### FORSCHUNGSZENTRUM JÜLICH GmbH

Jülich Supercomputing Centre 52425 Jülich, ☎ (02461) 61-6402

JuNet-Helpdesk, 🖀 (02461) 61-6440

#### **Technische Kurzinformation**

FZJ-JSC-TKI-0410 W.Anrath, S.Werner 05.09.2023

## Virtual Private Networks – Cisco Secure Client / Anyconnect VPN Microsoft Windows / Linux / macOS

### Inhaltsverzeichnis

- 1. Einführung
- 2. Distribution der Cisco Secure Client / Anyconnect VPN Software
- 3. Windows 10 / Windows 11
- 4. Linux (Ubuntu 20.04 LTS)
- 5. macOS
- 6. FAQ

## 1. Einführung

Der Cisco Secure Client / Anyconnect VPN (kurz: Anyconnect) ist das favorisierte VPN Zugangsangebot des JSC. Dieser VPN Client kann als Nachfolger der bisherigen IKEv1/IPSEC-basierten VPN Varianten bei Bedarf eingesetzt werden.

Insbesondere können bewährte Mechanismen wie beispielsweise die unterschiedlichen Tunnel-Policies *fzj* oder *fzj-nosplit* (siehe FAQ Frage 8) unmittelbar benutzergesteuert ausgewählt werden. Zudem kann bei Bedarf der Anyconnect VPN Client parallel zu L2TP/IPSEC (TKI-0387) installiert werden. Die Kompatibilität mit den Virenscannern ,TREND Micro Apex One' und ,Microsoft Windows Defender' ist gegeben.

Die Anyconnect-Software und die entsprechenden VPN-Gateway-Konfigurationen werden in vielen wissenschaftlichen Einrichtungen angeboten. Wechselseitig ist damit eine entsprechende Interoperabilität und Konnektivität zwischen den Forschungseinrichtungen gewährleistet. Technik – Hintergrund: Die Absicherung der Datenübertragung erfolgt mit TLS (TCP Port 443) oder DTLS (UDP Port 443). Die DTLS basierte Übertragung wird dabei bevorzugt.

Voraussetzung zur Nutzung dieser Software ist ein gültiges Benutzerzertifikat. Hinweis: Aufgrund von geänderten Anforderungen an Benutzerzertifikate hat der DFN diesen Dienst zum 29.08.2023 eingestellt. Der neue Dienstleister Sectigo (GEANT TCS) übernimmt ab dann die Ausstellung der Benutzer-Zertifikate.

Zertifikatswünsche (GEANT TCS) müssen per formloser E-Mail an user-services.jsc@fzjuelich geschickt werden. Nach einer eventuellen Ausweiskontrolle erhalten Sie eine E-Mail Einladung mit einem Link (Antragsformular).

Zulassungen/Accounts (Mitarbeiter) zur VPN-Benutzung können für Mitarbeiter beim "Office for User Services (user-services.jsc@fz-juelich.de)" beantragt werden

https://intranet.fz-juelich.de/de/organisation/it-portal/software\_services/infrastruktur/vpn

Sollten Zugänge für Kooperationspartner erforderlich sein, ist eine individuelle Konfiguration nötig. Für Beratung und Fragen dazu stehen die Ansprechpartner im JSC zur Verfügung (EMAIL: vpn@fz-juelich.de).

## 2. Distribution der Cisco Secure Client / Anyconnect VPN Software

Die Installation (Administrator-Rechte nötig) sollte *OFFLINE* erfolgen. Dazu können die sogenannten *PreDeploy Images* verwendet werden. Diese werden auf dem System pcsrv

\\pcsrv.zam.kfa-juelich.de\Public\VPN-Software\Cisco-Anyconnect

zum Download im Intranet angeboten. Bitte halten Sie kurzzeitig für die Installation den Virenscanner an.

Sollte die Cisco Secure Client / Anyconnect VPN Software (kurz: Anyconnect) auf einem System nicht lauffähig oder installierbar sein, steht mit der Open Source Lösung OpenConnect eine kompatible Alternative zur Verfügung. Insbesondere Ubuntu Anwender können die mit der Distribution bereitgestellten Pakete installieren und nutzen.

