Best Practices - Mobile User VPN mit IKEv2

Thomas Fleischmann

Senior Sales Engineer, Central Europe

Thomas.Fleischmann@watchguard.com

WatchGuard Training

IKEv2 Standard

- Definiert im RFC 4306
- Vorteile gegenüber IKEv1
  - Zum Aufbau der Verbindung braucht man weniger Pakete (Nur vier statt neun).
  - Stärke Standard Algorithmen wurden gewählt (3DES 168Bit, AES 128Bit oder grösser).
  - Einfache Fehlersuche, da die Zuständigkeiten der Peers klar geregelt wurde.
  - NAT-Traversal fester Bestandteil der Verbindung (UDP-Port 4500). (Auch IPSec Passthrough genannt).

Mobile VPN mit IKEv2

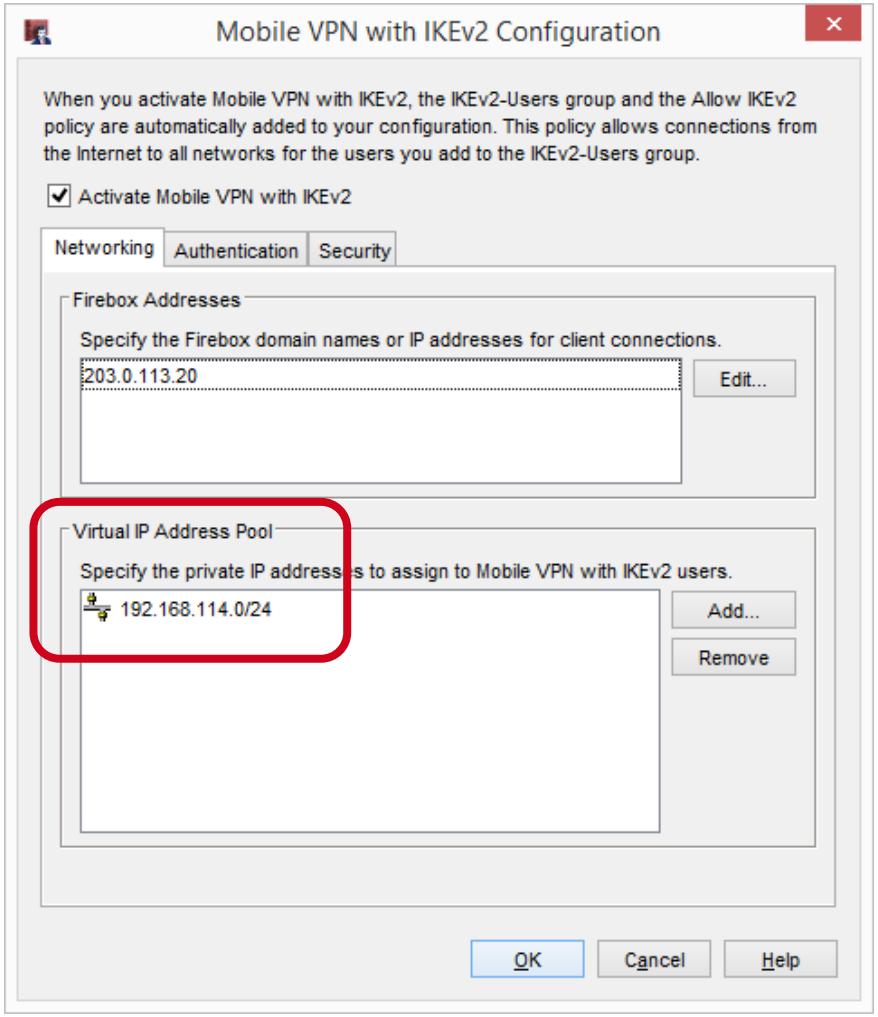
- IKEv2 ist ein Tunneling Protokoll für IKEv2/IPSec VPNs
- Es ist nun möglich, den nativen IKEv2 VPN Client für Windows, MacOS, und iOS Geräte zu verwenden, anstatt ein Third-Party Lösung
  - Mobile Benutzer können nun die internen Geschäfts Ressourcen durch einen IKEv2/IPSec Tunnel durch die WatchGuard Firebox erreichen.
- Zu einem kann man die Geräte im Vorfeld konfigurieren oder mit einen BYOD Verfahren den Zugang freigeben.
- Benutzer von Android Devices können mit der freien, Third-Party App *strongSwan* einen IKEv2 Verbindung aufbauen.

