Best Practices
Standortvernetzung mit SD-WAN

SD-WAN

SD-WAN (Software Defined Wide Area Networking) ermöglicht:

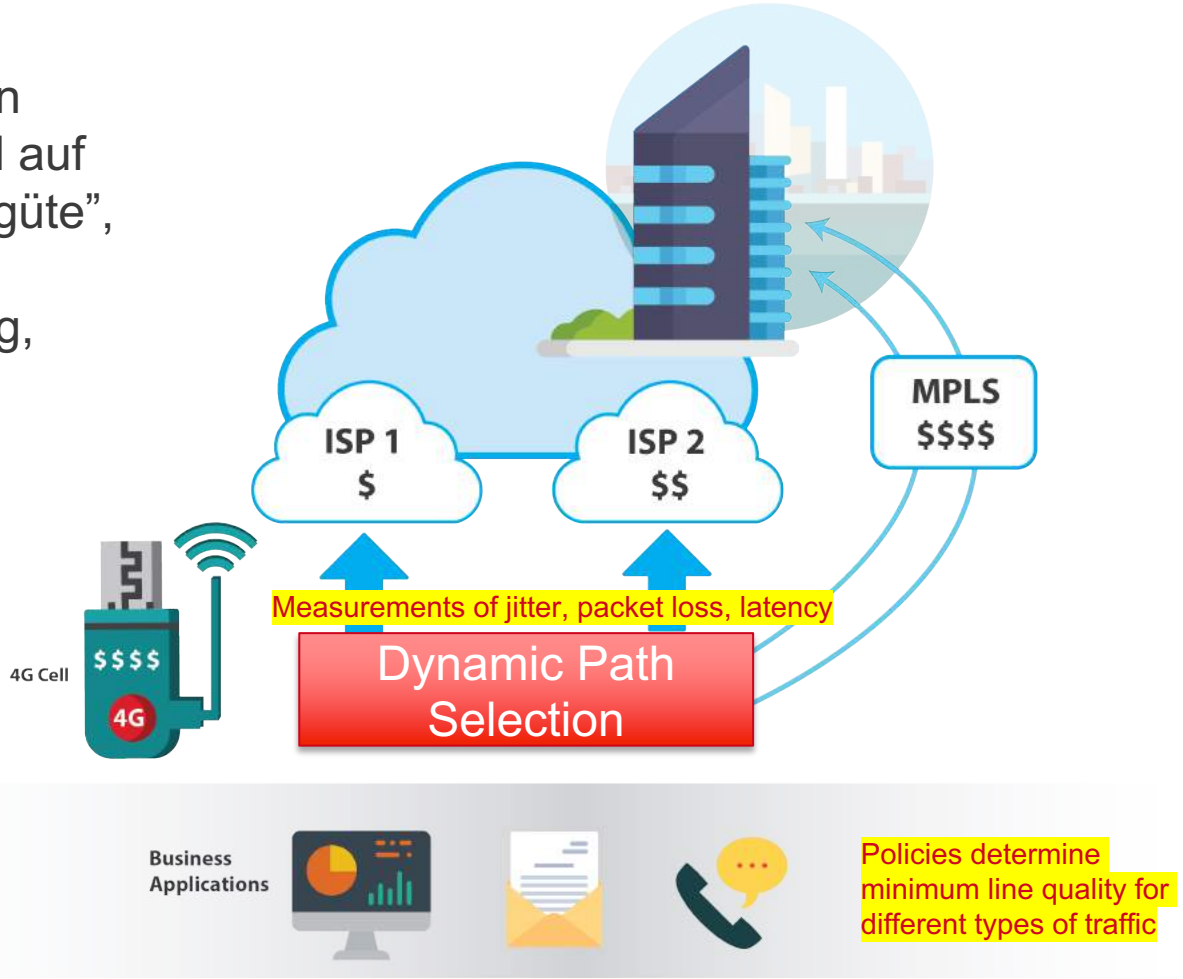
1) Eine Hybrid-WAN Architektur zur gesteigerten Performance bei Verwendung von Cloud Applikationen
2) Kontrolle der WAN Kosten mit geringer Auswirkung auf die Netzwerk Effizienz
3) Erleichterte Verwaltung mehrerer WAN Leitungen durch Automatisierung
4) Reduzierte Notwendigkeit von technischen Ressourcen vor Ort.