## 3. Windows 10 / Windows 11

VPN-Gateways: wingate.zam.kfa-juelich.de

Voraussetzung für den erfolgreichen Verbindungsaufbau ist ein gültiges Benutzerzertifikat (DFN oder Sectigo GÉANT TCS) im Windows-Zertifikatspeicher (Zertifikate – Aktueller Benutzer). Die Installation der VPN-Software erfordert Administratorrechte.

Die Installation kann mit dem bereitgestellten Pre-Deployment-Image (oder neuer)

cisco-secure-client-win-5.0.03072-core-vpn-predeploy-k9.msi

erfolgen. Benutzung:

• Sie können ab sofort mit dem installierten Programm die Verbindung herstellen.

٠

• Sie finden das Programm unter Start - Alle Apps - Cisco Secure Client

🕙 Cisco	Secure Clie	ent		-		×	oder ,Backup-Zugang'
	Rea wi	<b>/Connect V</b> ady to conne ngate.zam.k	<b>PN:</b> ct. fa-juelich.de	×	Connect	-	wingateb.zam.kfa- juelich.de
\$ (	D					cisco	
Cisco	Secure Clie Please ente Group: Username: Password:	ent   winga r your usern FZJ-NOSP	te.zam.kfa-ju ame and pas	uelich.de sword.	× M (si	ögliche iehe FA PN-Ben	Group-Policy auswählen. Q Frage 8) nutzerkennung!
Cisco Secure	Client	··· ×	ОК	Cancel			
Conn	connect VPN nected: wingate.zam 소 ENG 다 다 다	.kfa-juelich.de 11:00	0	Verbindun	os-ICON	in der	Task-Leiste

Verbindungs-ICON in der Task-Leiste:



Detailinformation (hier nach dem ,CONNECT') anzeigen durch ,Click' auf das Symbol.

Cisco Secure Client 1111111 Secure Client **CISCO** Virtual Private Network (VPN) Preferences Statistics Route Details Firewall Message History 10:58:46 Contacting wingate.zam.kfa-juelich.de. 10:59:58 User credentials entered. 10:59:58 Please respond to banner. 11:00:26 User accepted banner. 11:00:26 Establishing VPN session... 11:00:27 The Cisco Secure Client - Downloader is performing update checks... 11:00:27 Checking for profile updates... 11:00:27 Checking for product updates... 11:00:27 Checking for customization updates... 11:00:27 Performing any required updates...11:00:27 The Cisco Secure Client - Downloader update checks have been completed. 11:00:27 Establishing VPN - Initiating connection... 11:00:27 Establishing VPN session... 11:00:27 Establishing VPN - Examining system ... 11:00:27 Establishing VPN - Activating VPN adapter... 11:00:28 Establishing VPN - Configuring system... 11:00:28 Establishing VPN... 11:00:28 Connected to wingate.zam.kfa-juelich.de. Clear Mittlerweile haben zahlreiche Anwender im HomeOffice eine über DS-Lite realisierte Internet Anbindung; in diesem Fall ist das Protokoll IPv6 beim Verbindungsaufbau zu favorisieren (die suboptimale Kombination aus Carrier-Grade-NAT und UDP beim Internet Provider wird dabei vermieden).

Soll der Transport über IPv6 erfolgen, können die VPN-Gateways über die vollqualifizierten Namen (FQDNs)

wingate6.zam.kfa-juelich.de wingateb6.zam.kfa-juelich.de

erreicht werden. Im VPN-Tunnel werden sowohl IPv4 als IPv6 Nutzerdaten übertragen. Beispiel und Kontrolle: IPv6 VPN-Tunnel und wingate6b.zam.kfa-juelich.de

ISCO Secure Client		-  ×
Sec	ure Client	()
tual Private Network (VPI	۷)	
ferences Statistics Route Det	ails Firewall Message History	
Connection Information State: Tunnel Mode (IPv4): Tunnel Mode (IPv6): Dynamic Tunnel Exclusion: Dynamic Tunnel Inclusion: Duration: Session Disconnect: Management Connection State:	Connected Split Exclude Split Exclude None None 00:00:41 None Disconnected (user tunnel active)	· •
Address Information Client (IPv4): Client (IPv6): Server:	134.94.57.191 2001:638:404:3800:0:0:3800:ACC3 2001:638:404:6FB8:0:0:6FB8:1	wingate6.zam.kfa-juelich.de

