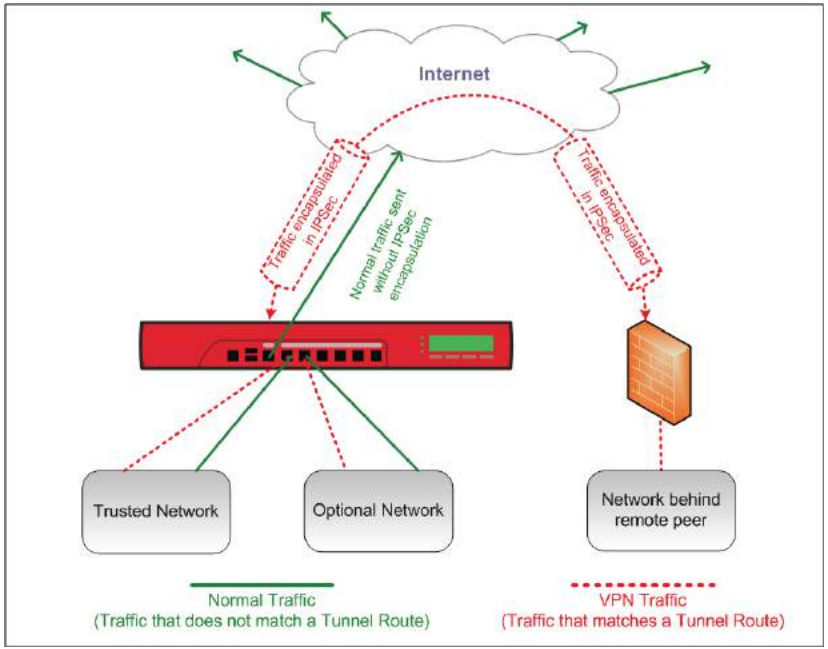
Standortvernetzung
BOVPN, Virtual Interface, BOVPN over TLS?

Jonas Spieckermann | Senior Sales Engineer
Jonas.Spieckermann@watchguard.com
WatchGuard Technologies Inc.

Grundlagen

VPN wird zur Datenübertragung über ein unsicheres Netzwerk (meist das Internet) genutzt, um durch Verschlüsselung und

Authentifizierung die Integrität und den Schutz der Daten sicherzustellen.



Grundlagen

VPN Aushandlung

- Peers prüfen Parameter (z.B. Verschlüsselung)
- „Initiator“ und „Responder“

- Phase 1 erzeugt einen sicheren Tunnel zum Start von Phase 2
  - Branch Office Gateway
- Phase 2 definiert welche Verbindungen über den VPN Tunnel ermöglicht werden
  - Security Assosiation
  - Branch Office Tunnel

Grundlagen

Ports und Protokolle

- UDP port 500 — Internet Security Association and Key Management Protocol (ISAKMP) and Internet Key Exchange (IKE)
- IP Protocol 50 — Encapsulating Security Payload (ESP)
- IP protocol 51 — Authentication Header (AH)
  - No encryption – only authentication
- UDP port 4500 — NAT Traversal (NAT-T)
  - Used if one VPN peer is behind a NAT-Router
  - Encrypted traffic send using UDP 4500
    - IPSec packet encapsulated in UDP 4500

Noch mehr Theorie?

Fireware > Fireware Help > Configure Network Settings > Manual Branch Office VPN Tunnels > About IPSec VPNs

How IPSec VPNs Work

WatchGuard Branch Office VPN, Mobile VPN with IPSec, Mobile VPN with L2TP, and Mobile VPN with IKEv2 use the IPSec protocol suite to establish virtual private networks between devices or mobile users. Before you configure an IPSec VPN, especially if you configure a manual branch office VPN tunnel, it is helpful to understand how IPSec VPNs work.

For more information, see:

- Branch Office VPN Terminology
- About IPSec Algorithms and Protocols
- About IPSec VPN Negotiations
- Configure Phase 1 and Phase 2 Settings

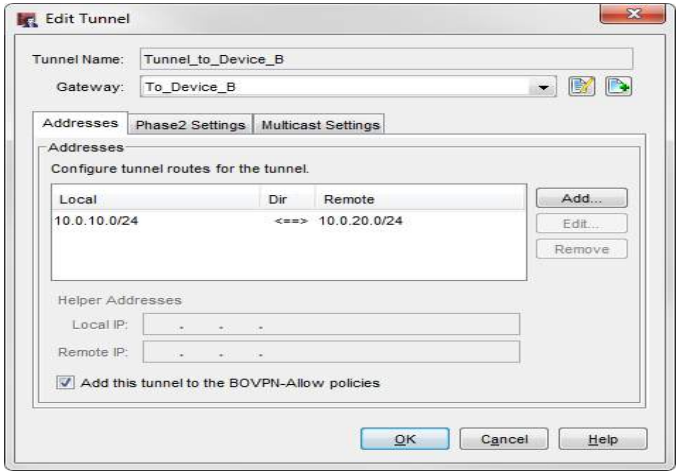
https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/mvpn/general/ipsec_vpn_intro_c.html

Varianten in WatchGuard Firebox

- Standortvernetzung über
  - Branch Office VPN Gateway und Tunnel
  - Branch Office VPN Virtual Interface
  - Branch Office VPN over TLS