Automatische Leitungswahl für beste Performance.

SD-WAN ist die “Echtzeit Navigation” für Netzwerke

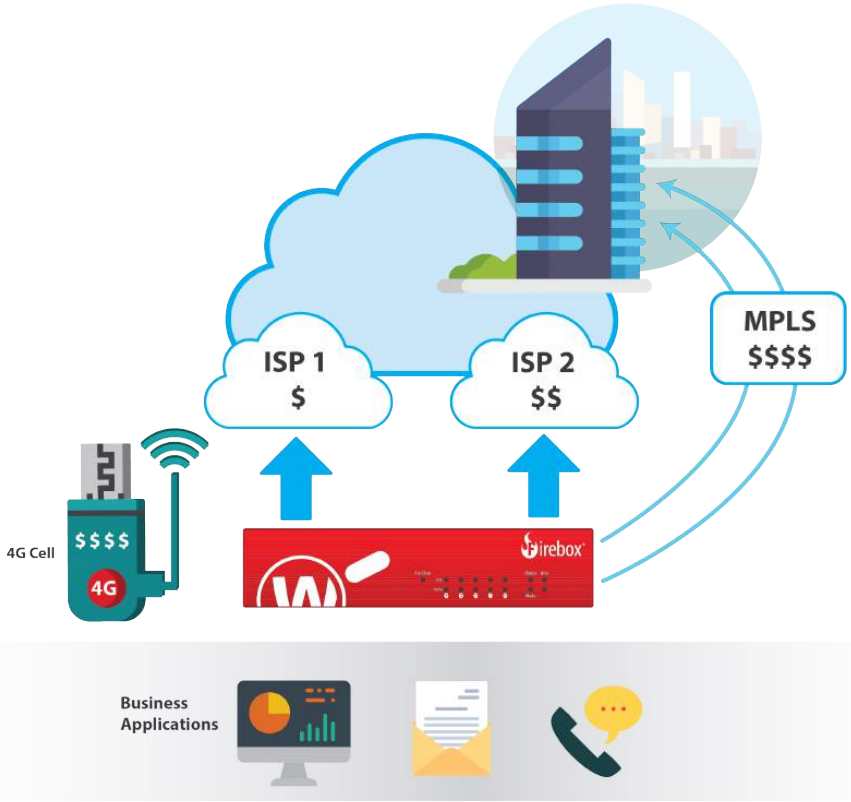
Dynamic Path Selection basierend auf aktuellem Zustand

Entscheidungen werden automatisiert basierend auf der aktuellen “Leitungsgüte”, ermittelt durch kontinuierliche Messung, durchgeführt



