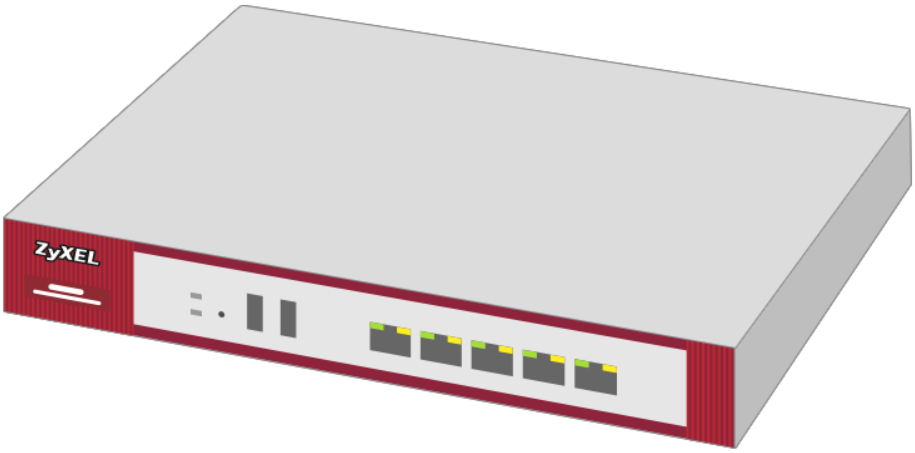
ZYXEL
Your Networking Ally



Anpassung von VPN Konfigurationsfiles

Zyxel Firewall-Serie

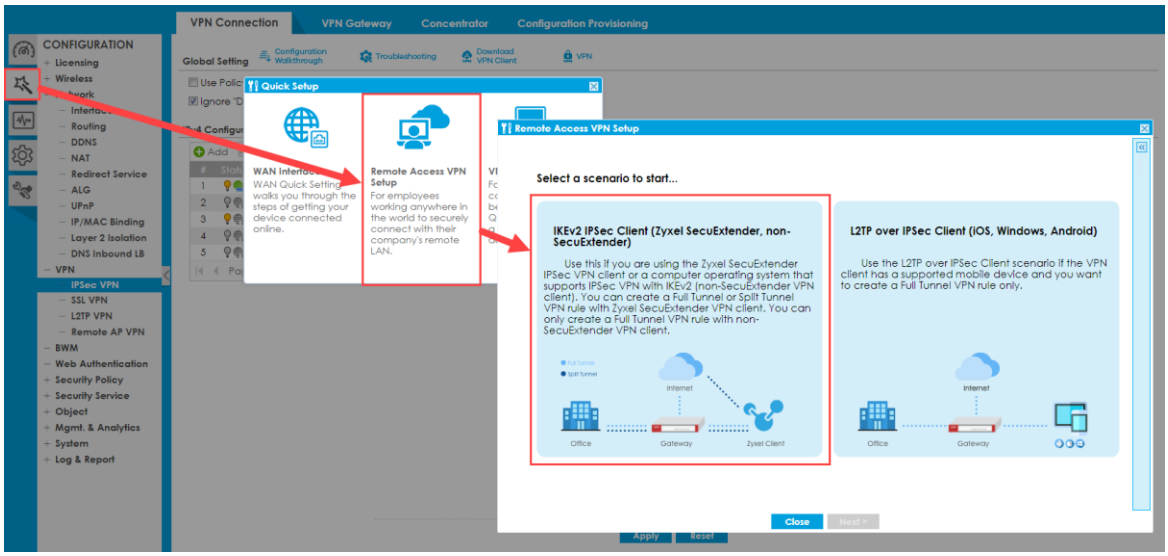
Knowledge Base KB-3824
Februar 2023

VPN-KONFIGURATIONSFILES FÜR REMOTE ACCESS (IKEV2)

