



Service-Release: 4.60 r29048
Datum: Oktober 2021

Voraussetzungen

Apple macOS Betriebssysteme:

Folgende macOS-Betriebssysteme werden mit dieser Version auf Hardware mit Apple M1 Chip oder Intel CPU unterstützt:

- macOS 11 Big Sur
- macOS 12 Monterey

Einschränkung in dieser Version 4.60

Diese Version des Clients enthält, im Gegensatz zu vorherigen Clientversionen, keine Firewallfunktionalität. Anwender, die diese Firewallfunktionalität nutzen möchten, sollten – sofern möglich – die Vorversion 4.0 des Clients nutzen.

1. Neue Leistungsmerkmale und Erweiterungen

Anpassung an macOS 11 Big Sur und macOS 12 Monterey sowie Apple M1 Chip

Der Client ist ab dieser Version kompatibel zum Apple M1 Chip als auch zur bisherigen Intel CPU. Als Betriebssystem werden macOS 11 Big Sur oder macOS 12 Monterey vorausgesetzt.

2. Verbesserungen / Fehlerbehebungen

Unterstützung von 250 Split Tunnel Netzen

Es werden nun für IPv4 als auch für IPv6 bis zu 250 Split Tunnel Netze beim Import einer INI-Konfigurationsdatei unterstützt.

Unterstützung von DNS Domains in der INI-Datei

DNS Domains die durch den VPN-Tunnel aufgelöst werden sollen, können nun über INI-Datei importiert werden.

Die Benutzerrechte des Installationsverzeichnis wurden angepasst

Fälschlicherweise war es einem Benutzer möglich durch falsch gesetzte Benutzerrechte des Installationsverzeichnis Aktionen im Root-Kontext auszuführen. Dieses Problem wurde behoben.

MFA-Dialog wird nicht vollständig angezeigt

Bei der Verwendung von Multi-Faktor-Authentifizierung kam es zu Anzeigefehlern. Das bisherige Anzeigefenster war zu klein für besonders lange Texte. Dieses Problem wurde behoben.



Fehlerhaftes Caching von Domainnamen bei Profilwechsel

Domainnamen werden fälschlicherweise nach Profilwechsel zwischengespeichert. Dieses Problem wurde behoben.

Konfiguration Split Tunneling: "Auch lokale Netze im Tunnel weiterleiten" hinzugefügt

Bisher war es nur im Windows-Client möglich lokale Netze im Tunnel weiterzuleiten. Dies ist nun auch im macOS Client möglich.

Ungewollte Proposaländerung (DH-Gruppe) nach Profilbearbeitung

Wurde in der INI-Konfigurationsdatei die DH-Gruppe ausschließlich in der Sektion IKEPOLICY konfiguriert, so wurde dieser Wert nach dem Bearbeiten des Profils im Client auf den Standardwert der DH-Gruppe gesetzt. Dieses Problem wurde behoben.

Probleme bei der Konfigurationsänderung von IPv4 auf IPv6

Nach Umschalten im Profil von IPv4 auf IPv6 war unter Split Tunneling die IPv6 Tabelle nicht verfügbar. Dieses Problem wurde behoben.

Unterstützung von PEM- und DER-Format unabhängig von der Datei-Endung

Bisher wurden nur Dateien mit .pem-Dateiendung als PEM Format gelesen, alle anderen wurden ausschließlich als binäres DER-Format gelesen. Nun werden auch für .cer- und .crt-Dateiendungen das DER- als auch das PEM-Format unterstützt.

Fehlende Menüleiste nach Start des Rechners

Nach dem Start des Rechners wurde unter bestimmten Umständen die Menüleiste des Clients trotz aktiver Client-GUI im Vordergrund nicht angezeigt. Dieses Problem wurde behoben.

Fehler beim Import der Konfigurationssperren

Das Importieren von Konfigurationssperren via INI-Konfigurationsdatei war fehlerhaft. Dieses Problem wurde nun behoben.