SD-WAN und WatchGuard Firebox

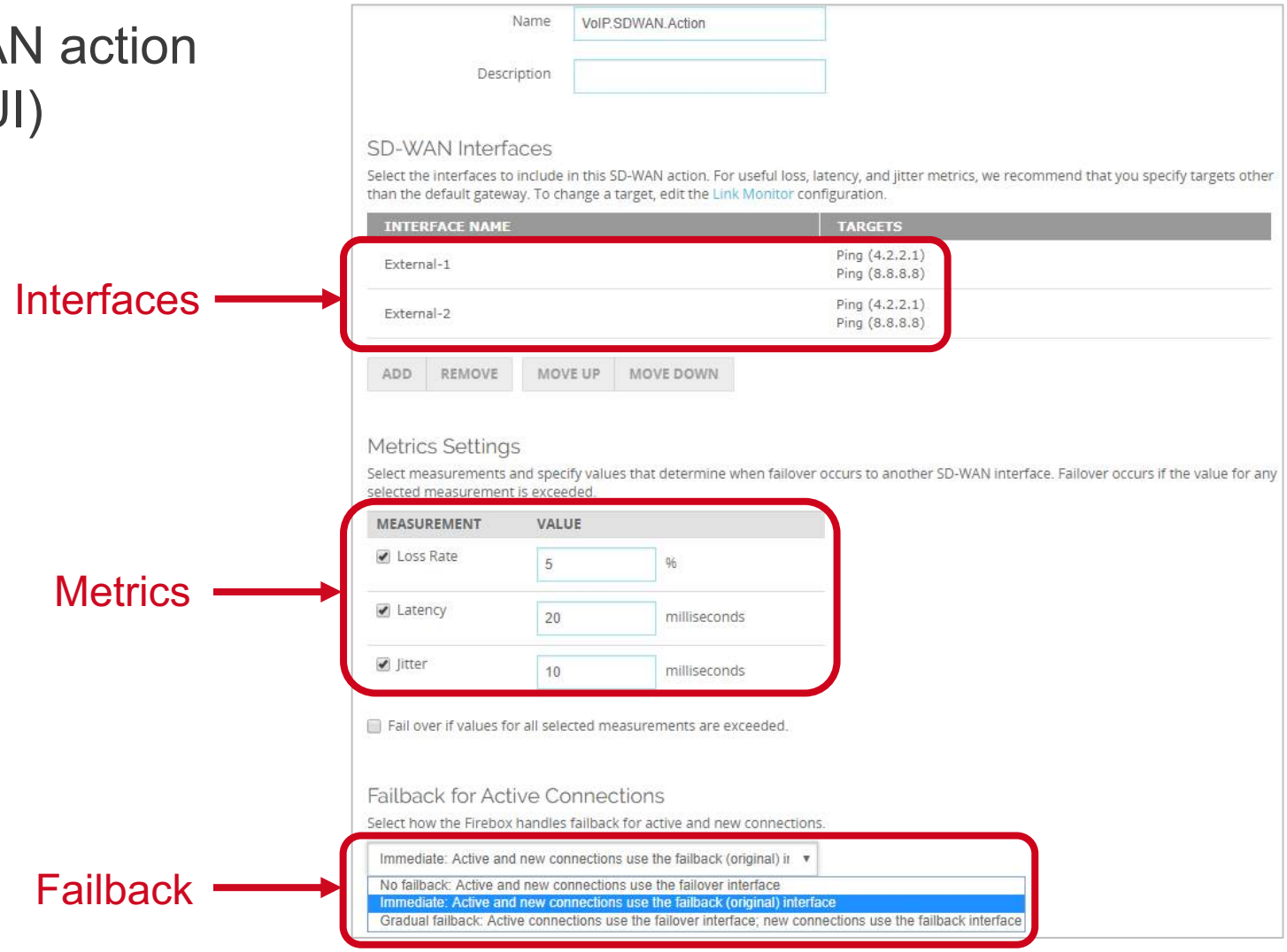
- Über 20 Jahre Erfahrung bei Firewalls mit fortschrittlicher Netzwerk-Funktionalität
- Durch RapidDeploy, zentralem Management und verlässlichen BOVPNs bestens geeignet für verteilte Infrastruktur
- Bekannt für einfach verwaltbare “enterprise-grade security” Funktionen



SD-WAN ist als Standard Funktion für alle Firebox Appliances verfügbar.

SD-WAN Actions

- SD-WAN action (Web UI)



