



SecurITy
made
in
Germany

Trust Seal
www.teletrust.de/itsmig

NCP

SECURE COMMUNICATIONS ■

Datenblatt

NCP Dynamic Net Guard



Windows 32/64-Bit Betriebssysteme

- Zentrales Management
- Für PCs im Firmen- und Filialnetz sowie Einzelplatz-PCs via VPN
- Location Awareness durch Friendly Net Detection zur dynamischen Anpassung von Firewallregeln
- Schutz des Endgerätes bereits bei Systemstart
- Silent Mode
- Kostenlose 30-Tage-Vollversion

Leistungsumfang und Funktionalitäten

Der NCP Dynamic Net Guard (Win32/64) ist ein Baustein der ganzheitlichen NCP Secure Communications-Lösung. Sie schützt Laptops, Notebooks, Netbooks, Tablet PCs und Desktops mit Windows 32/64-Bit Betriebssystemen – Windows 10, 8.x, 7 und Windows Vista – vor unberechtigten Zugriffen. Ob mobil oder stationär, ob im Internet, WLAN oder LAN, ob in fremden oder bekannten Netzen, das Endgerät ist immer gegen Attacken abgeschottet.

In Abhängigkeit vom Standort greift ein spezielles Regelwerk. So unterscheiden sich beispielsweise Firewall-Regeln an einem öffentlichen Hotspot von Regelwerken im Homeoffice oder am firmeneigenen WLAN. Einerseits garantiert die Software totale Abschottung des PCs auf höchstem Sicherheitsniveau, andererseits eine definierte Offenheit z.B. für administrative Zwecke.

Welches Netz „sicher“ und welches „unsicher“ ist, erkennt die Firewall Software automatisch. Die „Friendly Net Detection“ (FND) aktiviert in Abhängigkeit von der jeweiligen Umgebung die erforderlichen Firewall-Regeln. Der große Vorteil gegenüber herkömmlichen Firewall-Lösungen besteht darin, dass sich ein im Firmennetz installierter FND-Server gegenüber dem Dynamic Net Guard Client authentisiert (Local Awareness) und damit die Erkennung eines vertrauenswürdigen Netzes 100%ig gewährleistet.

Es können Regelwerke für Ports, IP-Adressen, Segmente und Applikationen erstellt werden. Auch kann festgelegt werden, ob der Zugriff auf das



Internet (generell/bestimmte Ziele) und/oder nur auf das Firmennetz erlaubt ist. Alle Client-Einstellungen können durch den Administrator gegenüber Veränderungen durch den Anwender gesperrt werden. Sicherheitslücken durch vorsätzliche Manipulation oder Fehlbedienung des Anwenders sind ausgeschlossen.

Der NCP Dynamic Net Guard ist bereits bei Systemstart aktiv und schließt damit eine wesentliche Sicherheitslücke an mobilen und stationären PCs bereits während des Bootens.

Der „Silent Mode“ bewirkt, dass Anwender nicht durch ständige Rückfragen der Software während Ihrer Arbeit unterbrochen werden. Der Modus ist fest vorgegeben und verhindert die häufigste Fehlerquelle – das zweifelhafte, routinemäßige Bestätigen von Anfragen der Firewall durch den Anwender.

Der Dynamic Net Guard ist sowohl im lokalen Netzwerk als auch für Remote Access in Verbindung mit beliebigen VPN-Technologien nutzbar.

Zentrales Management

Die zentrale Verwaltung der NCP Dynamic Personal Firewall Clients erfolgt durch das bewährte NCP Secure Enterprise Management. Es bietet als „Single Point of Administration“ alle Funktionalitäten und Automatismen für einen wirtschaftlichen Rollout und Betrieb.

Alle Firewall-Regeln können pro Arbeitsplatz granular eingestellt werden.

Der NCP Dynamic Net Guard bietet, neben dem

Schutz des Endgerätes, spezielle, für den Einsatz im Remote Access-Betrieb optimierte Leistungsmerkmale. Aktiviert werden diese bei Nutzung des „NCP Internet Connectors“ für den Verbindungsaufbau.