Update auf OpenSSL Version 1.0.2u-8

Die im NCP Secure Client verwendete OpenSSL-Version wurde auf 1.0.2u-8 angehoben. Damit wurde die OpenSSL-Sicherheitslücke CVE-2020-1971 geschlossen.

Optimiertes Handling von DNS-Requests

Einhergehend mit dem neu implementierten Netzwerkadapter konnte das Handling von DNS-Requests verbessert werden.

Verbesserungen bei VPN Path Finder in Verbindung mit einem konfigurierten Proxy

Sollte bisher eine VPN Verbindung mittels Pathfinder und einem Proxy für Pathfinder hergestellt werden, erfolgte keine Anfrage am Proxy-Server. Durch eine Verbesserung bei der dynamischen Konfigurationsübernahme ist dies nun möglich.



Absturz des ncprwsmac-Dienstes

In seltenen Fällen kam es zum Absturz des ncprwsmac-Dienstes. Dieses Problem wurde behoben.

3. Bekannte Einschränkungen

Ablageort für Zertifikatsdateien

Einhergehend mit Anpassungen für macOS Catalina können p12-Zertifikatsdateien im Client nicht von beliebigen Ablageorten genutzt werden. Im Falle der automatisch erzeugten Verzeichnisse im Home-Verzeichnis des Benutzers wie z.B. Dokumente, Schreibtisch, Downloads, etc., erscheint der Fehler „Zugriff verweigert“. Werden die Zertifikatsdateien direkt in einem Verzeichnis unterhalb des Benutzer-Home-Verzeichnisses abgelegt, so funktioniert der Zugriff.



Major Release: 4.00 r46079
Datum: Oktober 2019

Voraussetzungen

Apple macOS Betriebssysteme:

Folgende Apple macOS Betriebssysteme werden mit dieser Version unterstützt:

- macOS Catalina 10.15
- macOS Mojave 10.14
- macOS High Sierra 10.13

1. Neue Leistungsmerkmale und Erweiterungen

Anpassung an macOS Catalina 10.15

Der Client ist ab dieser Version notariert und damit vollständig kompatibel zu macOS Catalina 10.15. Bei der Installation muss die zu installierende Kerneextension explizit in den Einstellungen unter Sicherheit erlaubt werden.

Virtueller Netzwerkadapter

Der Client stellt sich in macOS mit einem eigenen Netzwerkadapter dar. Dies ermöglicht u.a. VoIP-Anwendungen die Kommunikation durch den VPN-Tunnel. Des Weiteren kann der Client dank dieses Netzwerkadapters auch ein IP-Protokoll innerhalb des VPN-Tunnels nutzen obwohl es im tatsächlich verwendeten physischen Netzwerk nicht verwendet wird. Beispiel: Nutzung von IPv6 innerhalb des VPN-Tunnels obwohl im angeschlossenen Netzwerk nur IPv4 vorhanden ist.

Verbinden/trennen-Menü im Dock-Icon

Verfügt der VPN-Client über ein konfiguriertes VPN-Profil, so kann die ausgewählte Verbindung durch Rechtsklick über dem Dock-Menü-Icon aufgebaut bzw. getrennt werden.

2. Verbesserungen / Fehlerbehebungen

Optimiertes Handling von DNS-Requests

Einhergehend mit dem neu implementierten Netzwerkadapter kann das Handling von DNS-Requests verbessert werden. Dabei sind folgende zwei Fälle zu unterscheiden:

1. Kein Split Tunneling-Betrieb
In diesem Betriebsmodus geschieht jegliche Kommunikation zu anderen IP-Adressen, die nicht innerhalb des aktuell verwendeten IP-Adressbereiches liegen, durch den VPN-Tunnel. Dies gilt demzufolge ebenso für DNS-Requests.
2. Split-Tunneling Betrieb
In diesem Betriebsmodus wird innerhalb der Split Tunneling-Konfiguration das oder die IP-