Mobile VPN mit IKEv2

- Auf der Firebox kann man manuell oder mit Hilfe eines Wizards eine Konfiguration erstellen.
- Mobile VPN mit IKEv2 sendet allen Traffic über den VPN Tunnel (Voller Tunnel Modus)
- Die Endgeräte kontrollieren das Routing, nicht die Firewall.
- Die Anzahl der *IPSec VPN Users* im Feature Key bezieht sich auf die Summe von Mobile VPN mit IKEv2 und Mobile VPN mit IPSec
  - Beispiel: Erlaubt ein Feature Key 250 IPSec VPN User Verbindungen, und es sind 200 User mit Mobile VPN mit IPSec verbunden, dann können sich 50 User mit Mobile VPN mit IKEv2 verbinden.

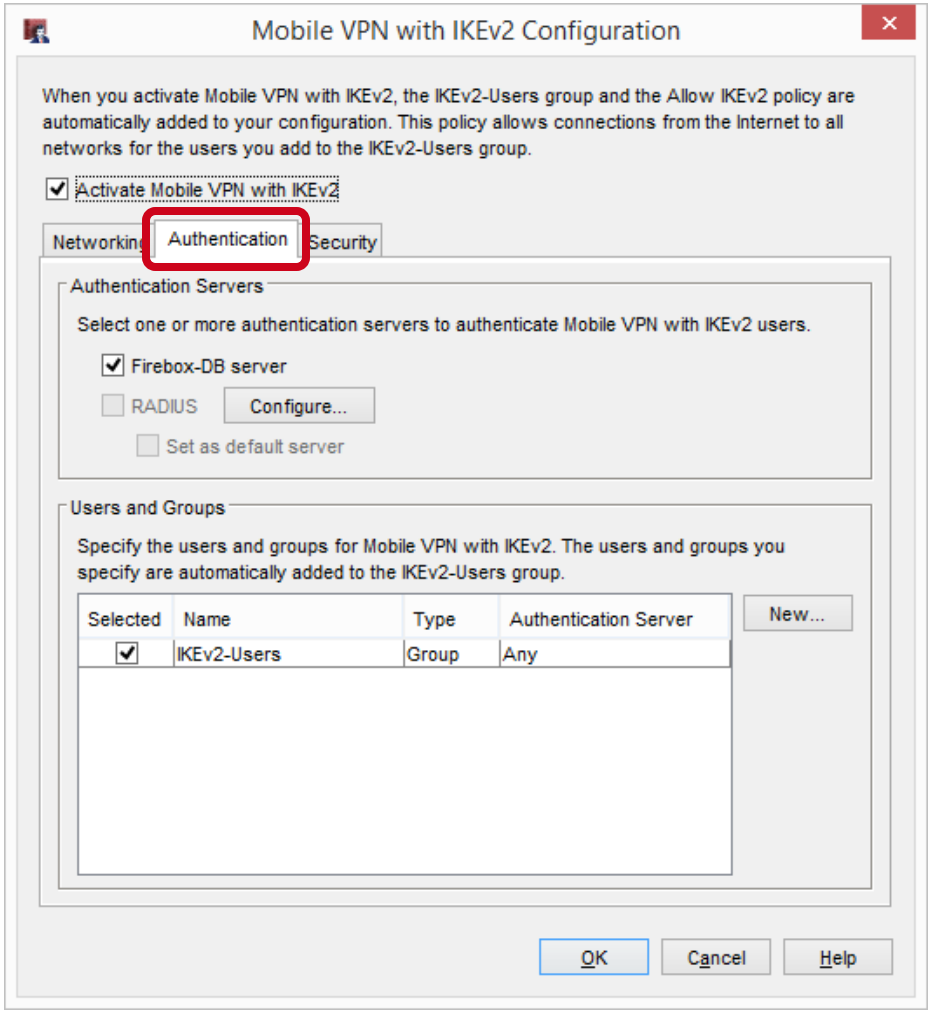
Mobile VPN mit IKEv2

- Wenn Mobile VPN mit IKEv2 eingeschaltet wird, erstellt die WatchGuard Firebox automatisch einen Default Virtual Address Pool für die IKEv2 Benutzer.



