NCP Secure Entry Mac Client

Service-Release 2.05 Rev. 32317
Januar 2017

Voraussetzungen

Apple OS X Betriebssysteme:

Folgende Apple OS X Betriebssysteme werden mit dieser Version unterstützt:
macOS 10.12
OS X 10.11
OS X 10.10

1. Neue Leistungsmerkmale und Erweiterungen

Unterstützung für macOS Sierra 10.12

2. Verbesserungen / Fehlerbehebungen

Keine

3. Bekannte Einschränkungen

In manchen Fällen kann es vorkommen, dass die deutsche Einstellung des macOS-Betriebssystems im Client nicht korrekt erkannt wird und die Client-GUI in englischer Sprache erscheint. In diesem Fall hilft ein Workaround mit der Eingabe des folgenden Befehls in der Kommandozeile:

```
defaults write com.ncp-e.ncpmon Language 1
```

Service-Release 2.05 Rev. 23310
Mai 2015

Aktuelle Ausgabe September 2015

Voraussetzungen

Apple OS X Betriebssysteme:

Folgende Apple OS X Betriebssysteme werden mit dieser Version unterstützt:
OS X 10.11 EL Capitan
OS X 10.10 Yosemite
OS X 10.9 Mavericks
OS X 10.8 Mountain Lion

1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Verbesserungen / Fehlerbehebungen

Optimierung des Startprozesses unter OSX 10.10 Yosemite

3. Bekannte Einschränkungen

Keine

Service-Release 2.05 Build 14711
Dezember 2013

Voraussetzungen

Apple OS X Betriebssysteme:

Folgende Apple OS X Betriebssysteme werden mit dieser Version unterstützt:
OS X 10.9 Mavericks
OS X 10.8 Mountain Lion

1. Neue Leistungsmerkmale und Erweiterungen

OS X 10.8 und 10.9 Unterstützung

Dieser Version unterstützt NUR OS X 10.9 und 10.8.

2. Verbesserungen / Fehlerbehebungen

Kein Verbindungsabbau wenn die Chipkarte gezogen wird

Frühere Probleme bei Einsatz dieses Features sind behoben.

Kompatibilitäts- und Zuverlässigkeits-Verbesserungen

3. Bekannte Einschränkungen

Keine

Service-Release 2.02 Build 14
Oktober 2011

Voraussetzungen

Apple OS X Betriebssysteme:

Folgende Apple OS X Betriebssysteme werden mit dieser Version unterstützt:
OS X 10.7
OS X 10.6
OS X 10.5

1. Änderungen in der Version 2.02 Build 14

DNS Domains im Tunnel auflösen

Im Konfigurationsfeld „IPsec-Adresszuweisungen" kann unabhängig davon, ob Split-Tunneling genutzt wird, definiert werden, welche DNS-Anfrage durch den VPN-Tunnel geleitet werden soll. Dazu wird der gewünschte DNS-Name unter „DNS Domains im Tunnel auflösen" eingetragen.

In der Standard-Einstellung eines neuen VPN-Profiles ist „DNS Domains im Tunnel auflösen" leer, was bewirkt, dass alle DNS-Anfragen am VPN-Tunnel vorbei an den DNS Server geschickt werden, der (vom Provider) aus dem Internet zugewiesen wird.

2. Fehlerbehebung

Auswahl einer definierten VPN-Verbindung

Unter bestimmten Umständen konnte in der Client-Oberfläche kein VPN-Profil aus der Profil-Auswahl selektiert werden. Dieser Fehler wurde behoben.

Kommunikation zwischen Zentralseite und Client bei Einsatz von XAUTH

Wurde die erweiterte Authentisierung (XAUTH) eingesetzt, schlug die Kommunikation zwischen Zentralseite und Client fehl, so dass die Dialoge zur zentralseitigen Abfrage eines neuen Passworts nicht korrekt angezeigt wurden (z. B. bei Einsatz von externer Authentisierung). Dieser Fehler wurde behoben.