#### Fehlerursachen und Meldungen:

(I) das Benutzerzertifikat ist nicht korrekt installiert oder vorhanden



(II) lokale Remote Desktop Session (RDP) oder Internetverbindungsfreigabe (ICS) aktiv



## 4. Linux (Ubuntu 20.04 LTS)

#### Voraussetzung für den erfolgreichen Verbindungsaufbau ist ein gültiges Benutzerzertifikat (DFN oder Sectigo GÉANT TCS). Die Installation der VPN-Software erfordert ROOT-Rechte.

Aufgrund der besseren Integration in die diversen Linux-Derivate wird der Einsatz der kompatiblen Open-Source Software ,openconnect' empfohlen. Diese Software ist kompatibel zur Cisco Anyconnect Lösung und wird bei allen gängigen Derivaten als installierbares Paket (openconnect) angeboten. Die Steuerung der VPN-Verbindung kann auf Shell-Ebene (ROOT-Rechte) oder bei Bedarf auch durch den Network-Manager in der grafischen Benutzeroberfläche erfolgen:

openconnect -k PKCS12 -c {file.pfx} wingate.zam.kfa-juelich.de

Zur Vorbereitung der Konfiguration im Network-Manager ist gegebenenfalls nach der Software-Installation (bei Ubuntu Gnome Desktop: network-manager-openconnect und network-manager-openconnect-gnome)

> sudo apt install network-manager-openconnect sudo apt install network-manager-openconnect-gnome

die eigene persönliche PKCS12-Datei (hier im Beispiel: file.pfx gennant - Benutzerzertifikat aus der Global-Zertifizierungshierarchie des DFN-Vereins oder alternativ von GEANT TCS) mit den folgenden Befehlen zu konvertieren; schützen Sie dabei den exportierten privaten Schlüssel mit einer "Pass Phrase":

openssl	pkcs12	-in	{file.pfx}	-clcerts	-nokeys	-out	myCert.pem
openssl	pkcs12	-in	{file.pfx}	-nocerts		-out	myKey.pem

## Erstellen der Konfiguration:

Q	Settings		Network		
۲	Network				
*	Bluetooth		Wired	+	
Ç	Background		Connected - 100 Mb/s		
P	Appearance	Cancel	Add VPN	+	
Û	Notifications	Layer 2 T	unneling Protocol (L2TP)		
Q	Search	Compatible	e with Microsoft and other L2TP VPN servers.		
	Applications	Multi-pro Compatible	e with Cisco AnyConnect, Juniper Network Connect and Junos Pulse, and PAN GlobalProtect SSL VPNs.		
₿	Privacy	OpenVPI	N		
$\bigcirc$	Online Accounts	Compatible	e with the OpenVPN server.		
∝°	Sharing	Point-to- Compatible	Point Tunneling Protocol (PPTP) e with Microsoft and other PPTP VPN servers.		
1	Sound	Cisco Co	mpatible VPN (vpnc) e with various Cisco, Juniper, Netscreen, and Sonicwall IPsec-based VPN gateways.		
(•)	Power				

ancelual	eways:	OTLS Ope	nconnect - win	gate VPN	ļ
etails	Identity	IPv4	IPv6		
Name	DTLS Oper	nconnect -	wingate		
Gen	eral				
	VPN Prot	ocol	Cisco AnyCo	nnect or openconne	ct 🔻
	Gat	eway		wingate.zam.kfa-j	uelic
	CA Certif	icate		(None)	F
	F	гоху			
<i>I</i>	Allow securit	y scanner	trojan (CSD)		
	Trojan (C	SD) Wrapp	oer Script		
	R	eported C	)S		
Cert	ificate Auth	enticatio	n		
	Us	er Certific	ate	myCert.pem	F
		Private I	Key	🖻 myKey.pem	F
	Jse FSID for	key passpl	hrase		
F	Prevent user	from man	ually accepting	invalid certificates	
Soft	ware Token	Authent	ication		
	Token Mo	de	Disabled		•
				Token	Secret

