



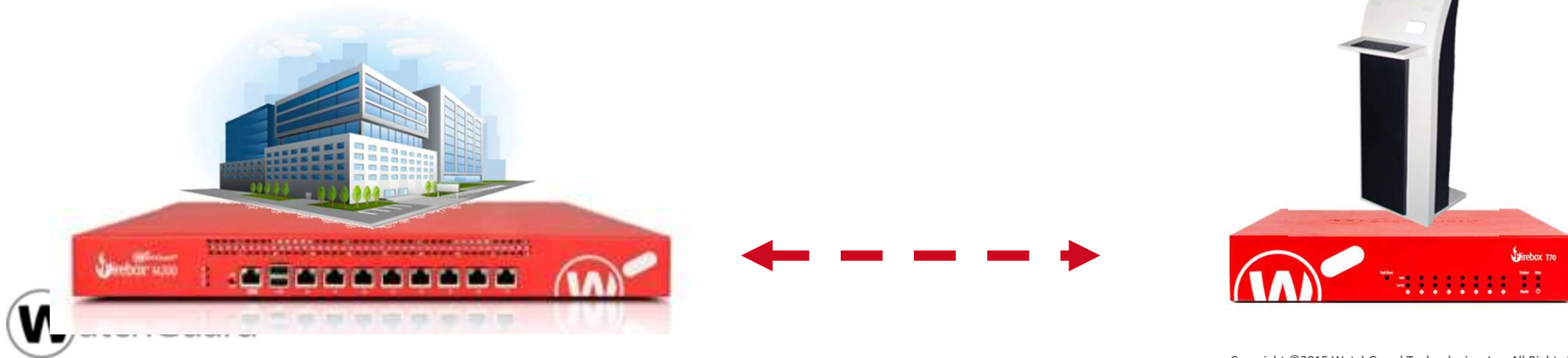
Branch Office VPN mit TLS VPN Anbindung per TCP 443

Jonas Spieckermann
Senior Sales Engineer

Jonas.Spieckermann@watchguard.com

BoVPN over TLS

- Site-to-Site VPN mit TLS 1.2
 - Standortanbindung
 - Basierend auf Client/Server
 - Hub and Spoke Topology
- Vorteile
 - Anbindung kleiner Standorte, “Kiosk Systeme”, Ladenketten, Homeoffice, etc.
 - Nutzt TCP 443 (ist aber kein HTTPS)



BOVPN over TLS

- BOVPN over TLS nutzt TCP Port 443 (üblicherweise erlaubt in Netzwerken)
- In folgenden Fällen als Alternative zu IPSec BOVPN empfohlen:
 - Außenstellenanbindung in eingeschränkten und nicht selbst kontrollierten Lokationen, bei denen IPSec BOVPN unterbunden wird.
z.B. “Shared Office”, Einkaufszentren, Krankenhäuser
 - IPSec Datenverkehr wird nicht korrekt durch den ISP, oder verwendete Hardware (Router / Modem) verarbeitet.
 - IPv6 Light Anschlüsse

BOVPN Over TLS

- BOVPN over TLS nutzt ein Client/Server Modell
 - Eine Firebox im Server mode, kann VPN-Tunnel zu einer oder mehreren Fireboxen im Client mode herstellen.
 - Eine Firebox im Client mode kann VPN-Tunnel zu einer oder mehreren Fireboxen im Server mode herstellen.
 - Eine Firebox kann nicht gleichzeitig als Server und Client genutzt werden.
 - Unterstützt nur Hub-and-Spoke Topology
- BOVPN over TLS Unterstützung nur für Firebox Gegenstellen.
- BOVPN over TLS kann in Fireware v12.1 nur per Fireware Web UI konfiguriert werden.

BOVPN Over TLS

- Aktivierung Client Mode

Branch Office VPN over TLS

Enable Branch Office VPN over TLS to configure a hub-and-spoke VPN when IKE/IPSec traffic is not allowed.

Branch Office VPN over TLS is **Enabled In Client Mode**. Click to [Change Mode](#) or [Disable](#).

Client Settings

BOVPN over TLS Servers

ENABLED	TUNNEL NAME	PRIMARY SERVER	DESCRIPTION
Yes	BovpnTLS.1	198.51.100.2	Tunnel to the Toronto TLS server

[ADD](#) [EDIT](#) [REMOVE](#)

BOVPN Over TLS

- Konfiguration des Client mode

BOVPN over TLS (Client Mode) / Edit Server

Specify the connection settings for a BOVPN over TLS server that can create a tunnel with this BOVPN over TLS client.