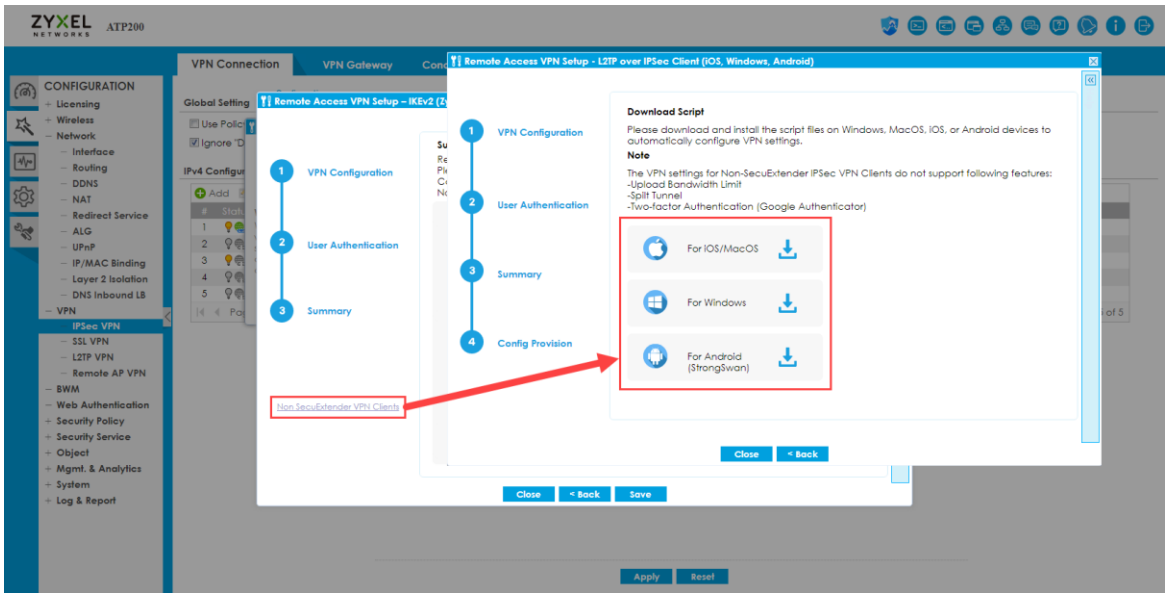
Die Zyxel Firewall-Serie stellt für Client-to-Site VPN Konfigurationsfiles zur Verfügung, welche das Einrichten eines VPN-Tunnels wesentlich erleichtern.

VPN-WIZZARD

Quick Setup > Remote Access VPN Setup > IKEv2 IPSec Client



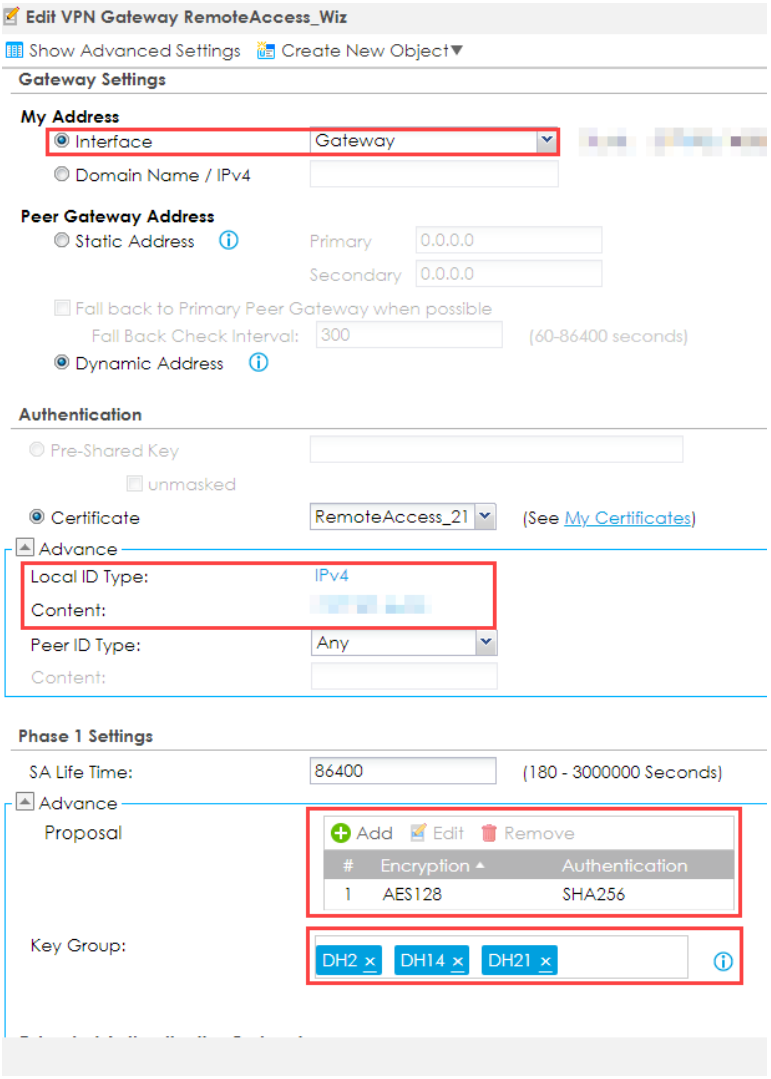
Am Ende des Assistenten kann für Windows, Android, MacOS und iOS ein Konfigurationsfile bezogen werden:



