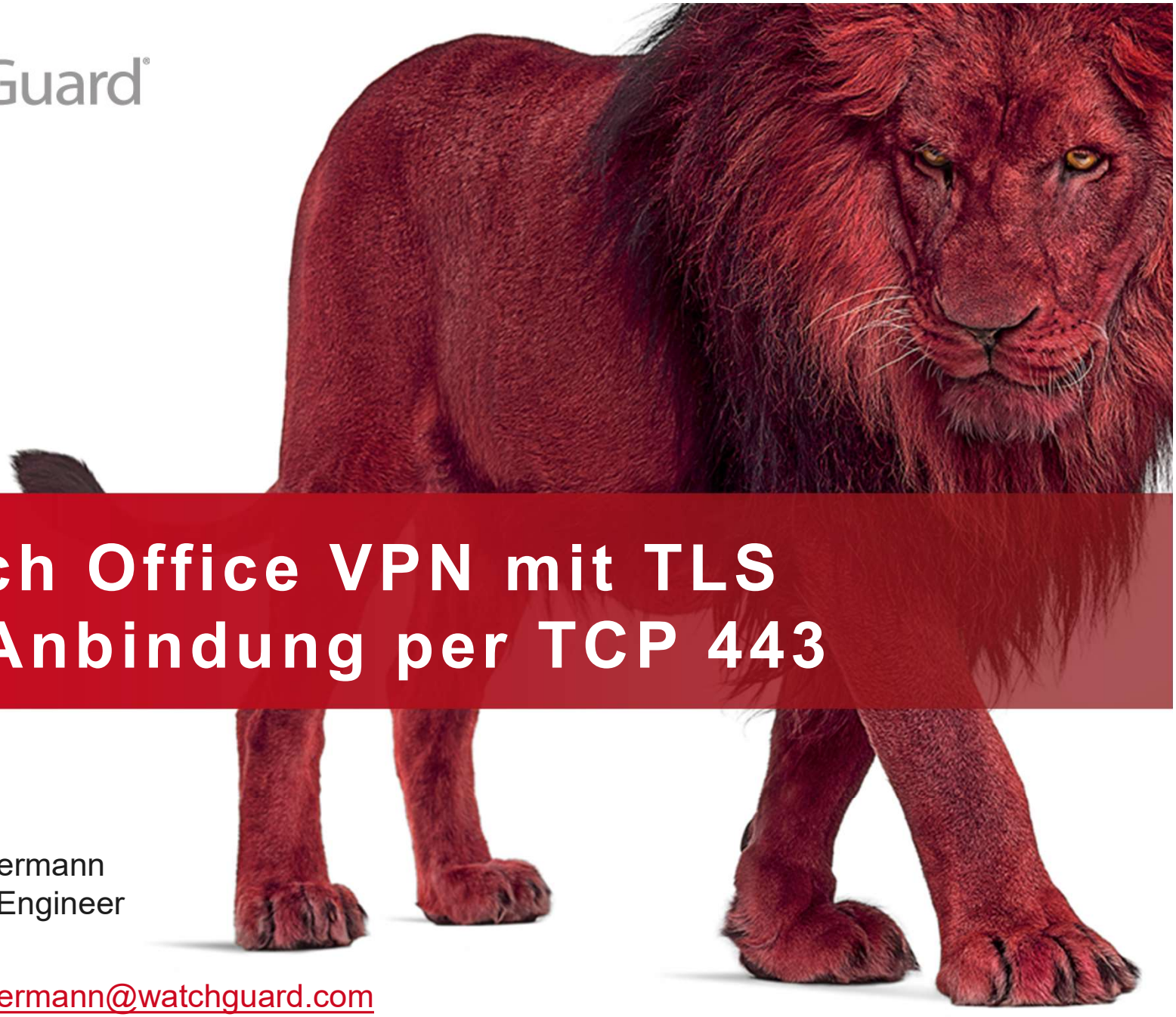


Branch Office VPN mit TLS
VPN Anbindung per TCP 443

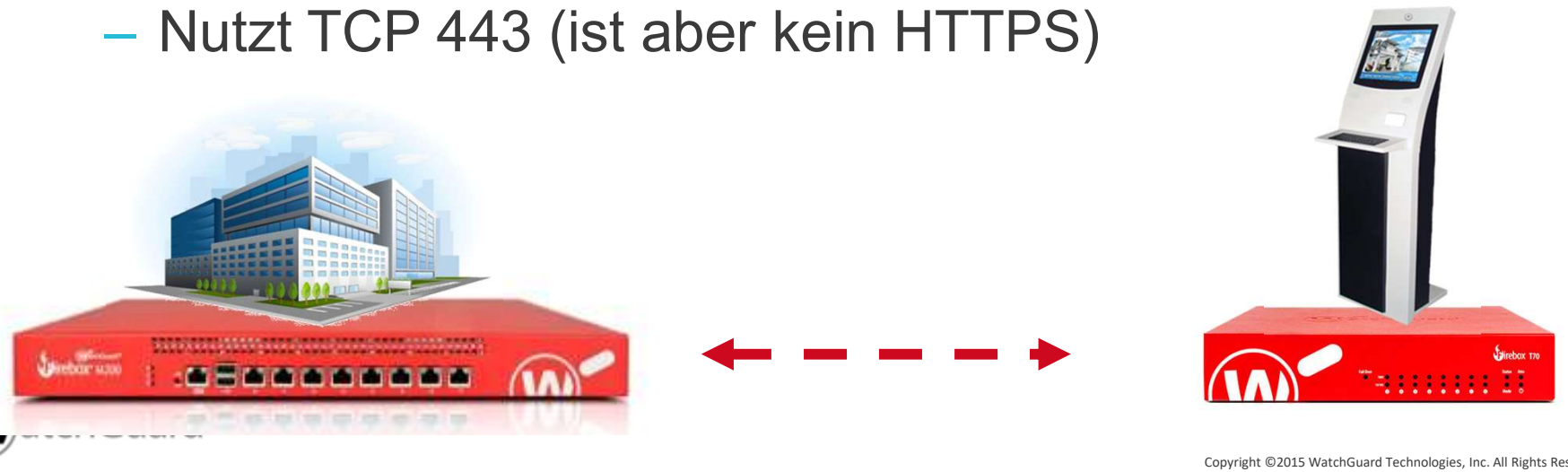
Jonas Spieckermann
Senior Sales Engineer

Jonas.Spieckermann@watchguard.com

Copyright ©2015 WatchGuard Technologies, Inc. All Rights Reserved

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)