Tunnel Name

Description *Optional*

Enable

Specify the Firebox IP addresses or domain names for client connections.

Primary Server

Backup Server *Optional*

For authentication, specify a Tunnel ID to identify this Firebox and a pre-shared key.

Tunnel ID

Pre-Shared Key

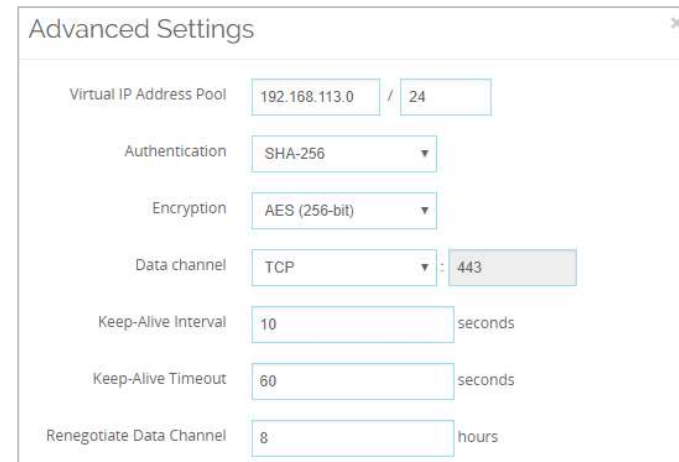
Advanced Options

Add this tunnel to the BOVPN-Allow policies



BOVPN Over TLS

- **Advanced Settings** ermöglicht Anpassungen der Authentication und Encryption Settings
- Der TCP data channel ist dauerhaft auf Port 443
- Soll ein anderer Port als 443 genutzt werden, muss UDP zum Einsatz kommen
- **Import configuration file** ist nur zu Testzwecken vorhanden und wird bald entfernt.



Advanced Settings

Virtual IP Address Pool: 192.168.113.0 / 24

Authentication: SHA-256

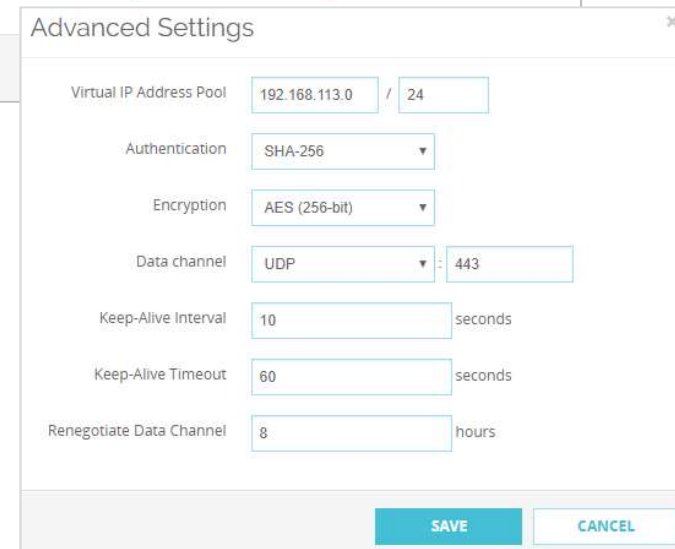
Encryption: AES (256-bit)

Data channel: TCP : 443

Keep-Alive Interval: 10 seconds

Keep-Alive Timeout: 60 seconds

Renegotiate Data Channel: 8 hours



Advanced Settings

Virtual IP Address Pool: 192.168.113.0 / 24

Authentication: SHA-256

Encryption: AES (256-bit)

Data channel: UDP : 443

Keep-Alive Interval: 10 seconds

Keep-Alive Timeout: 60 seconds

Renegotiate Data Channel: 8 hours

SAVE CANCEL

BOVPN Over TLS

- VPN Tunnel zu mehreren TLS Servern sind möglich

Branch Office VPN over TLS

Enable Branch Office VPN over TLS to configure a hub-and-spoke VPN when IKE/IPSec traffic is not allowed.

Branch Office VPN over TLS is **Enabled in Client Mode**. Click to [Change Mode](#) or [Disable](#).

Client Settings

BOVPN over TLS Servers

ENABLED ↑	TUNNEL NAME	PRIMARY SERVER	DESCRIPTION
Yes	BovpnTLS.1	198.51.100.2	Tunnel to the Toronto TLS server
Yes	BovpnTLS.2	192.0.2.2	Tunnel to the New York TLS server

[ADD](#) [EDIT](#) [REMOVE](#)

BOVPN Over TLS

- Aktivierung Server mode

BOVPN over TLS Mode ✕

Specify the BOVPN over TLS mode. The Firebox can operate as a BOVPN over TLS client or a BOVPN over TLS server, but not both at the same time.