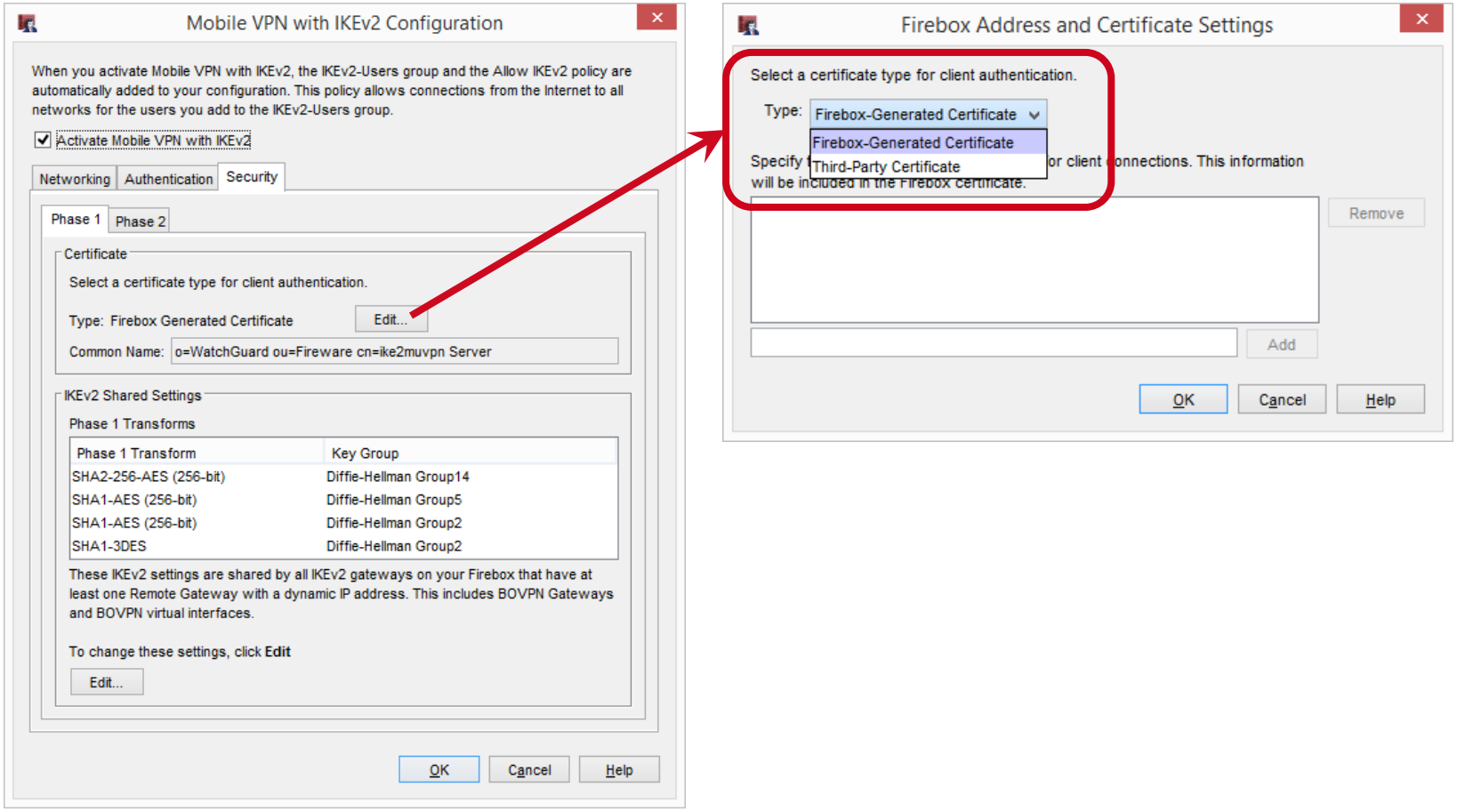
Mobile VPN mit IKEv2

- Der **Authentication** Reiter



Mobile VPN mit IKEv2

- Man kann ein Firebox Zertifikat oder ein Third-Party Zertifikat verwenden

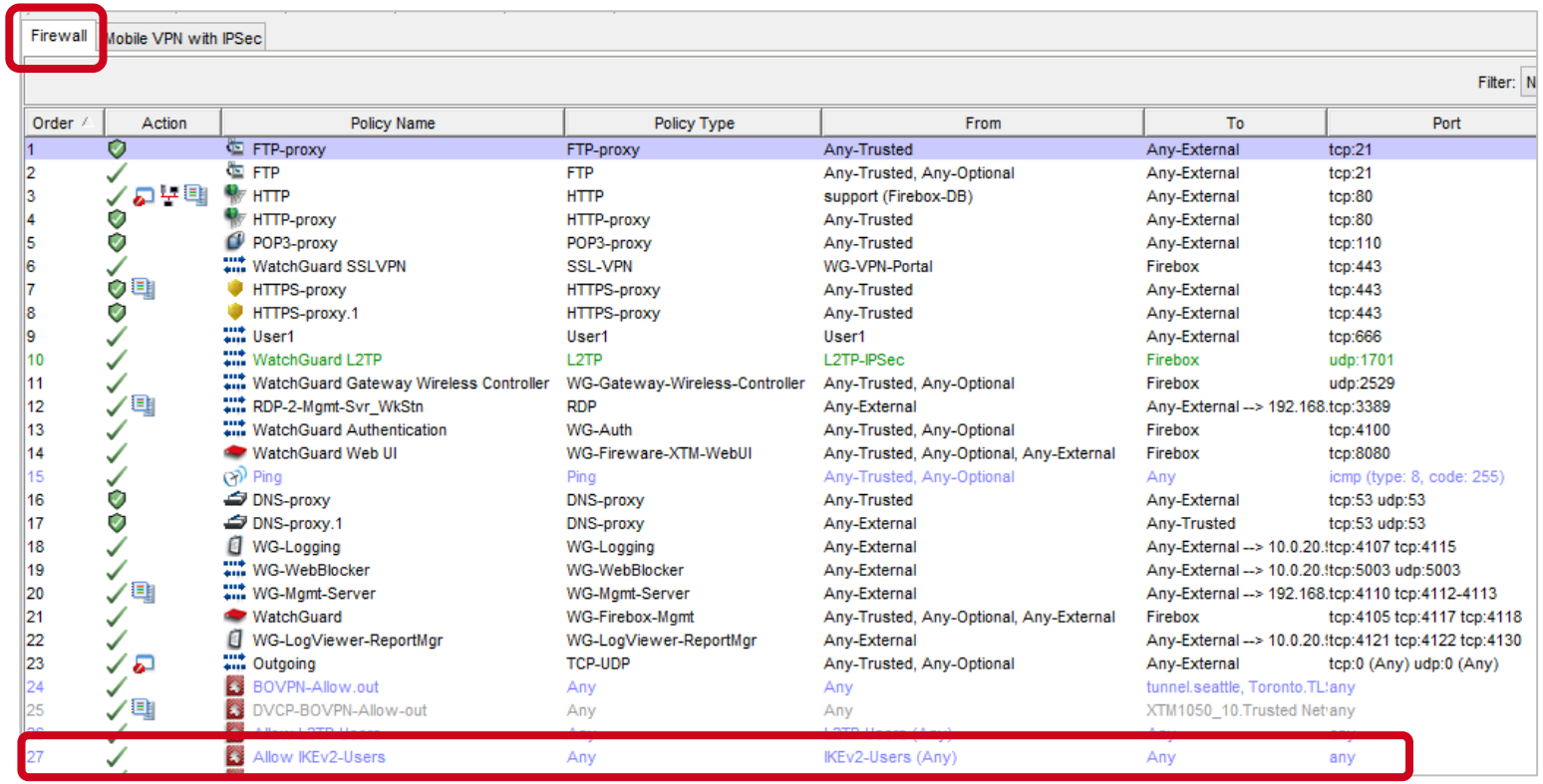


Mobile VPN mit IKEv2

- Firebox und Third-Party Zertifikate haben diese Anforderungen:
  - Extended Key Usage (EKU) flags *serverAuth* und *IP Security IKE Intermediate* (OID 1.3.6.1.5.5.8.2.2)
  - **IP Address** oder **DNS Name** ist ein **Subject Alternative Name** Wert

Mobile VPN mit IKEv2

- Die Richtlinie für Mobile VPN mit IKEv2 erscheint im **Firewall** Reiter in der Liste der Richtlinien.



Order	Action	Policy Name	Policy Type	From	To	Port
1		FTP-proxy	FTP-proxy	Any-Trusted	Any-External	tcp:21
2		FTP	FTP	Any-Trusted, Any-Optional	Any-External	tcp:21
3		HTTP	HTTP	support (Firebox-DB)	Any-External	tcp:80