Copyright ©2015 WatchGuard Technologies, Inc. All Rights Reserved

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

Copyright ©2015 WatchGuard Technologies, Inc. All Rights Reserved

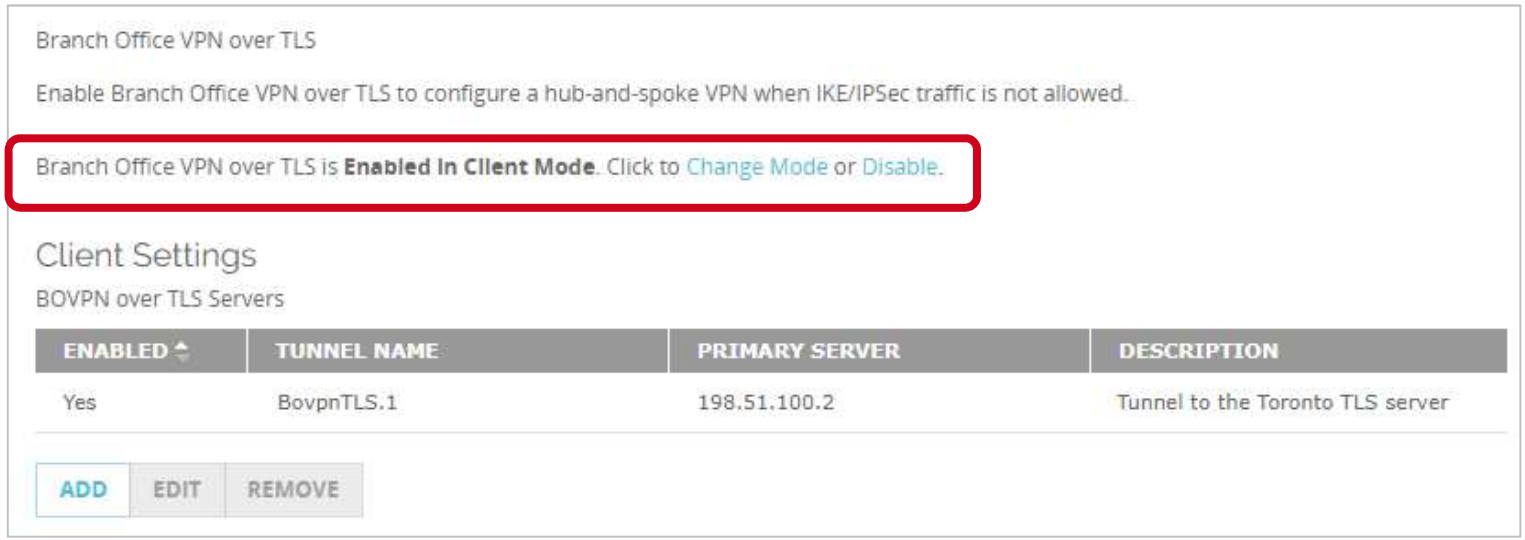
BOVPN Over TLS

- 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.