3. Bekannte Einschränkungen

Keine

4. Hinweise zum NCP Secure Entry Mac Client

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:
http://www.ncp-e.com/de/downloads.html

Weitere Unterstützung bei Fragen zum NCP Secure Entry Mac Client erhalten Sie über die Mail-Adressen auf folgender Seite:
http://www.ncp-e.com/de/unternehmen/kontakt.html

Mail: support@ncp-e.com

5. Leistungsmerkmale

Betriebssysteme

Siehe Voraussetzungen auf Seite 1

Security Features

Der NCP Secure Entry Client unterstützt die Internet Society's Security Architecture für das Internet Protokoll (IPsec) und alle zugehörigen RFCs.

Personal Firewall

- Stateful Packet Inspection
- IP-NAT (Network Address Translation)
- Friendly Net Detection (automatische Umschaltung der Firewall-Regeln bei Erkennung des angeschlossenen Netzwerkes anhand des Adressbereichs oder des NCP FND-Servers*)
- differenzierte Filterregeln bezüglich: Protokolle, Adressen und Ports, Schutz des LAN-Adapters
- Im Gegensatz zur applikationsbasierten Konfiguration der Mac OS X-Firewall ist die Konfiguration dieser Firewall portbasierend.

Virtual Private Networking

- IPsec (Layer 3 Tunneling)
- IPsec-Proposals können determiniert werden durch das IPsec -Gateway (IKE, IPsec Phase 2)
- Kommunikation nur im Tunnel
- Message Transfer Unit (MTU) Size Fragmentation und Reassembly
- Dead Peer Detection (DPD)
- Event log
- Network Address Translation Traversal (NAT-T)
- IPsec Tunnel Mode

Authentisierungsverfahren

- Internet Key Exchange (IKE):
  - Aggressive Mode und Main Mode,
  - Quick Mode
  - Perfect Forward Secrecy (PFS)
  - IKE Config-Mode zur dynamischen Zuweisung von priv. IP-Adresse aus Adress-Pool
  - Pre-shared Secrets oder RSA-Signaturen (und zugehöriger Public Key Infrastructure)
- XAUTH für erweiterte Benutzer-Authentisierung
  - One-Time-Passwörter und Challenge Response Systeme
  - Zugangsdaten aus Zertifikaten (PKI)
- Unterstützung von Zertifikaten in einer PKI:
  - Multi-Zertifikats-Konfiguration für die Schnittstellen PKCS#11 und PKCS#12
- Seamless Rekeying (PFS)
- IEEE 802.1x:
  - Extensible Authentication Protocol – Message Digest 5 (EAP-MD5): Erweiterte Authentisierung gegenüber Switches und Zugriffspunkten (layer 2)
  - Extensible Authentication Protocol – Transport Layer Security (EAP-TLS): - gegenüber Switches und Zugriffspunkten auf der Basis von Zertifikaten (Layer 2)
- RSA SecurID Ready

Verschlüsselung (Encryption)

- Symmetrisch: AES 128, 192, 256 Bit; Blowfish 128, 448 Bit; Triple-DES 112 /168 Bit
- Asymmetrisch: RSA bis 2048 Bit, für dynamischen Schlüsselaustausch
- Seamless Rekeying (Perfect Forward Secrecy)

FIPS Inside

Der IPsec Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 zertifiziert (Zertifikat #1051). Die FIPS Kompatibilität ist immer gegeben, wenn die folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden:

- DH-Gruppe: Gruppe 2 oder höher (DH ab einer Länge von 1024 Bit)
- Hash-Algorithmen: SHA1, SHA 256, SHA 384 oder SHA 512 Bit
- Verschlüsselungsalgorithmen: AES mit 128, 192 und 256 Bit oder Triple DES

Hash / Message Authentisierungs-Algorithmen

- SHA1, SHA-256, SHA-384, SHA-512, MD5
- Diffie Hellman Gruppen 1, 2, 5, 14 für asym. Schlüsselaustausch und PFS