4		HTTP-proxy	HTTP-proxy	Any-Trusted	Any-External	tcp:80
5		POP3-proxy	POP3-proxy	Any-Trusted	Any-External	tcp:110
6		WatchGuard SSLVPN	SSL-VPN	WG-VPN-Portal	Firebox	tcp:443
7		HTTPS-proxy	HTTPS-proxy	Any-Trusted	Any-External	tcp:443
8		HTTPS-proxy.1	HTTPS-proxy	Any-Trusted	Any-External	tcp:443
9		User1	User1	User1	Any-External	tcp:666
10		WatchGuard L2TP	L2TP	L2TP-IPSec	Firebox	udp:1701
11		WatchGuard Gateway Wireless Controller	WG-Gateway-Wireless-Controller	Any-Trusted, Any-Optional	Firebox	udp:2529
12		RDP-2-Mgmt-Svr_WkStn	RDP	Any-External	Any-External --> 192.168.	tcp:3389
13		WatchGuard Authentication	WG-Auth	Any-Trusted, Any-Optional	Firebox	tcp:4100
14		WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-Trusted, Any-Optional, Any-External	Firebox	tcp:8080
15		Ping	Ping	Any-Trusted, Any-Optional	Any	icmp (type: 8, code: 255)
16		DNS-proxy	DNS-proxy	Any-Trusted	Any-External	tcp:53 udp:53
17		DNS-proxy.1	DNS-proxy	Any-External	Any-Trusted	tcp:53 udp:53
18		WG-Logging	WG-Logging	Any-External	Any-External --> 10.0.20.	tcp:4107 tcp:4115
19		WG-WebBlocker	WG-WebBlocker	Any-External	Any-External --> 10.0.20.	tcp:5003 udp:5003
20		WG-Mgmt-Server	WG-Mgmt-Server	Any-External	Any-External --> 192.168.	tcp:4110 tcp:4112-4113
21		WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Optional, Any-External	Firebox	tcp:4105 tcp:4117 tcp:4118
22		WG-LogViewer-ReportMgr	WG-LogViewer-ReportMgr	Any-External	Any-External --> 10.0.20.	tcp:4121 tcp:4122 tcp:4130
23		Outgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External	tcp:0 (Any) udp:0 (Any)
24		BOVPN-Allow.out	Any	Any	tunnel.seattle, Toronto.TL	any
25		DVCP-BOVPN-Allow-out	Any	Any	XTM1050_10.Trusted Net	any
27		Allow IKEv2-Users	Any	IKEv2-Users (Any)	Any	any