Copyright ©2015 WatchGuard Technologies, Inc. All Rights Reserved

BOVPN Over TLS

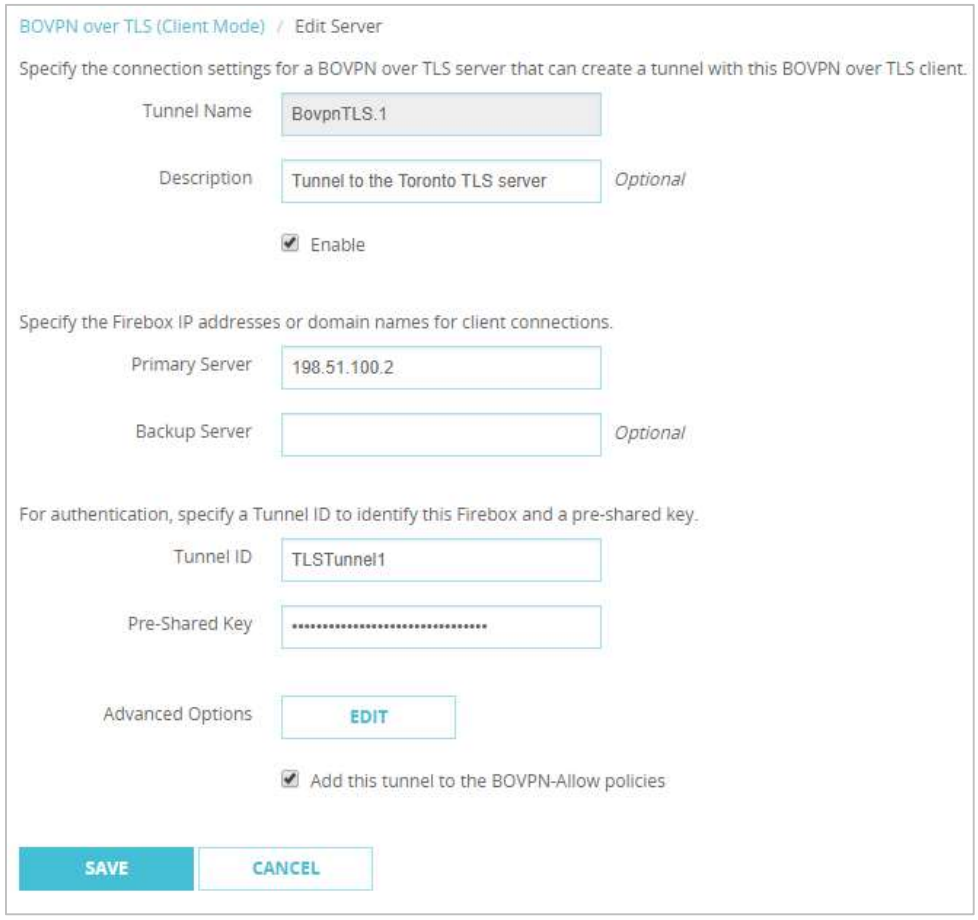
- Aktivierung Client Mode



Copyright ©2015 WatchGuard Technologies, Inc. All Rights Reserved

BOVPN Over TLS

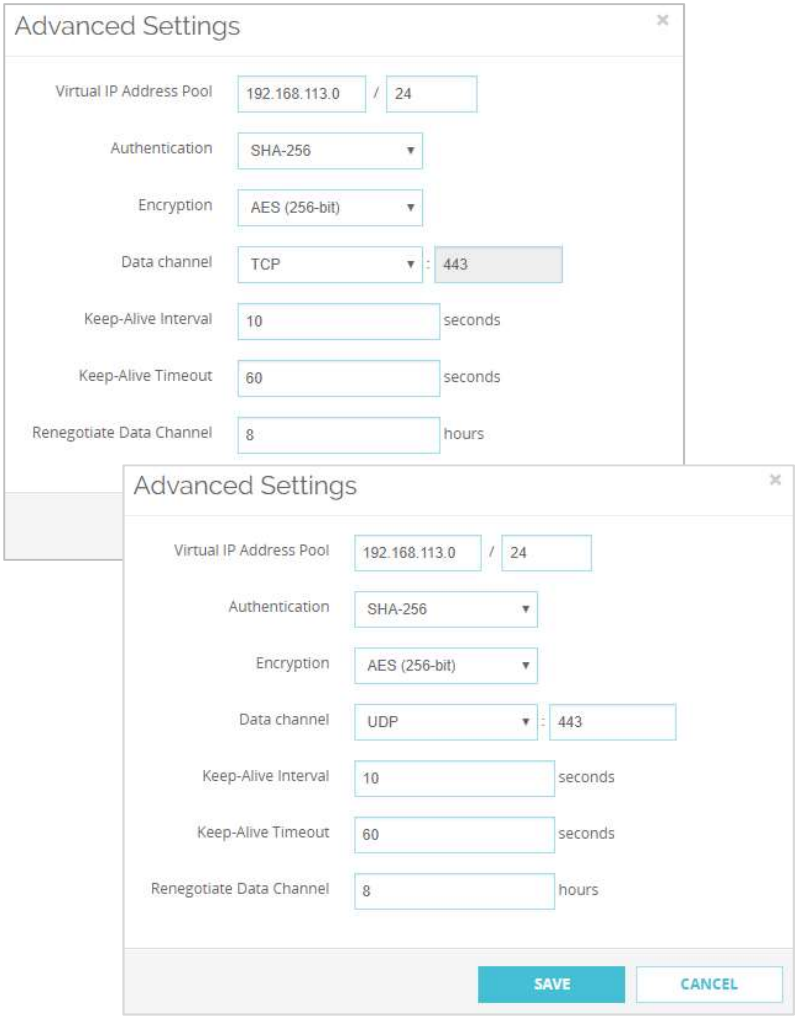
- Konfiguration des Client mode



Copyright ©2015 WatchGuard Technologies, Inc. All Rights Reserved

BOVPN Over TLS

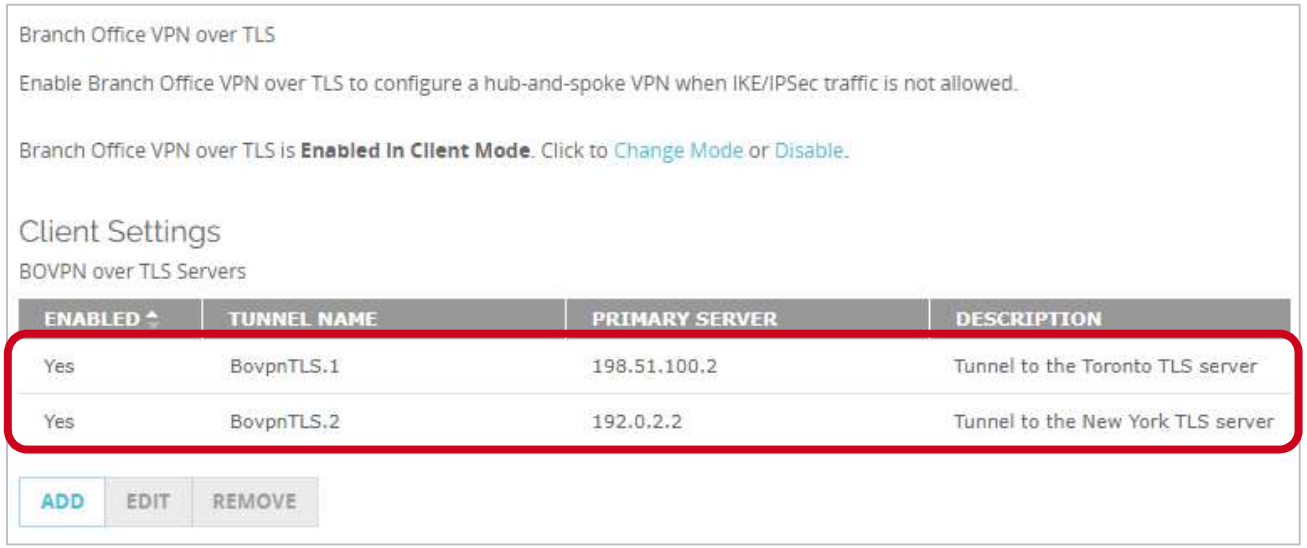
- **Advanced Settings** ermöglicht Anpassungen der Authentication und Encryption Settings
- Der TCP data channel ist dauerhaft auf Port 443
- Soll ein anderer Port als 443 genutzt werden, muss UDP zum Einsatz kommen
- **Import configuration file** ist nur zu Testzwecken vorhanden und wird bald entfernt.