## wingate.zam.kfa-juelich.de

oder (Backup-Zugang)

wingateb.zam.kfa- juelich.de

Aufbau der VPN-Verbindung (bzgl. ,GROUP' siehe FAQ Frage 8):

	8	Å	● 🕛 ◄
<b>(</b> )			
			0
Å	Wired Connected		•
VPN	VPN Off		-
	DTLS Openconnect -	win	$\bigcirc$



## 5. macOS

Voraussetzung für die nachfolgenden Schritte ist ein gültiges Benutzerzertifikat aus der Global-Zertifizierungshierarchie des DFN-Vereins oder von GEANT TCS.

● ⊖ ⊖	Schlüsselbundverwalt	ung	
Klicken Sie hier	, um den Schlüsselbund "Anmeldung" zu sch	lützen Q	
Schlüsselbunde			
System System-Roots			
Kataania	Name	Art	Verfällt
<ul> <li>Alle Objekte</li> <li>Kennwörter</li> <li>Sichere Notize</li> <li>Meine Zertifika</li> <li>Schlüssel</li> <li>Zertifikate</li> </ul>	Deutsche Telekom Root CA 2 DFN-Verein PCA Global - G01 FZJ Certification Authority - G02 Vorname Name	Zertifikat Zertifikat Zertifikat Zertifikat	10.07.2019 01:59:00 01.07.2019 01:59:00 30.06.2019 02:00:00 19.12.2013 10:03:09
	+ i Kopieren	4 Objekte	

Die Installation erfordert Administratorrechte und kann mit dem bereitgestellten Pre-Deployment-Image

cisco-secure-client-macos-5.0.03072-predeploy-k9.dmg

(oder neuer) erfolgen.

Die nachfolgende Vorgehensweise gilt allgemein für die Versionen 5.x:



,Cisco Secure Client.pkg' auswählen

Bestätigen Sie die Lizenzbedingungen. Installieren Sie bitte nur die VPN-Komponente.



💗 Install Cisco Secure Client

	Custom Install on "Macintosh HD"		
	Package Name	Action	Size
Introduction	AnyConnect VPN	Upgrade	61,7 MB
Licence	AMP Enabler	Skip	1,4 MB
Destination Select	Diagnostics and Reporting Tool	Skip	10,3 MB
Installation Type	Secure Firewall Posture	Skip	59,3 MB
	ISE Posture	Skip	8,5 MB
Installation	Network Visibility Module	Skip	12,9 MB
Summary	🗌 Umbrella	Skip	20,7 MB
	Space Required: 61,7 MB	Remaining:	210,64 GB
	Installs the module that enables Umbrella.		
cisco			
		Go Back	Continue

Die Ausnahmeeinstellung für Anyconnect (System Extension) ist vorzunehmen.