Geräte Einrichtung

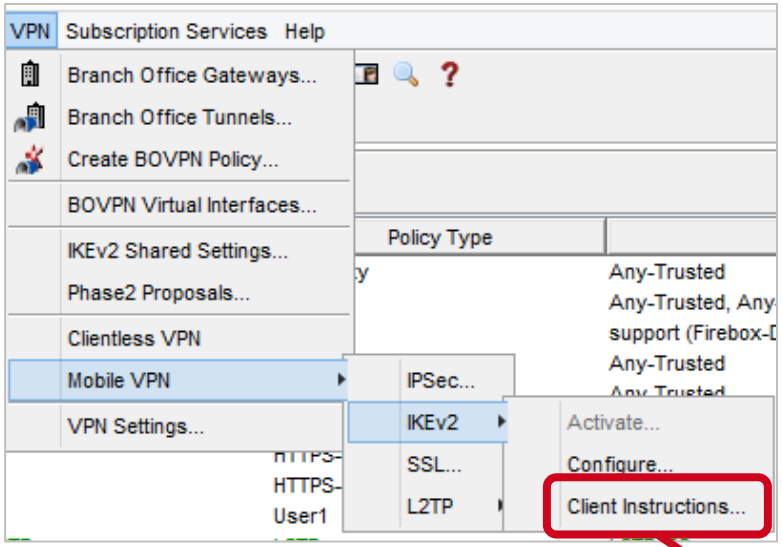
WatchGuard Training

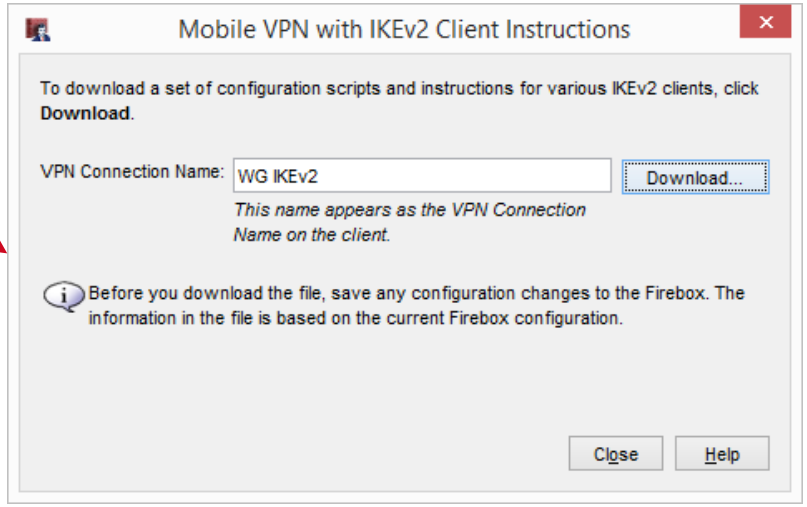
Mobile VPN mit IKEv2

- Man kann ein sog. „Client Instructions File“ von der WatchGuard Firebox herunterladen, welches automatische Installationsdateien und Anleitungen für die IKEv2 VPN Client von Windows, MacOS, iOS und Android enthält
  - Die Client Konfiguration und das Zertifikat werden automatisch mit einen Skript eingerichtet.
  - Man muss vorher auf der WatchGuard Firebox die Konfiguration speichern, bevor man das Konfiguration File herunterladen kann.