Copyright ©2015 WatchGuard Technologies, Inc. All Rights Reserved

BOVPN Over TLS

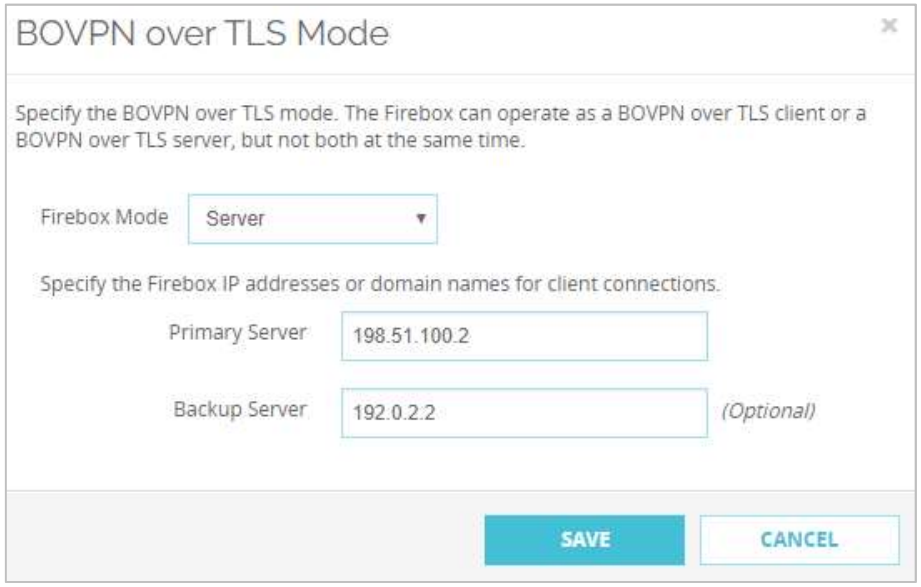
- VPN Tunnel zu mehreren TLS Servern sind möglich