Firebox Mode

Specify the Firebox IP addresses or domain names for client connections.

Primary Server

Backup Server *(Optional)*

BOVPN Over TLS

- Konfiguration Server mode

BOVPN over TLS (Server Mode) / Add Client

Specify the connection settings for a BOVPN over TLS client that can create a tunnel with this Firebox.

Tunnel ID

Description *Optional*

Pre-Shared Key

Enable

Client Routes

- Send all client traffic through the tunnel
- Specify the destination addresses that the client will route through the tunnel

Server Routes Specify the destination addresses that the server will route through the tunnel.

DESTINATION	METRIC
10.0.50.0/24	101

Add this tunnel to the BOVPN-Allow policies



BOVPN Over TLS

- Konfiguration Server mode

Branch Office VPN over TLS

Enable Branch Office VPN over TLS to configure a hub-and-spoke VPN when IKE/IPSec traffic is not allowed.

Branch Office VPN over TLS is **Enabled In Server Mode**. Click to [Change Mode](#) or [Disable](#).

Server Settings

Specify the Firebox IP addresses or domain names for clients to connect to.

Primary Server: Backup Server:

[EDIT](#)

Aliases for the BOVPN over TLS clients in this list are automatically created for use in firewall policies.

ENABLED	TUNNEL ID	DESCRIPTION
Yes	TLSTunnel1	

[ADD](#) [EDIT](#) [REMOVE](#)

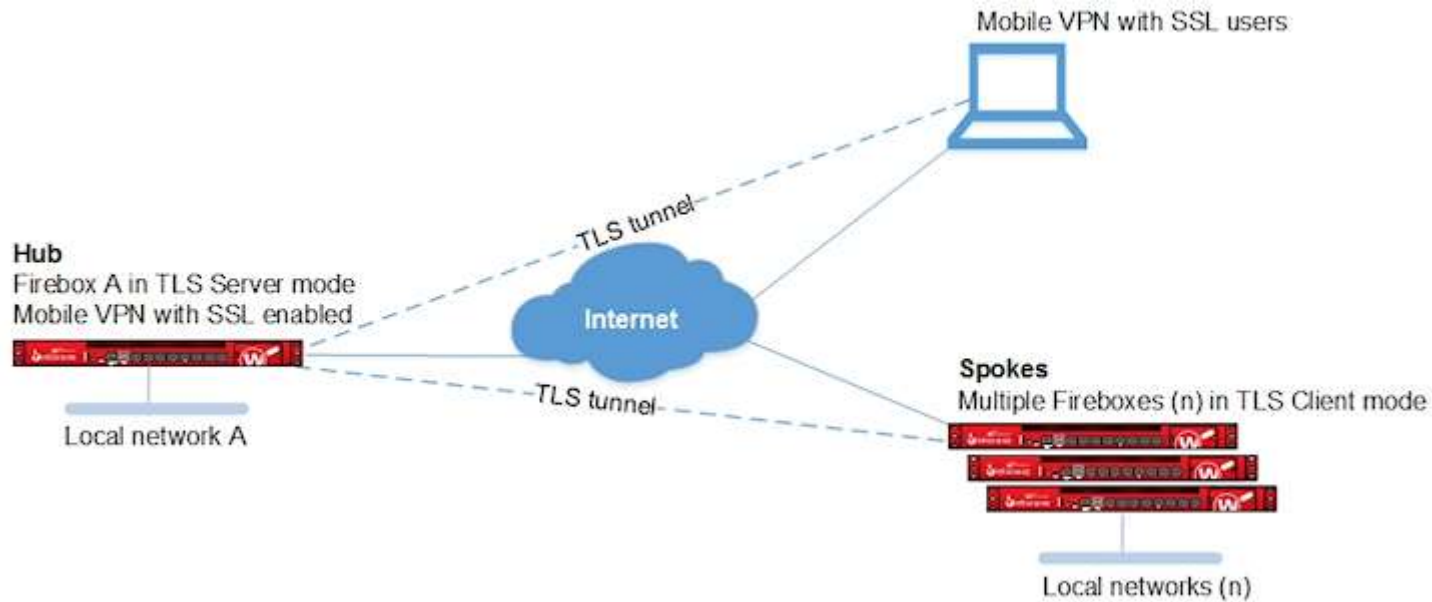
The BOVPN over TLS server is configured to use **TCP** port **443** and assign IP addresses to clients from **192.168.113.0/24**.