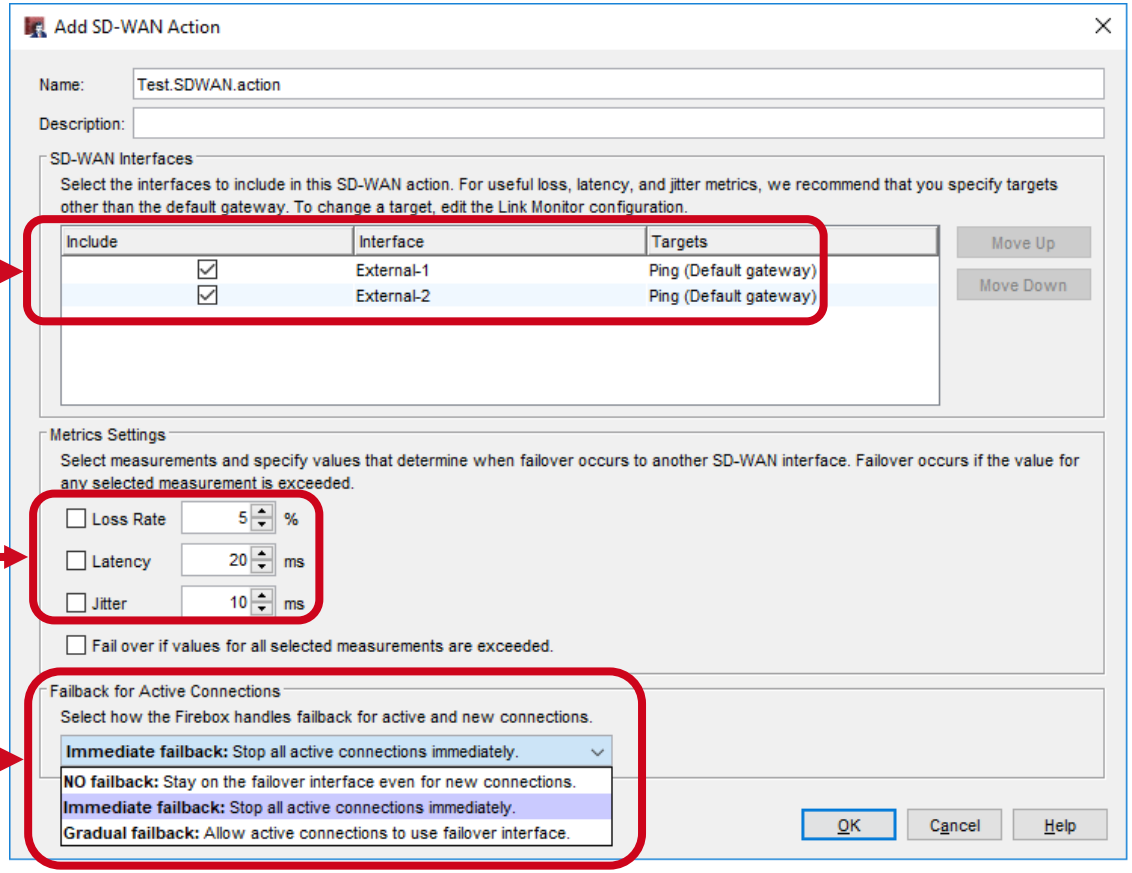
SD-WAN Actions

- SD-WAN action (Policy Manager)

Interfaces

Metrics

Failback



SD-WAN Actions

- *SD-WAN actions* ersetzen policy-based routing
- *SD-WAN actions* bieten optimierte granulare Kontrolle über die Verwendung der WAN-Leitungen (inclusive Failover und Failback) pro Policy.
  - Netzwerk Performance Parameter (packet loss, latency, jitter) fließen in die Betrachtung ein und können für Failover und Failback genutzt werden.
  - Alternativ kann (wie bisher) der Zustand (up/down) der Schnittstelle für eine Failover/Failback Entscheidung genutzt werden.
- Insbesondere für Latenz-sensitive Applikationen (VoIP, Video-Conferencing) sind *SD-WAN actions* ein effektives Werkzeug.