Public Key Infrastructure (PKI) - Starke Authentisierung

- X.509 v.3 Standard
- PKCS#11-Schnittstelle für Verschlüsselungs-Token (Token / Smartcards)
- PKCS#12-Schnittstelle für private Schlüssel (Soft-Zertifikate)
- Administrative Vorgabe für die Eingabe beliebig komplexer PINs
- Widerrufs- und Sperrverfahren (Revocation):
  - End-entity Public-key Certificate Revocation List (EPRL vormals CRL)
  - Certification Authority Revocation List, (CARL vormals ARL)
  - Online Certificate Status Protocol (OCSP)

Networking Features

Sichere Netzwerk-Schnittstelle

- Interface Filter
  - NCP Interface-Filter stellen die Schnittstelle zu allen Netzwerk-Interfaces der PPP- und Ethernet-Familie her
  - Volle Unterstützung von Wireless Local Area Network (WLAN)
  - Volle Unterstützung von Wireless Wide Area Network (WWAN)

Netzwerkprotokoll

- IP

Verbindungs-Medien

- LAN
- Unterstützte Verbindungsmedien für Apple oder Medienschnittstellen und Management Tools von Drittherstellern:
  - LAN / Ethernet
  - WLAN
  - GPRS / UMTS und GSM
  - ISDN
  - Modem

- iPhone tethering via USB oder Bluetooth

Split Tunneling

- Bei Split-Tunneling ist die genaue Spezifizierung jener Domains möglich, deren DNS-Pakete über den VPN-Tunnel geleitet werden sollen

VPN Path Finder

- NCP VPN Path Finder Technology
  - Fallback to HTTPS (port 443) from IPsec wenn weder Port 500 noch UDP Encapsulation möglich sind (Vorausetzung: NCP Secure Enterprise Server V 8.0 oder später)

IP Address Allocation

- Dynamic Host Control Protocol (DHCP)
- Domain Name Service (DNS): Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server

Line Management

- Dead Peer Detection mit konfigurierbarem Zeitintervall

Datenkompression

- IPCOMP (LZS), deflate

Weitere Features

- UDP-Encapsulation, Importfunktion der Dateiformate:*.ini, *.pcf, *.wgx, *.wge and *.spd.

Internet Society RFCs und Drafts

- Security Architecture for the Internet Protocol and assoc. RFCs (RFC2401 - 2409),
  - Internet Key Exchange Protocol (IKE) (includes IKMP/Oakley) (RFC 2406),
  - Negotiation of NAT-Traversal in the IKE (RFC 3947),
  - UDP encapsulation of IPsec Packets (RFC 3948),
  - IKE Extended Authentication (XAUTH), IKE configure (IKECFG) and Dead Peer Detection (DPD)

Client Monitor (intuitive grafische Benutzeroberfläche)

- zweisprachig (Deutsch, Englisch)
- Ampelsymbol für Anzeige des Verbindungsstatus
- Konfiguration, Verbindungsstatistik, Log-Files (farbige Darstellung, Copy&Paste-Funktion)
- Konfigurations- und Profil-Management mit Passwortschutz
- Trace-Werkzeug für Fehlerdiagnose
- Konfigurationssperren
- Monitor kann firmenspezifisch mit Firmenlogo und Support-Informationen ausgestattet werden
- Tipp des Tages: In die Oberfläche des Client-Monitors ist ein Feld für Konfigurationstipps und Anwendungsbeispiele integriert
- Der Client Monitor kann bei Systemstart sowohl als Großbild oder als Icon in der Menüleiste angezeigt werden

*) Der NCP FND-Server kann kostenlos als Add-On hier heruntergeladen werden:
http://www.ncp-e.com/de/downloads/software.html

Eine kostenlose 30-Tage Vollversion können Sie hier herunterladen:
http://www.ncp-e.com/de/downloads/software.html