Copyright ©2015 WatchGuard Technologies, Inc. All Rights Reserved

BOVPN Over TLS

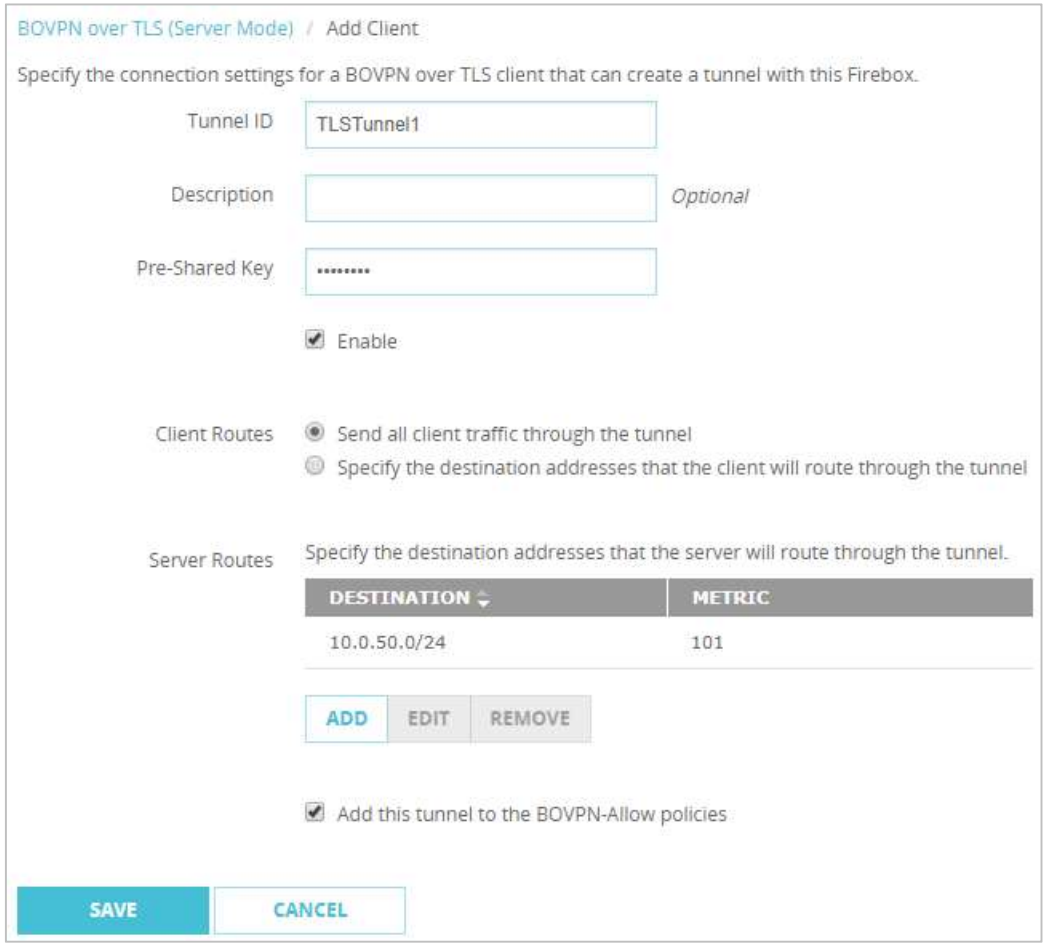
- Aktivierung Server mode



Copyright ©2015 WatchGuard Technologies, Inc. All Rights Reserved