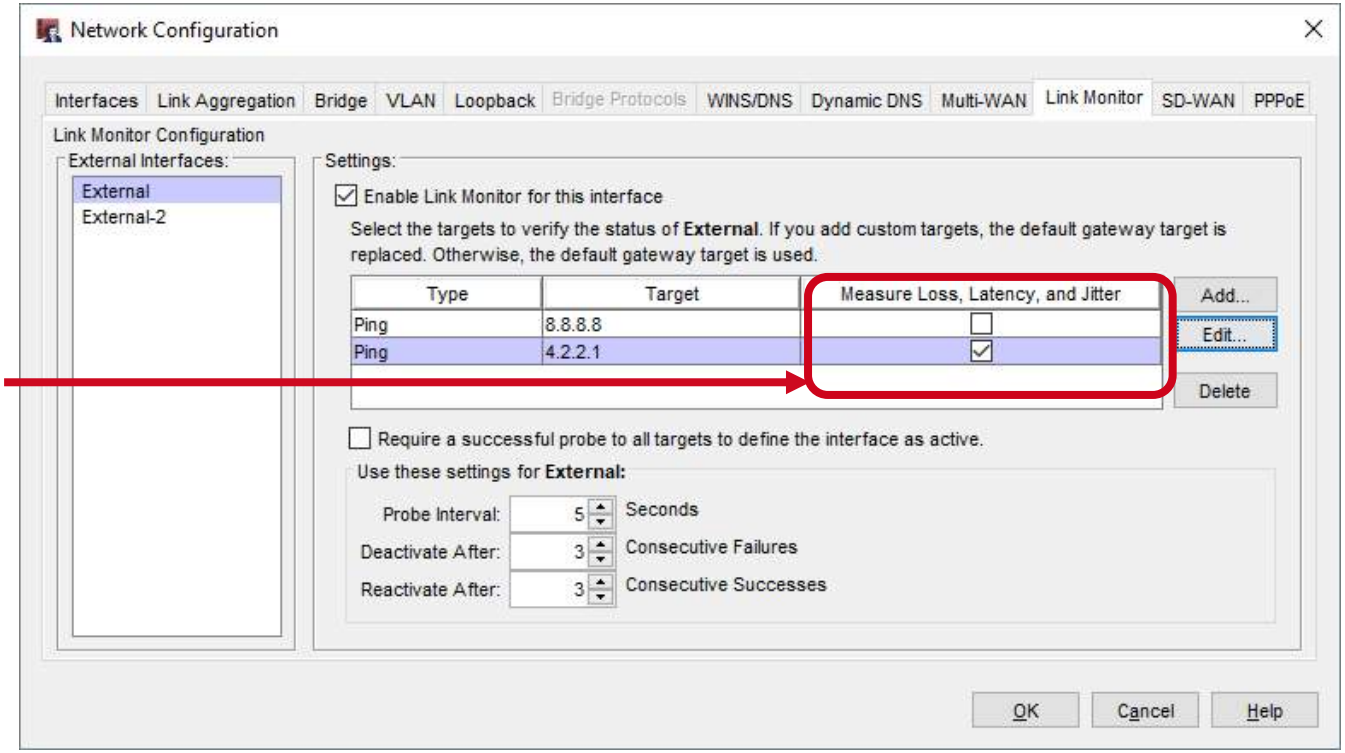
SD-WAN Actions

- *SD-WAN actions* in einer Policy haben Vorrang vor den globalen multi-WAN Einstellungen.
- Konfiguration von *SD-WAN actions*:
  - Web UI — **Network > SD-WAN**
  - Policy Manager — **Network > Configuration > SD-WAN**
- Anpassungen können auch direkt über die Policy durchgeführt werden.
- Eine *SD-WAN action* definiert:
  - Eine oder mehrere Schnittstellen
  - (Optional) Loss, latency, und jitter Schwellwerte
  - Failback Methode