Your system r System Extensi capabilities. S enabled. Please allow t Extension in S	equires you to enable the Cisco Secure Client - sion to leverage the full extent of the client's ome functions will not operate correctly until this is he "Cisco Secure Client - Socket Filter" System					
Your system ro System Extens capabilities. S enabled. Please allow t Extension in S	equires you to enable the Cisco Secure Client - sion to leverage the full extent of the client's ome functions will not operate correctly until this is he "Cisco Secure Client - Socket Filter" System					
Please allow t Extension in S	he "Cisco Secure Client - Socket Filter" System					
Extension in S	······································					
	Extension in System Settings -> Privacy & Security page Please					
also allow sub	sequent related prompts					
also allow suc	sequent related prompts.					
(						
	Privacy & Security					
Q Search	Security					
(0) General	Allow applications downloaded from					
M Appearance	App Store					
Appearance     Accessibility	App Store App Store and identified developers					
Appearance     Accessibility     Control Cen	App Store  App Store and identified developers  ter  System software from application "Cisco Secure Client - Socket					
Control Cen	App Store App Store and identified developers for System software from application "Cisco Secure Client - Socket pit Filter.app" was blocked from loading.					
<ul> <li>Accessibility</li> <li>Control Cen</li> <li>Siri &amp; Spoti</li> <li>Privacy &amp; St</li> </ul>	Aop Store and identified developers      System software from application *Cisco Secure Client - Socket      pit     Flar app* was blocked from loading.      Autow					
Accessibility     Control Cen     Siri & Spoti     Privacy & Se     Desktop & C	Aco Store Aco Store and identified developers ter System software from application "Cisco Secure Client - Socket pit Piter application "Cisco Secure Client - Socket Piter application" Allow Nock					
Appearance     Accessibility     Control Cen     Siri & Spoti     Privacy & S     Desktop & E     Desktop & E     Desktop & E	App Store and identified developers  ter  pht  System software from application "Cisco Secure Client - Socket  Fiter.app" was blocked from loading.  Cutory  Cuto					
Appearance     Accessibility     Control Cen     Siri & Spoti     Privacy & Sr      Desktop & C     Siplays     Wallpaper	Aco Store Aco Store and identified developers ter ght System software from spolication "Cisco Secure Client - Socket Fitter app" was blocked from loading. Monty Took Fitter app" was blocked from loading. Monty Took Fitter automatically. Toro Off.					
Accessibility     Accessibility     Sontrol Cee     Siri & Spoti     Privacy & S     Desktop & D     Siri & Spoti     Desktop & D     Siri & Sirie & Siri	A cos Store     Acos Store and identified developers      for     get     System software from application "Cisco Secure Client - Socket     Filter app" was blocked from loading.     (allow     )     Cost     Cost     Filterapp" (Cost     Cost     Co					
Appearance     Appearance     Appearance     Appearance     Control Cen     Siri & Spoti     Protecty & S     Desktop & C     Desktop & C     Desktop & C     Soreen Sev     Soreen Sev     Encrys Seve	Aco Store     Aco Store and identified developers      ter      ght     System software from application "Cisco Secure Client - Socket     Filter.app" was blocked from lading.     (Allow     (Comparison of the application of the software from application     (Comparison of the					
Appendiation     Accessibility     Control Cen     Sin & Spoti     Desktop & C     Desktop & C     Displays     Willpaper     Screen Sav     Lock Screen	Allo Store Allo Store Allo Store and identified developers ter and Allow System software from application "Cisco Secure Client - Socket Pitter app" was blocked from loading. Client Pitter app" was blocked from loading. Client C					
Augustantos     Augustantos     Augustantos     Control Cen     Siris & Spoid     Pronce, A.9     Desktop & I     Desktop & I     Outpalya     Streem Sav     Energy Save     Lock Screem     Lock Screem	A do Store A do Store and identified developers for agent and a dentified developers System software from application "Cisco Secure Client - Socket Filter.app" was blocked from loading. Socket					

11

8

**Cisco Secure Client - Notification** 



#### **Action Required**

Cisco Secure Client - System Extension Blocked.

Your system requires you to enable the Cisco Secure Client -System Extension to leverage the full extent of the client's capabilities. Some functions will not operate correctly until this is enabled.

Please allow the "Cisco Secure Client - Socket Filter" System Extension in System Settings -> Privacy & Security pane. Please also allow subsequent related prompts.







#### Benutzung:

•••	Cisco Secure Client	cisco
	AnyConnect VPN: Ready to connect. wingatelzam.kfa-juelich.de	Connect
* 2		

Akzeptieren Sie gegebenenfalls einmalig beim ersten Verbindungsaufbau die Server-Zertifikate **wingate.zam.kfa-juelich.de** bzw. **wingateb.zam.kfa-juelich.de**.

Erlauben Sie beim Verbindungsaufbau den Zugriff auf das eigene Benutzer-Zertifikat im Schlüsselbund. (Falls kein gültiges Zertifikat verfügbar ist, endet der Verbindungsversuch mit der Meldung ,Certificate Validation Failure'.)

**VPN-Gateways:** 

#### wingate.zam.kfa-juelich.de

oder (Backup-Zugang)

wingateb.zam.kfa-juelich.de

Mögliche Group-Policy im Feld ,Group' auswählen (siehe FAQ Frage 8).

Cisco Secu	re Client   wingate.zam.kfa-juelich.de	
Please enter	r your username and password.	
Group:	FZJ-NOSPLIT	0
Username:		
Password:		
	Cancel	ок

Die VPN-Benutzerkennung ist einzugeben.