BOVPN Over TLS

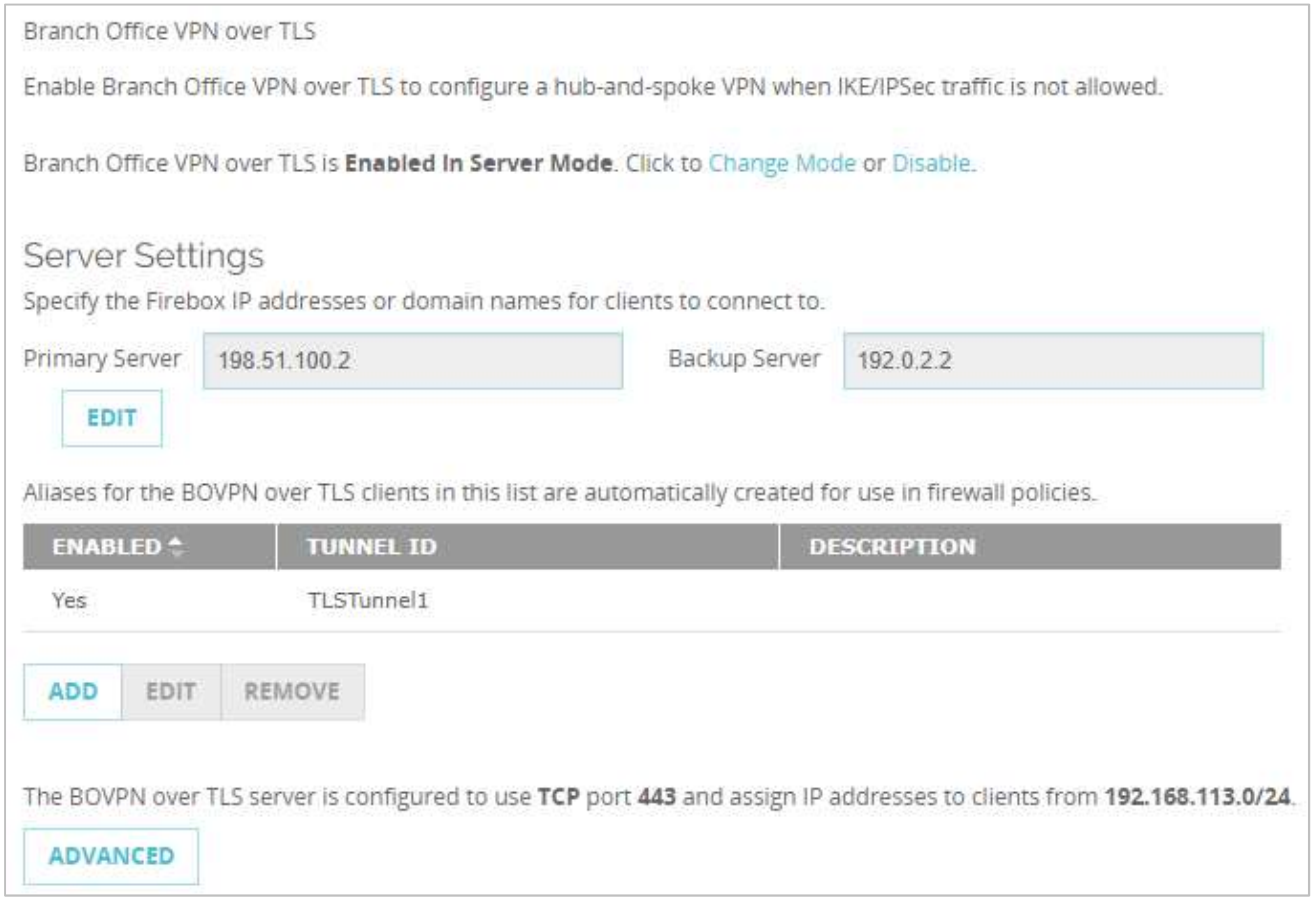
- Konfiguration Server mode



Copyright ©2015 WatchGuard Technologies, Inc. All Rights Reserved

BOVPN Over TLS

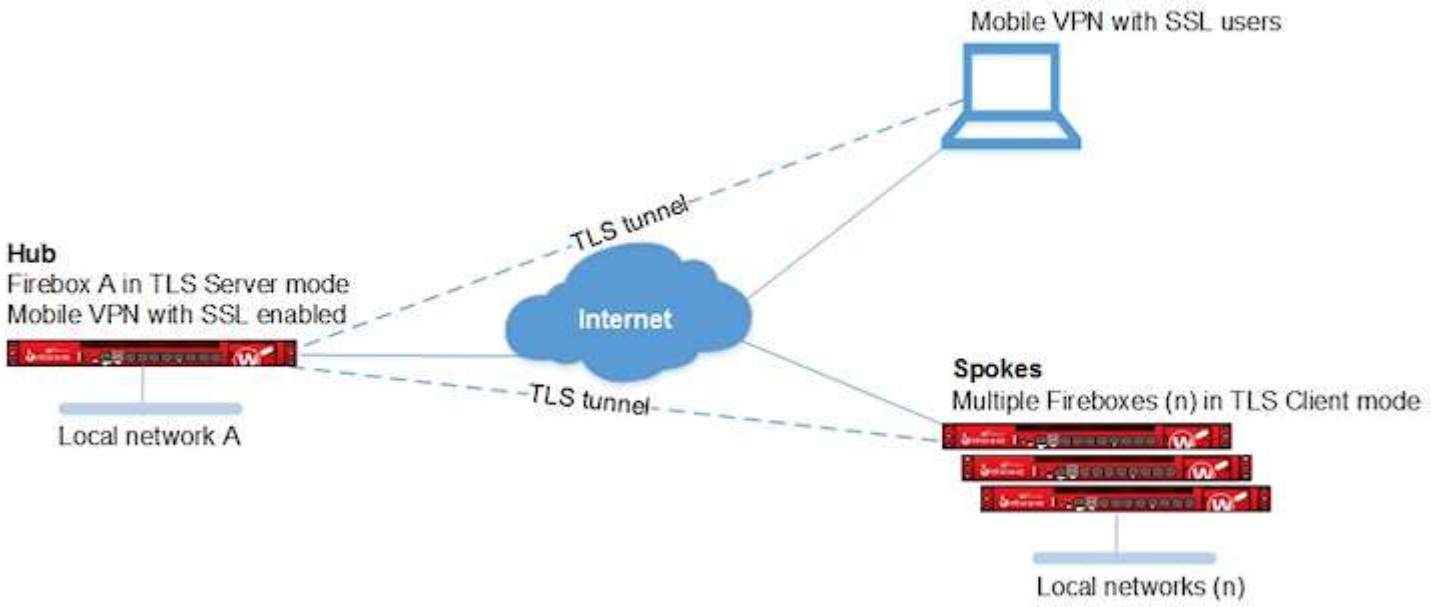