Remotenetzwerk(e) definiert. Werden nun Ziele innerhalb des Remotenetzwerkes adressiert, so fließen die Daten durch den VPN-Tunnel. Alle anderen Daten, insbesondere auch DNS-Requests fließen am VPN-Tunnel vorbei. Dadurch lassen sich Ziele im Remotenetzwerk zunächst nicht über ihren Domainnamen erreichen, denn typischerweise lösen allgemein erreichbare DNS-Server keine firmeninternen DNS-Namen auf.

Dieses Problem lässt sich durch die explizite Konfiguration der internen Domainnamen, die innerhalb des Remotenetzwerkes liegen, lösen. So bewirkt der Eintrag `firma.local`, dass entsprechende DNS-Requests, z.B. `intranet.firma.local`, durch den VPN-Tunnel an firmeninterne DNS-Server fließen.

Durch diese Konfigurationsoption lässt sich der Datenverkehr durch den VPN-Tunnel und am VPN-Tunnel vorbei komplett trennen.

Neuer Verbindungsmodus

Der Verbindungsmodus „automatisch“ wurde entfernt und dafür der Modus „immer“ hinzugefügt. Ist „immer“ konfiguriert, so versucht der Client zu jeder Zeit einen VPN-Tunnel aufzubauen. Dies geschieht im Unterschied zum Modus „automatisch“ ohne anliegende, zu versendende, Daten.

3. Bekannte Einschränkungen

Ablageort für Zertifikatsdateien

Einhergehend mit Anpassungen für macOS Catalina können p12-Zertifikatsdateien im Client nicht von beliebigen Ablageorten genutzt werden. Im Falle der automatisch erzeugten Verzeichnisse im Home-Verzeichnis des Benutzers wie z.B. `Dokumente`, `Schreibtisch`, `Downloads`, etc., erscheint der Fehler „Zugriff verweigert“. Werden die Zertifikatsdateien direkt in einem Verzeichnis unterhalb des Benutzer-Home-Verzeichnisses abgelegt, so funktioniert der Zugriff.



4. Hinweise zum NCP Secure Entry macOS Client

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:

<https://www.ncp-e.com/de/service/download-vpn-client/versionsinformationen/>

E-Mail: support@ncp-e.com

5. Leistungsmerkmale

Betriebssysteme

Siehe Voraussetzungen auf Seite 1.

Security Features

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

Virtual Private Networking / RFC-konformes IPsec (Layer 3 Tunneling)

- IPsec Tunnel Mode
- IPv4/6 Dual Stack-Unterstützung
- IPsec-Proposals werden über das IPsec-Gateway ausgehandelt (IKE, Phase 2)
- Kommunikation nur im Tunnel
- Message Transfer Unit (MTU) Size Fragmentation und Re-assembly

Verschlüsselung (Encryption)

Symmetrische Verfahren:

AES-CBC 128, 192, 256 Bit;

AES-CTR 128, 192, 256 Bit;

AES-GCM 128, 256 Bit (nur IKEv2);

Blowfish 128, 448 Bit;

Triple-DES 112, 168 Bit;

Dynamische Verfahren für den Schlüsselaustausch:

RSA bis 4096 Bit;

ECDSA bis 521 Bit, Seamless Rekeying (PFS);

Hash Algorithmen: SHA, SHA-256, SHA-384, SHA-512, MD5;

Diffie-Hellman-Gruppen: 1, 2, 5, 14-21, 25-30 (ab Gruppe 25: Brainpool-Kurven);

Schlüsselaustauschverfahren

IKEv1 (Aggressive Mode und Main Mode): Pre-shared key, RSA, XAUTH;

IKEv2: Pre-shared key, RSA, EAP-MS CHAPv2, EAP-MD5, EAP-TLS, EAP-PAP,

Signature Authentication (RFC 7427), IKEv2 Fragmentation (RFC 7383);

Next Generation Network Access Technology



VPN Path Finder

NCP VPN Path Finder Technology: Fallback IPsec / HTTPS (Port 443) von IPsec wenn Port 500 bzw. UDP Encapsulation nicht möglich ist. *

FIPS Inside

Der Secure Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 gemäß Implementation Guidance section G.5 guidelines zertifiziert (Zertifikat #1747).