Manual BOVPN

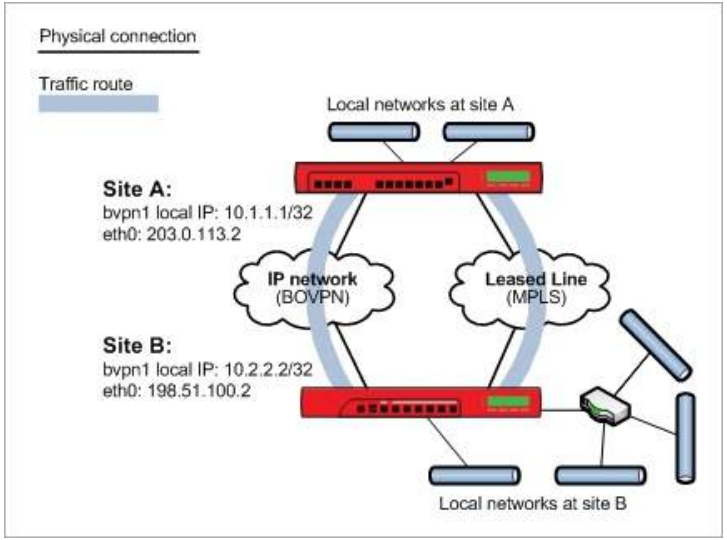
- Konfiguration von Gateway und Tunnel
  - **Gateway** — Interface, IP Parameter, PSK, Zertifikat (Phase 1 der VPN Verbindung)
  - **Tunnel** — Netzwerkzuordnung und Tunnel Routen (Phase 2 der VPN Verbindung)
- Verwendung:
  - VPN Verbindung zwischen 2 Firebox Systemen
  - VPN Verbindung zu 3rd Party Firewall
  - VPN Verbindung mit Zero-Route VPN für ein Netzwerk – andere Netzwerke ohne Zero-Route VPN



BOVPN Virtual Interface

- Das BOVPN Virtual Interface wird als “Schnittstelle” eingerichtet
  - Über VPN Routen können Zielnetze angegeben werden
  - Steuerung und Kombination mit Routing Tabelle
  - Metric entscheidet über Routingentscheidung
  - “Ziel Entscheidung”

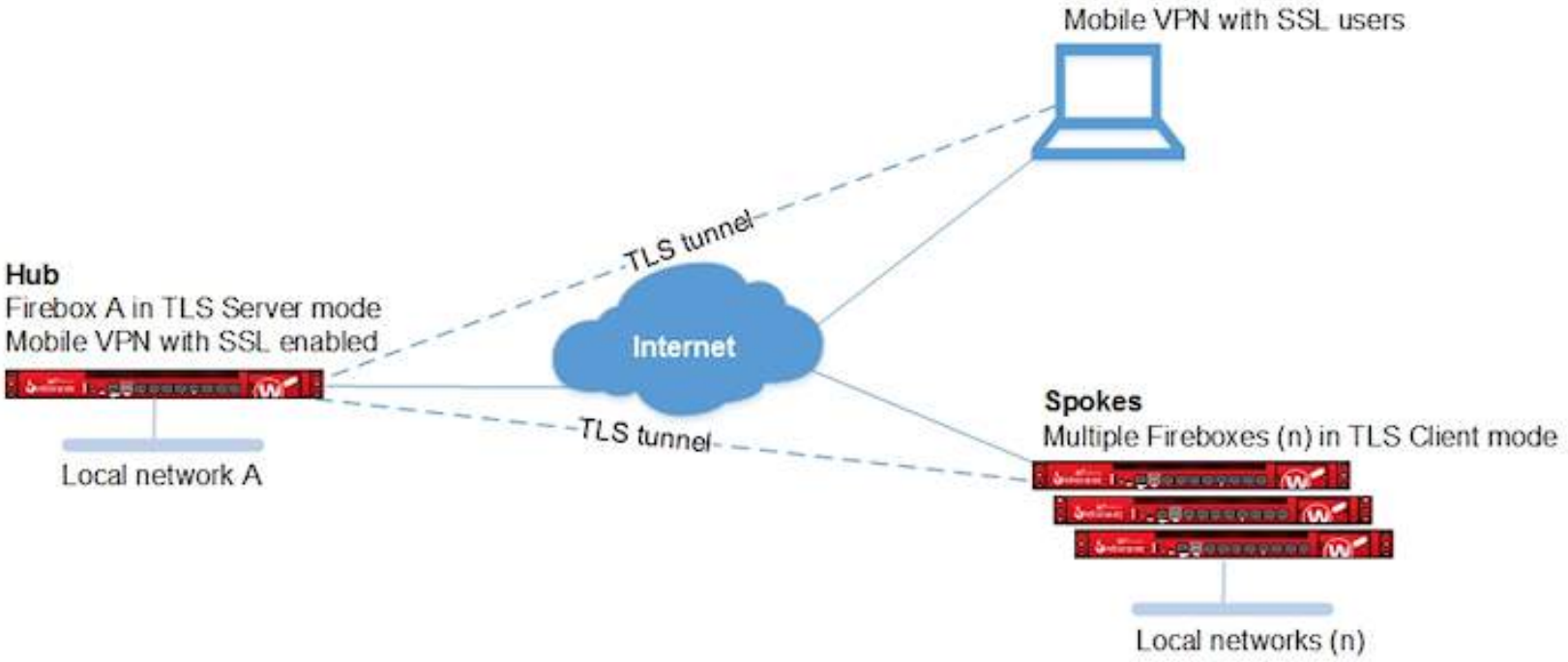
- Verwendung:
  - Policy-based routing
  - Metric-based failover and failback
  - Dynamic routing
  - SD-WAN inklusive VPN
  - IPv6 routing through the IPv4 tunnel
  - Anbindung an Azure, AWS, etc.



BoVPN over TLS

- Site-to-Site VPN mit TLS 1.2
  - 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

- 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

Vielen Dank!

Jonas Spieckermann | Senior Sales Engineer
Jonas.Spieckermann@watchguard.com
WatchGuard Technologies Inc.