- Konfiguration Server mode



Copyright ©2015 WatchGuard Technologies, Inc. All Rights Reserved

BOVPN Over TLS

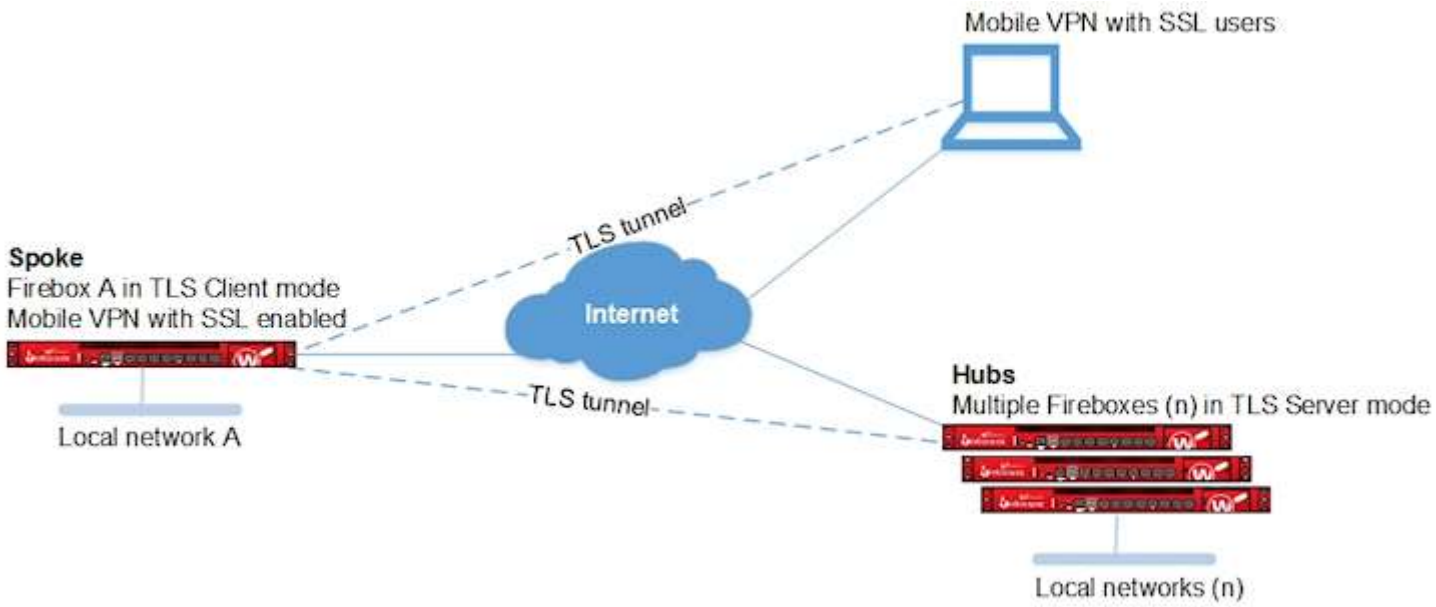
- Option 1: TLS server connects to multiple TLS clients



