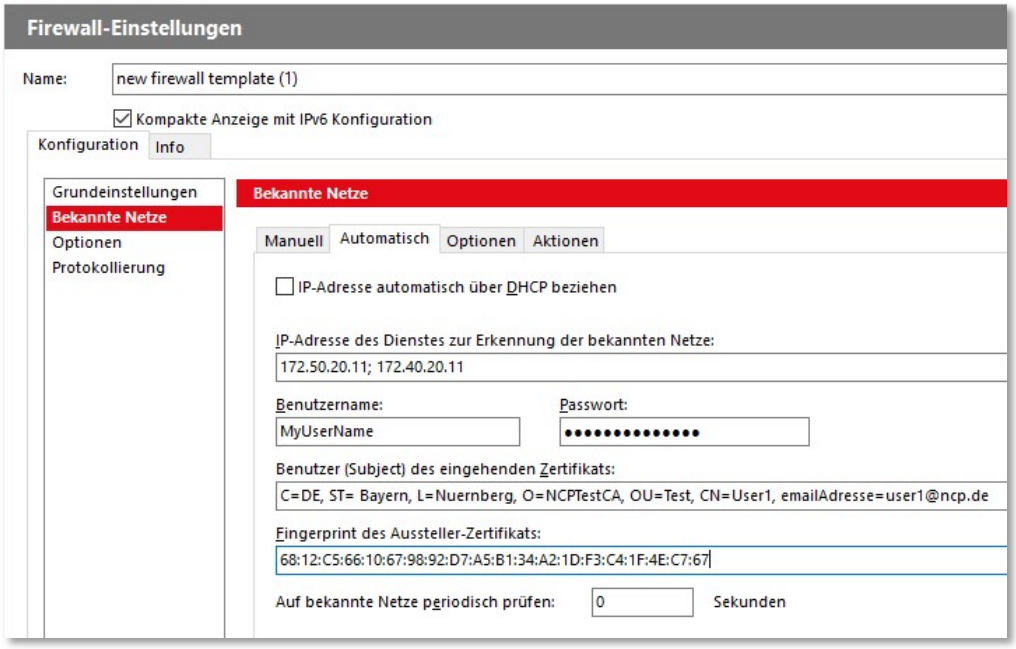

Abbildung 1 Dialog zur FND Konfiguration

Bei EAP-TLS müssen das Aussteller-Zertifikat bzw. alle Zertifikate, die für die Validierung des FNDS-Zertifikates notwendig sind, am Client zur Verfügung stehen. Weiter kann am Client der Fingerprint des Aussteller-Zertifikats und das Subject des FNDS-Zertifikats konfiguriert werden. Damit kann verhindert werden, dass ein versierter Anwender zu Hause ein FN nachbaut. Einzig beim VS-Govnet Connector wird ein anderes Verfahren angewandt.

Im Falle von TLS fällt Benutzername und Passwort weg. Im Client wird ein sog. CA Zertifikat oder das Zertifikat des FND Servers hinterlegt. Wenn eine TLS Verhandlung zu einem FND Server erfolgreich hergestellt wird, so befindet sich der Client im Friendly Net.

TLS wird vom FND Server ab Version 4.0 und im Client ab Govnet v2.10 unterstützt. Die vorhergehenden Versionen unterstützen lediglich EAP bzw EAP-TLS.

Nachdem alle Informationen für die Authentifizierung konfiguriert wurden, muss hinterlegt werden, unter welcher IP-Adresse der FNDS erreichbar ist. Dies können – um die Ausfallsicherheit zu erhöhen – maximal zehn IPv4 oder IPv6-Adressen sein. Alternativ können die IPAdressen des FNDS auch über DHCP auf den FNDC verteilt werden, wodurch die maximale Anzahl der zu definierenden FNs beliebig ist.

Zusammenfassung

Friendly Net Detection ist ein bedeutendes Feature der NCP Secure Client Suite für den universellen Einsatz in beliebigen Remote Access- und Kommunikations-Umgebungen. Die Regeln der integrierten Personal Firewall für „internen Betrieb“ im bekannten Netz sowie „externen Betrieb“ im unbekannten Netz werden vom Administrator zentral vorgegeben und sind vom Anwender nicht manipulier- bzw. abschaltbar. Der Anwender kann in jeder Situation hochsicher und transparent auf das Firmennetz zugreifen.

Für zentral gesteuerte Veränderungen an den Konfigurationsparametern des NCP Secure Clients, bietet NCP optional das Secure Enterprise Management (SEM) als „Single Point of Administration“.

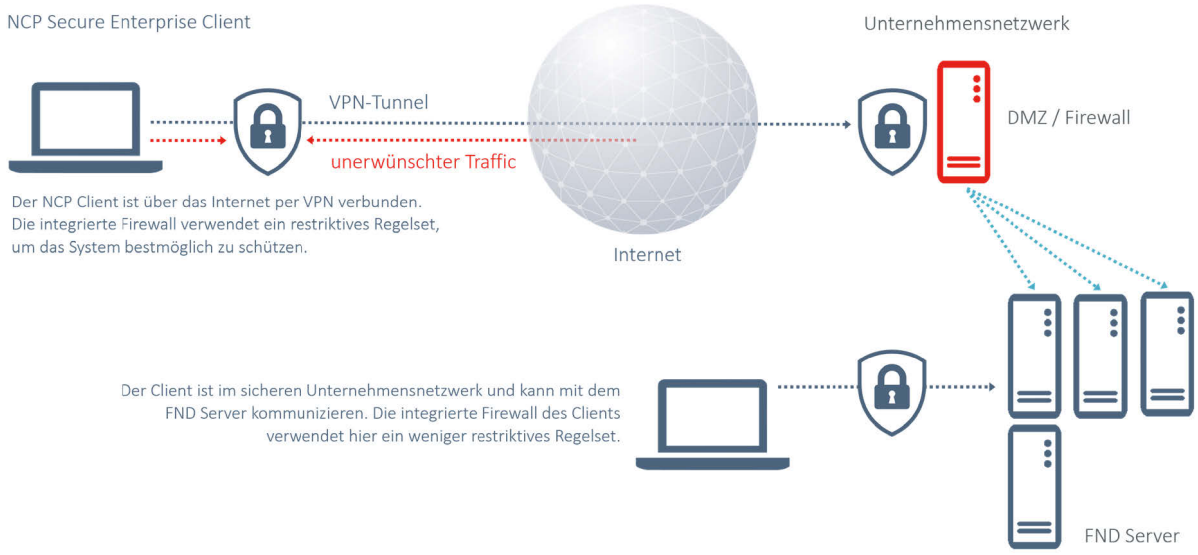

Abbildung 2 Szenario mit Friendly Net Detection

NCP engineering GmbH
Dombühler Straße 2
90449 Nürnberg

Tel.: +49 911 9968 0
vertrieb@ncp-e.com
www.ncp-e.com