Die FIPS-Kompatibilität ist immer gegeben, wenn einer der folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden:

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

Split Tunneling

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

Authentisierungsverfahren

Internet Key Exchange (IKE):

Aggressive Mode, Main Mode,
Quick Mode, IKEv2

Perfect Forward Secrecy (PFS),

IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP-Adresse),

Pre-shared Secrets oder RSA-Signaturen (mit entsprechender Public Key Infrastructure);

Benutzer-Authentisierung:

XAUTH für erweiterte Benutzer-Authentisierung,
One-Time-Passwörter und Challenge Response Systeme,
Zugangsdaten aus Zertifikaten;

Unterstützung von Zertifikaten in einer PKI:

Multi-Zertifikats-Konfiguration für die Schnittstellen PKCS#11 und PKCS#12;

Maschinen-Authentisierung:

Zertifikatsbasierte Authentisierung mittels Zertifikaten aus dem Dateisystem oder dem macOS-Schlüsselbund;

Seamless Rekeying (PFS);

IEEE 802.1x:

EAP-MD5: Extensible Authentication Protocol (Message Digest 5), erweiterte Authentisierung gegenüber Switches und Zugriffspunkten (Layer 2);

EAP-TLS: Extensible Authentication Protocol (Transport Layer Security), erweiterte Authentisierung gegenüber Switches und Zugriffspunkten auf Basis von Zertifikaten (Layer 2);

RSA SecurID Ready;

Next Generation Network Access Technology



IP Adress-Zuweisung

DHCP (Dynamic Host Configuration Protocol);

IKE Config Mode (IKEv1);

Config Payload (IKEv2);

DNS (Domain Name Service): Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server. Bei Split-Tunneling ist die genaue Spezifizierung jener Domains möglich, deren DNS-Pakete über den VPN-Tunnel geleitet werden sollen.

Starke Authentisierung (Standards)

X.509 v.3 Standard;

Schnittstellen zur Zertifikatsunterstützung in einer PKI:

PKCS#11-Schnittstelle für Authentisierungslösungen von Drittanbietern (Token / Smartcards);

PKCS#12-Schnittstelle für private Schlüssel (Soft-Zertifikate);

Line Management

DPD (Dead Peer Detection) mit konfigurierbarem Zeitintervall;

Timeout;

VPN on Demand für den automatischen Aufbau des VPN-Tunnels und die ausschließliche Kommunikation darüber;

Internet Society, RFCs und Drafts

RFC 4301 (IPsec), RFC 4303 ESP, RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IKEv1, RFC 3526, ISAKMP, RFC 7296 (IKEv2), RFC 4555 (MOBIKE), RFC 5685 (Redirect), RFC 7383 (Fragmentation), RFC 7427, 3279 Section 2.2.3, 3447 Section 8 (Signature Authentication), RFC 5903, 6954, 6989, 4754 (ECC), RFC 2451, 3686 (AES with ESP), 5930 (AES-CTR), 4106 (AES-GCM), 5282, 6379 (Suite B), RFC 3447 Section 8 (Padding)

Client GUI

Intuitive graphische Benutzeroberfläche

Deutsch, Englisch;

Konfigurations-Update;

Profilauswahl;

Verbindungssteuerung und -überwachung, Verbindungsstatistik, Log-Files;

Fehlerdiagnose-Export;

Netzwerkinformationen;

* Voraussetzung: NCP Secure Enterprise VPN Server