Copyright ©2015 WatchGuard Technologies, Inc. All Rights Reserved

BOVPN Over TLS

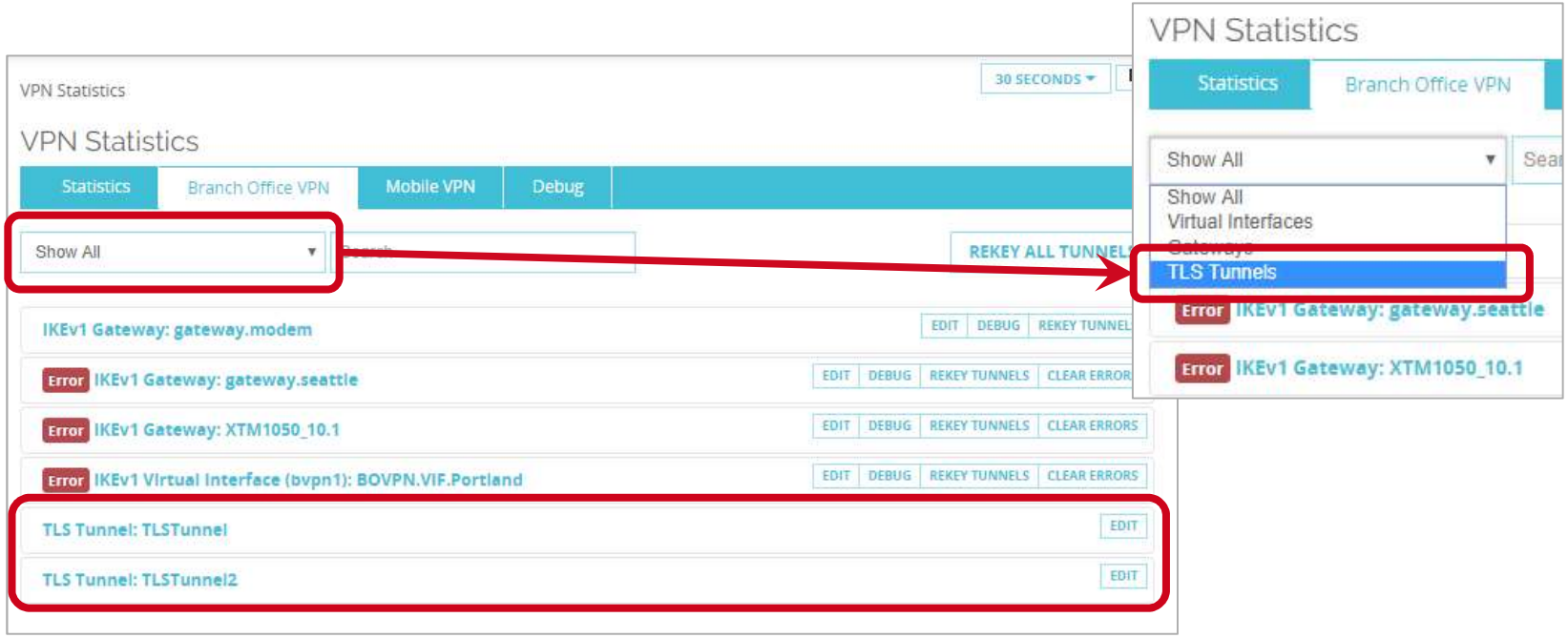
- Option 2: TLS client connects to multiple TLS servers



Copyright ©2015 WatchGuard Technologies, Inc. All Rights Reserved

BOVPN Over TLS

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



Copyright ©2015 WatchGuard Technologies, Inc. All Rights Reserved

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

Copyright ©2015 WatchGuard Technologies, Inc. All Rights Reserved

Live: BOVPN mit TLS

Copyright ©2015 WatchGuard Technologies, Inc. All Rights Reserved

Vielen Dank

Jonas Spieckermann
Senior Sales Engineer

Jonas.Spieckermann@watchguard.com

Copyright ©2015 WatchGuard Technologies, Inc. All Rights Reserved