ANPASSEN DER KONFIGURATION AUF DER FIREWALL

Configuration > VPN > IPSec VPN > VPN Gateway (Phase 1)

Um eine bessere Verschlüsselung zu erreichen, kann die Konfiguration angepasst werden.
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt folgende Mindestparameter: AES256 / SHA256 / DH15.



Interface: Definiert das Interface der Firewall, auf welches die Verbindung aufgebaut wird. Alternativ kann auch ein DNS-Name, eine IP-Adresse oder 0.0.0.0 (Alle Adressen) verwendet werden.

Local ID: Wird aus dem Zertifikat bezogen. Um allfällige Probleme zu vermeiden, sollte dieser Eintrag mit der Adresse übereinstimmen, auf welche die Verbindung aufgebaut wird.

Encryption: Verschlüsselung der Verbindung.

Authentication: Integrität der Verbindung

Key Group: Diffie-Hellman Group

BEZEICHNUNG DER PARAMETER AUF VERSCHIEDENEN SYSTEMEN

Die Bezeichnung der Parameter variiert zwischen unterschiedlichen Systemen.
Nachfolgend eine Übersicht mit unterstützten Einstellungen der aktuellen Firewall-Serie:

USG	**Windows Gateway** **Phase 1**	**Windows Connection** **Phase 2**	**StrongSwan**	**MacOS**
Verschlüsselung:				
DES	DES	DES		DES
3DES	3DES	3DES	3des	3DES
AES128	AES128	AES128	aes	AES-128
AES192	AES192	AES192	aes192	
AES256	AES256	AES256	aes256	AES-256
Integritätsprüfung				
MD5	MD596	MD5	md5	
SHA1	SHA196	SHA1	sha1	SHA1-96
SHA256	SHA256128	SHA256	sha256	SHA2-256
SHA515			sha512	SHA2-512
DH-Gruppe		PFS		
DH1	Group1	PFS1	modp768	1
DH2	Group2	PFS2	modp1024	2
DH5			modp1536	5
DH14	Group14	PFS2048	modp2048	14
DH15			modp3072	15
DH16			modp4096	16
DH17			modp6144	17
Dh18			modp8192	18
DH19	ECP256	ECP256	ecp256	19
DH20	ECP384	ECP384	ecp384	20
DH21			ecp521	21

Grau: Verschlüsselungsmethode gilt nicht mehr als sicher (Stand 2023).

Gelb: DH-Gruppe gilt als sicher, ist aber weniger effizient

Grün: Gilt bis auf weiteres als sicher

KONFIGURATIONSFILE STRONGSWAN ANDROID:

Das Android-Konfigurationsfile ist sehr kurz und übersichtlich gestaltet.

Die Verbindungsparameter lassen sich mit 2 Einträgen für die Phase 1 und Phase 2 definieren.

Soll keine DH-Gruppe verwendet werden, kann der Eintrag weggelassen werden.

