NCP Friendly Net Detection Server

für Linux

Release Notes

Major Release: **3.00 r47008**
Datum: **März 2020**

Voraussetzungen

Linux Distributionen:

Die folgenden Linux Distributionen werden mit diesem Release unterstützt:

- Debian GNU/Linux 10.3
- Red Hat Enterprise Linux Release 8.1

1. Neue Leistungsmerkmale und Erweiterungen

Zertifikatsbasierte Authentisierung des Friendly Net Detection Servers mit TLS 1.2

Die Authentisierung des FND Servers am NCP Secure Client unterstützt ab dieser Version sowohl TLS 1.2 als auch TLS 1.0 sofern ein älterer NCP Secure Client verwendet wird.

2. Verbesserungen / Fehlerbehebungen

Passwort und PIN werden verschlüsselt in der Konfigurationsdatei abgelegt

Beim Start des NCP Friendly Net Detection Servers werden in der Konfigurationsdatei enthaltene, unverschlüsselte Benutzer-Passwörter und die Zertifikats-PIN ab dieser Version verschlüsselt in die Konfigurationsdatei zurückgeschrieben.

Die mitgelieferten Demo-Zertifikate wurden aktualisiert

3. Bekannte Einschränkungen

Keine.

4. Hinweise zum NCP Friendly Net Detection Server

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:
https://www.ncp-e.com/de/loesungen/vpn/remote-access-vpn-technologien/friendly-net-detection/

Eine Auflistung der im Produkt verwendeten Open Source Komponenten finden Sie im beigelegten Dokument „OpenSourceLicenseTerms.pdf“.

5. Leistungsmerkmale des NCP Friendly Net Detection Servers

Mit Hilfe der Friendly Net Detection (FND)-Technologie, ist der NCP Secure Client in der Lage ein vertrauenswürdiges, „freundliches“ Netzwerk automatisch zu erkennen. Daraus resultierend kann sich das Regelwerk der Firewall des NCP Secure Clients automatisch anpassen. So können beispielsweise vorkonfigurierte Zugriffe auf den Rechner des Anwenders automatisch im „befreundeten“ Firmennetz aktiviert werden, wogegen der Rechner in unbekannten Netzwerk-Umgebungen vor externen Zugriffen abgeschirmt wird.

- Der Friendly Net Detection Server (FNDS) ist ein separater Dienst, der unabhängig vom VPN-Gateway auf einem permanent verfügbaren Computer im „Friendly Net“ bzw. „bekannten Firmennetzwerk“ installiert wird. Dieser Dienst muss vom Anwender-Rechner bzw. dem NCP Secure Client aus allen Teilen des Netzwerks verfügbar sein. Dazu müssen in einigen Fällen ggf. die Router-Einstellungen geändert werden.
- Der im NCP Secure Client enthaltene Friendly Net Detection-Client (FNDC) wird über die Firewall-Einstellungen des NCP Secure Clients konfiguriert. Wird der Anwender-Rechner mit einem neuen Netzwerk verbunden, versucht der FNDC, eine Verbindung zum konfigurierten FNDS herzustellen. Im Falle einer erfolgreichen Authentisierung des FNDS am NCP Secure Client wird bestätigt, dass sich der Anwender Rechner in einem „Friendly Net“ befindet. Die Firewall-Regeln des NCP Secure Clients werden automatisch, entsprechend den Vorgaben durch den Administrator, geändert.
- Der Administrator konfiguriert alle Firewallregeln im NCP Secure Client sowohl für das „Friendly Net“ als auch für unbekannte Netzwerke. Die zugrundeliegende Firewall ist Teil der NCP Secure Entry und Enterprise Clients. Konfigurationssperren verhindern, dass ein Anwender selbsttätig die Firewallregeln ändert oder die Firewall deaktiviert. In zentral verwalteten Umgebungen kann diese Konfiguration mit Hilfe des NCP Secure Enterprise Managements durchgeführt werden.

Die Friendly Net Detection-Technologie basiert auf etablierten Standards, die eine konsistente Systemsicherheit gewährleisten und das System vor Fehlern schützen, die bei proprietären Lösungen häufig auftreten.

Betriebssysteme

Siehe Voraussetzungen auf Seite 1.

Sicherheitsfunktionen

Authentisierung
EAP, TLS oder Zertifikats-basierte Authentisierung zwischen dem NCP Friendly Net Detection Server und dem NCP Secure Client.

Unterstützung von Zertifikaten innerhalb einer PKI:

- Soft Zertifikate