Mobile VPN mit IKEv2

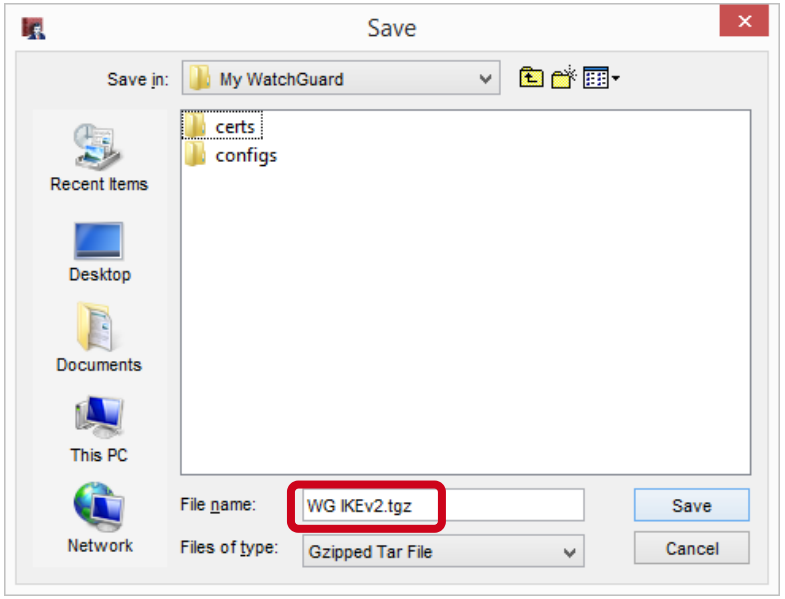
- Herunterladen des **Client Instructions File** von der Firebox

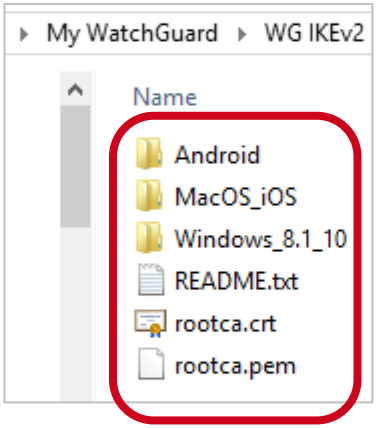




Mobile VPN mit IKEv2

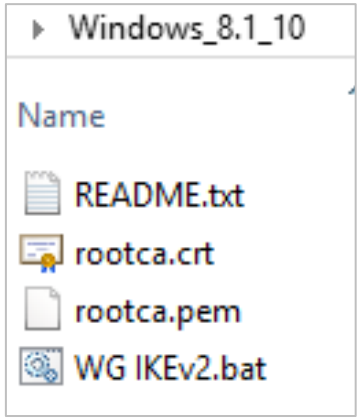
- Speichern des .TGZ Archives
- Extrahieren des Dateien aus dem .TGZ Archive

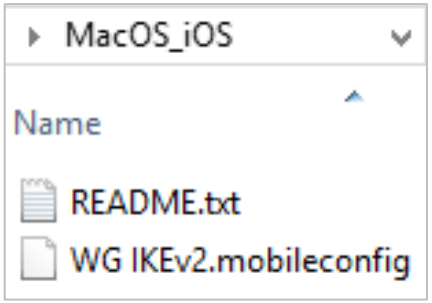


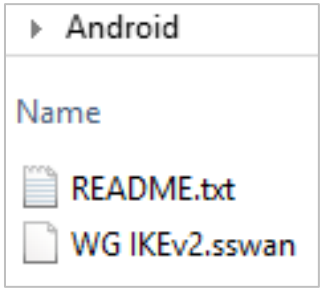


Mobile VPN mit IKEv2

- Jeder Ordner enthält eine Anleitung und ein automatische Konfiguration Skript, welches für das Betriebssystem angepasst ist







Mobile VPN mit IKEv2

- Es ist auch möglich, die Konfiguration der IKEv2 VPN Verbindung manuell auf den Gerät einzurichten.
  - Auf dem Device muss man jeweils die Datei `rootca.pem` oder `rootca.crt,` welche sich in der Archive .TGZ enthalten sind, installiert werden, damit eine IKEv2 VPN Verbindung aufgebaut werden kann.
  - Eine Anleitung für die manuelle Installation befindet sich in den jeweiligen Ordner in dem .TGZ Archive.

Thank You!

WatchGuard Training

NOTHING GETS PAST RED.

WatchGuard

WatchGuard Training