Beispiel einer aktiven VPN-Verbindung -> öffnen Verbindungs ICON:

• • • Statistics		O Cisco Secure Client	AnyConnect VPN
Virtual Private Network (V	PN)		
Statistics	Route Details Firewall	Message History	
Connection Information			
State:	Connect	ed	
Tunnel Mode (IPv4):	Tunnel A	II Traffic	
Tunnel Mode (IPv6):	Tunnel A	II Traffic	
Dynamic Tunnel Exclusion:	None		
Dynamic Tunnel Inclusion:	None		
Duration:	00:00:4	9	
Session Disconnect:	None		
Management Connection St	ate: Disconn	ected (user tunnel active)	
<ul> <li>Address Information</li> </ul>			
Client (IPv4):	134.94.5	56.129	
Client (IPv6):	2001:63	8:404:3800:0:0:3800:AD3	34
Server:	134.94.1	11.185	
~ Bytes			
Sent:	19641		
Received:	65549		
✓ Frames			
Sent:	150		
Dessived	100		
		Reset Ev	nort Stats
		NOJEL LA	port otats

Das "Message History' zeigt den zeitlichen Verlauf des Verbindungsaufbaus. Die Datei /var/log/system.log (Zugriff: Administratorrechte) enthält darüber hinaus Meldungen zur Diagnose von Verbindungsproblemen:

#### grep acvagent /var/log/system.log

Alternativ kann im Problemfall das ,Diagnostic and Reporting Tool' nachinstalliert werden.

## 6. FAQ

1. Wer sind die richtigen Ansprechpartner bei weiteren Fragen?

#### Bei Fragen zum VPN-Antrag und Password-Reset:

Ansprechpartner: JSC "Office for User Services" Telefon: 02461 61- 5642 E-Mail: user-services.jsc@fz-juelich.de

Halten Sie bitte die folgenden Informationen bereit oder teilen Sie diese mit: Name und Organisationseinheit
VPN-Benutzername (z.B.m.mustermann)
Datum und Uhrzeit der Antragsstellung bzw. des Passwort-Resets

#### Bei Verbindungsproblemen und techn. Problemen:

Ansprechpartner: Abteilungskommunikationssysteme im JSC Telefon: 02461 61 – 6440 E-Mail: vpn@fz-juelich.de

Halten Sie bitte die folgenden Informationen bereit oder teilen Sie diese mit: Name und Organisationseinheit
VPN-Benutzername
Betriebssystem (Software: Cisco Anyconnect oder Openconnect)
Ihr Internet Provider zu Hause (Telekom, Vodafone, etc.)
IP-Adressen, die vom Provider zugewiesen wurden
Datum und Uhrzeit, wann Ihr Problem auftrat

## 2. Kann beim Import (Windows) eines Zertifikates die Funktion "Hohe Sicherheit für den privaten Schlüssel" aktiviert werden?

Ja-dieses Sicherheitsfeature wird unterstützt.

#### 3. Kann Start-Before-Logon (SBL) unterstützt werden?

Nein. Die Client-Authentifizierung mit Zertifikaten und SBL sind nicht kompatibel.

# 4. Welches Windows Firewall-Profil wird für den VPN-Adapter/Verbindung verwendet?

Nach der Installation ist der Cisco Anyconnect Adapter in allen Firewall-Profilen eingetragen (Name: LAN-Verbindung *n*, der Befehl ipconfig /all zeigt die Zuordnung der Indexnummer *n* zum aktiven Anyconnect Adapter). Dadurch gilt das "Öffentliche Profil". In der "Windows Firewall mit erweiterter Sicherheit" kann diese Auswahl im Menu "Geschützte Netzverbindungen" explizit angepasst werden, um beispielsweise das "Private Profil" für die VPN-Verbindung zu aktivieren.

## 5. Kann gleichzeitig die Windows Funktion ,Internet Connection Sharing' genutzt werden?

Nein. Diese Komponente ist nicht kompatibel mit Anyconnect.