[ADVANCED](#)



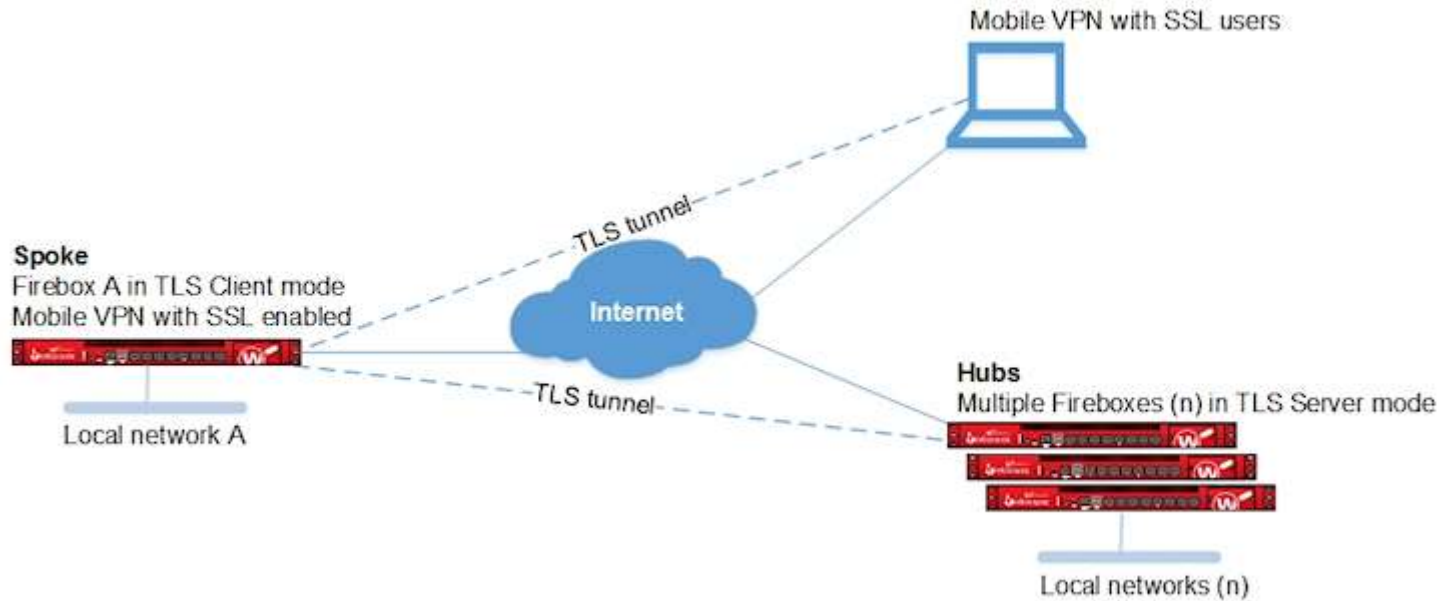
BOVPN Over TLS

- Option 1: TLS server connects to multiple TLS clients



BOVPN Over TLS

- Option 2: TLS client connects to multiple TLS servers



BOVPN Over TLS

- **System Status > VPN Statistics > Branch Office VPN** zeigt den Status der BOVPN over TLS Tunnel

The screenshot displays the WatchGuard VPN Statistics interface. The main panel shows the 'Branch Office VPN' configuration with a 'Show All' dropdown menu highlighted by a red box. A red arrow points from this dropdown to a secondary 'VPN Statistics' panel on the right. This secondary panel shows a search filter dropdown also highlighted by a red box, with 'TLS Tunnels' selected. Below the search filter, there are error messages for 'IKEv1 Gateway: gateway.seattle' and 'IKEv1 Gateway: XTM1050_10.1'. The main panel also shows error messages for 'IKEv1 Gateway: gateway.seattle', 'IKEv1 Gateway: XTM1050_10.1', and 'IKEv1 Virtual Interface (bvpn1): BOVPN.VIF.Portland'. At the bottom of the main panel, two 'TLS Tunnel' entries are listed: 'TLS Tunnel: TLSTunnel' and 'TLS Tunnel: TLSTunnel2', both with 'EDIT' buttons. A red box highlights these two entries.

BOVPN Over TLS

- Unsupported features:
 - Drop-in Mode
 - Bridge Mode
 - Active/active FireCluster
 - IP address ranges
 - BOVPN NAT
 - Dynamic routing over the VPN tunnel
 - Multicast traffic over the VPN tunnel
 - Policy-based routing
- Third-party certificates werden nicht supported



Live: BOVPN mit TLS



Vielen Dank

Jonas Spieckermann
Senior Sales Engineer

Jonas.Spieckermann@watchguard.com