Technische Daten Personal Firewall

Betriebssysteme	Windows (32 und 64 Bit): 10, Windows 8.x, Windows 7
Security Features	Stateful Packet Inspection, anwendungsbezogene Firewall-Regeln; Friendly Net Detection (Auswertung von: aktueller Netzwerkadresse, IP-Adresse und MAC-Adresse des DHCP-Servers); Secure Hotspot Logon; Differenzierte Firewall-Regeln bezüglich: Protokolle, Ports und Adressen
Zentrales Management	NCP Secure Enterprise Management
Konfigurationsparameter	Applikations- und verbindungsabhängige Filterregeln Protokoll-, port- und adressbezogene Filterregeln Vorgaben für die Erkennung von „friendly networks“ (IP-Adresse Netzwerk, Netzwerkmaske, IP-Adresse des DHCP-Server, MAC-Adresse) Logging-Einstellungen Zentrale Vorgabe der Zugangsmöglichkeiten auf die Firewallkonfiguration für den Benutzer Friendly Net Detection (FND)-Serverkonfiguration

Leistungsumfang des NCP Internet Connectors (Dialer)

Betriebssysteme	Windows (32 und 64 Bit): 10, Windows 8.x, Windows 7, Windows Vista
Übertragungsmedien	Internet, LAN, WLAN, GSM (inkl. HSCSD), GPRS, UMTS, LTE, HSDPA, analoges Fernsprechnetz, ISDN
Authentisierungsverfahren	PAP, CHAP, MS CHAP V.2; IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): erweiterte Authentifikation gegenüber Switches und Access Points (Layer 2); EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): erweiterte Authentifikation gegenüber Switches und Access Points auf Basis von Zertifikaten (Layer 2); Unterstützung von Zertifikaten in einer PKI: Soft-Zertifikate, Smart Cards und USB Tokens
Budget Manager	Verwaltung von Verbindungszeit und/oder –volumen für GPRS/UMTS und WLAN, bei GPRS/UMTS getrennte Verwaltung für Roaming im Ausland
Automatische Mediatype-Erkennung	Automatische Erkennung und grafische Anzeige aller verfügbaren Verbindungsarten, Auswahl des jeweils schnellsten Übertragungsmediums. Priorisierung in der Suchroutine: LAN, WLAN, DSL, UMTS/GPRS, ISDN, Modem
IP Address Allocation	DHCP (Dynamic Host Control Protocol)
Line Management	Short Hold Mode; Kanalbündelung (dynamisch im ISDN) mit frei konfigurierbarem Schwellwert; Timeout (zeit- und gebührengesteuert)
Point-to-Point Protokolle	PPP over ISDN, PPP over GSM, PPP over PSTN, PPP over Ethernet, LCP, IPCP, MLP, CCP, PAP, CHAP, ECP

Client Monitor
 Intuitive, grafische
 Benutzeroberfläche

Mehrsprachig (Deutsch, Englisch, Französisch);
 Konfiguration, Verbindungssteuerung und -überwachung,
 Verbindungsstatistik, Log-Files, Trace-Werkzeug für
 Fehlerdiagnose; Ampelsymbol für Anzeige des
 Verbindungsstatus; Integrierte Unterstützung von Mobile
 Connect Cards (PCMCIA, embedded); Konfigurations- und
 Profil-Management mit Passwortschutz,
 Konfigurationsparametersperre



Option: Upgrade VPN Client – NCP Secure Enterprise Client (Win32/64)
<https://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/>



NCP

SECURE COMMUNICATIONS ■

NCP engineering GmbH
Dombühler Straße 2
90449 Nürnberg
Germany

+49 911 9968 0
info@ncp-e.com
www.ncp-e.com

NCP engineering, Inc.
19321 US Highway 19 N, Suite 401
Clearwater, FL 33764
USA

+1 650 316 6273
info@ncp-e.com
www.ncp-e.com