#### 6. Welche VPN-Pool-Adressen müssen Systeme im JuNet bei der Firewall-Konfiguration beachten?

Bei der VPN-Einwahl (Verbindungsaufbau) werden IP-Adressen aus vordefinierten Bereichen vergeben. Die Bereiche sind

134.94.79.0/24 134.94.112.0/24 **134.94.48.0/20 2001:638:404:3000::/52** 2001:638:404:4f00::/64 2001:638:404:7000::/64

Je nach Sicherheitsanforderungen kann ein System im JuNet die Kommunikation durch entsprechende Einträge im Firewall Regelwerk blockieren oder erlauben. (Linux: TKI-0402 Linux Personal Firewall). Eine aktuelle Gesamtliste für alle VPN-Varianten (inkl. L2TPoverIPSEC ) finden Sie unter

https://junet-portal.fz-juelich.de/cgi-bin/public/junet\_server.cgi

#### 7. Kann auf Freigaben (NetBIOS-Shares) im JuNet zugegriffen werden?

Ja. Die NetBIOS-Ports sind freigeschaltet! Beispiele zum Testen (Windows Client):

net time \\zelcds.zel.kfa-juelich.de

net view \\zelcds.zel.kfa-juelich.de

# 8. Der Zugriff auf elektronische Zeitschriften der ZB funktioniert nicht / ist nicht erlaubt.

Wegen der Split-Tunnel-Einstellung in der Tunnel-Policy *fzj* wird nur der IP-Traffic zu Rechnern im JuNet (134.94.0.0/16 bzw. 2002:638:404::/48) in den VPN-Tunnel geleitet. Die Kommunikation zum Internet erfolgt direkt über den jeweiligen Service-Provider (z.B. T-Online) mit deren IP-Adressen. Durch Änderung der VPN-Gruppe auf *fzj-nosplit* wird der gesamte IP-Traffic in den VPN-Tunnel geleitet und der Zugriff auf die Zeitschriften erfolgt mit einer gültigen JuNet-IP-Adresse (IPv4/IPv6).

#### 9. Windows Anyconnect und DS-Lite im HomeOffice – IPv6 Transport

Die Kommunikation kann durch Verwendung der vollqualifizierten DNS Namen

wingate6.zam.kfa-juelich.de wingateb6.zam.kfa-juelich.de

fest auf Basis von IPv6 erfolgen.

#### 10. Anyconnect und Linux

Die Installation erfolgt mit dem bereitgestellten Pre-Deployment-Image. Für die Installation werden Administratorrechte verlangt. Nutzen Sie aus dem Download-Bereich das jeweils aktuelle TAR-Archiv: anyconnect-predeploy-linux-64-4.5.03040-k9.tar.gz

Die nachfolgende Vorgehensweise gilt allgemein für die Versionen 4.x:

mount -r -t cifs //pcsrv.zam.kfa-juelich.de/public /mnt

Das Archiv in ein lokales Verzeichnis kopieren, auspacken und die Installation starten:



Die Verbindung kann wie folgt aufgebaut werden:

linux-oglv:~ # linux-oglv:~ # cd /opt/cisco/anyconnect/bin linux-oglv:/opt/cisco/anyconnect/bin # linux-oglv:/opt/cisco/anyconnect/bin # ./vpnui

Statt der grafischen Bedienoberfläche

/opt/cisco/vpn/bin/vpnui

۵ 🕑	Cisco AnyConnect Secure Mobility Client	$\odot$	$\odot$ $\otimes$	
🗞 Connectio	on 🚯 Statistics   🍰 About			
alati				
	cisco			
Connect to:	wingate.zam.kfa-juelich.de	~	<u>_</u>	
Group:	FZJ-NOSPLIT		~	
Username:	[			
Password:				
Connect				
Please enter your username and password.				

kann alternativ das Kommandozeilen-Tool

/opt/cisco/anyconnect/bin/vpn

VPN> connect wingate.zam.kfa-juelich.de

VPN> disconnect

genutzt werden. Speicherung der Zertifikate – ,\$HOME/.cisco':

./.cisco: certificates	*
./.cisco/certificates: client	
./.cisco/certificates/client: myCert.pem <b>private</b>	
./.cisco/certificates/client/µ myCert.key	private:

(Stand: 05.09.2023 / Letzte Kontrolle: 05.09.2023)