{	
"uuid": "E02D41CE-E835-D7DB-C6FB-15AE9E0985C1",	frei definierbare UUID v4
"name": "RemoteAccess_123.145.167.189",	Name der Verbindung
"type": "ikev2-eap",	
"remote": {	
"addr": "123.145.167.189",	WAN-IP-Adresse der Firewall
"id": "123.145.167.189",	Local ID der Firewall bzw. Common Name des Zertifikates
"cert": "xyz..zyx="	Inhalt des Zertifikates
},	
"split-tunneling": {	
"subnets": "0.0.0.0/0"	Erreichbares Remote Netz
},	
"ike-proposal": "aes128-sha256-modp1024", Empfehlung: aes256-sha256-ecp256	Verschlüsselung VPN Gateway Verschlüsselung-Integrität-DH Gruppe
"esp-proposal": "aes128-sha256" Empfehlung: aes256-sha256-ecp256	Verschlüsselung VPN Connection Verschlüsselung-Integrität-PFS
}	

KONFIGURATIONSFILE WINDOWS

Im Windows File werden alle Parameter am Anfang als Variablen definiert:
Im Gegensatz zu anderen Systemen wird das Zertifikat separat mitgeliefert und befindet sich nicht direkt im Konfigurationsfile.

@echo off	
set Name="RemoteAccess_123.145.167.189"	Name der Verbindung
set ServerAddress="123.145.167.189"	Adresse und Local ID der Firewall Common Name des Zertifikates
set TunnelType="IKEv2"	
set AuthenticationMethod="EAP"	
set EncryptionLevel="Required"	
set UseWinlogonCredential=$False	
set RememberCredential=$False	
set SplitTunneling=$False	
set IKEEnc="AES128" Empfehlung: AES256	Verschlüsselung VPN Gateway
set IKEAuth="SHA256128"	Integritätsprüfung VPN Gateway
set IKEKey="Group2" Empfehlung: Group14	DH Gruppe VPN Gateway
set ESPEnc="AES128" Empfehlung: AES256	Verschlüsselung VPN Connection
set ESPAuth="SHA256"	Integritätsprüfung VPN Connection
set ESPPfs="None" Empfehlung: PFS2048	PFS VPN Connection
Zeile 38: … .\RemoteAccess_Win_xxx.crt	

KONFIGURATIONSFILE MACOS / IOS

Das Konfigurationsfile für Apple-Produkte ist wesentlich komplexer aufgebaut. Die Einstellungen müssen im File allenfalls etwas gesucht werden. Nachfolgend ein Auszug aus dem File:

<key>**ChildSecurityAssociationParameters**</key>	VPN-Connection Parameter
<dict>	
<key>DiffieHellmanGroup</key>	
<integer>14</integer> Empfehlung: 19	PFS DH-Gruppe
<key>EncryptionAlgorithm</key>	
<string>AES-128</string> Empfehlung: AES-256	Verschlüsselung VPN-Connection
<key>IntegrityAlgorithm</key>	
<string>SHA2-256</string>	Integritätsprüfung VPN-Connection
<key>LifeTimeInMinutes</key>	
<integer>480</integer>	
</dict>	
<key>**EnablePFS**</key>	
<false/> Empfehlung: true/	PFS aktivieren / deaktivieren
<key>**IKESecurityAssociationParameters**</key>	VPN-Gateway Einstellungen
<dict>	
<key>DiffieHellmanGroup</key>	
<integer>2</integer> Empfehlung: 19	DH-Gruppe
<key>EncryptionAlgorithm</key>	
<string>AES-128</string> Empfehlung: AES-256	Verschlüsselung VPN-Gateway
<key>IntegrityAlgorithm</key>	
<string>SHA2-256</string>	Integritätsprüfung VPN-Gateway
<key>LifeTimeInMinutes</key>	
<integer>1440</integer>	
</dict>	
<key>RemoteAddress</key>	
<string>123.145.167.189</string>	VPN Gateway Adresse
<key>RemoteIdentifier</key>	
<string>123.145.167.189</string>	Local ID VPN Gateway
<key>ServerCertificateIssuerCommonName</key>	
<string>123.145.167.189</string>	Common Name des Zertifikates (-> entspricht Local ID VPN Gateway)
<key>UserDefinedName</key>	
<string>RemoteAccess_Wiz_123.145.167.189</string>	Name der VPN-Verbindung