Link Monitor

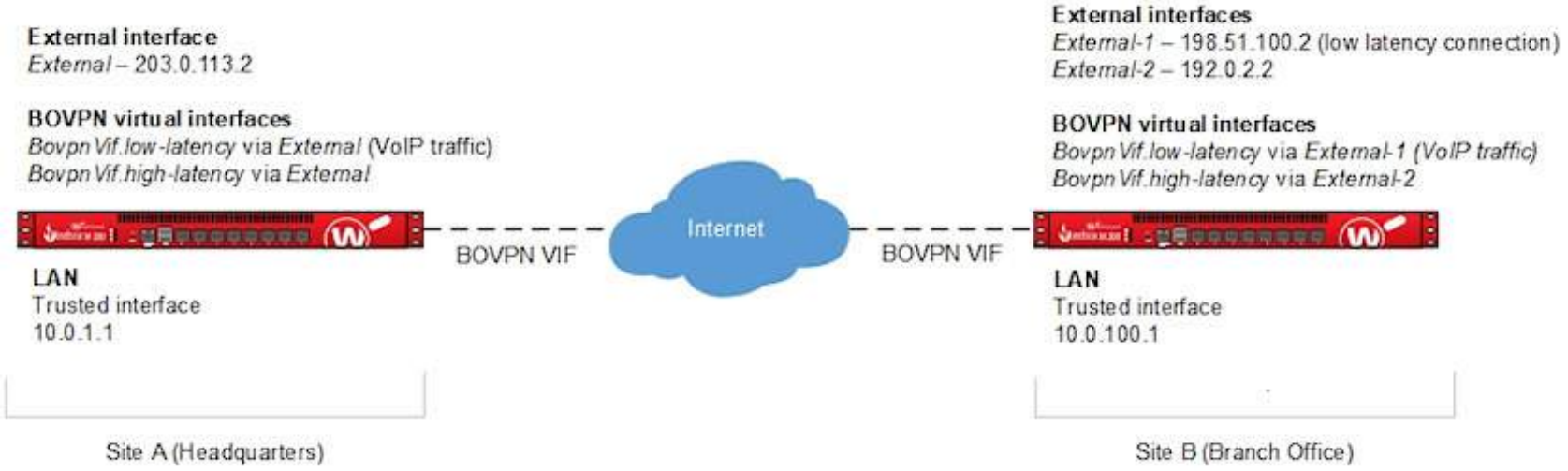
- Die Link Monitor Einstellungen ermöglichen eine “Überwachung” der Leitungen
- Auch VPN Virtual Interfaces können geprüft werden

Select to measure loss, latency, and jitter for one target



SD-WAN mit BOVPN

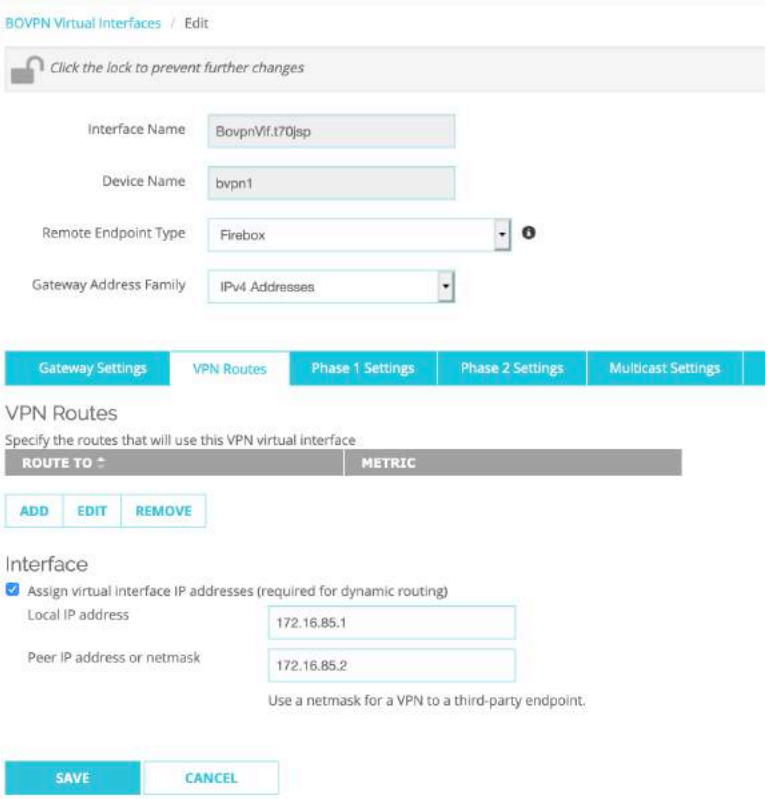
- 2 BOVPN Virtual Interface Tunnel zwischen den Standorten
  - Mit Konfiguration einer „virtual Interface IP“
- Aktivierung des Link-Monitor für das VPN Interface
- SD-WAN Actions ermöglichen eine flexible Lastverteilung

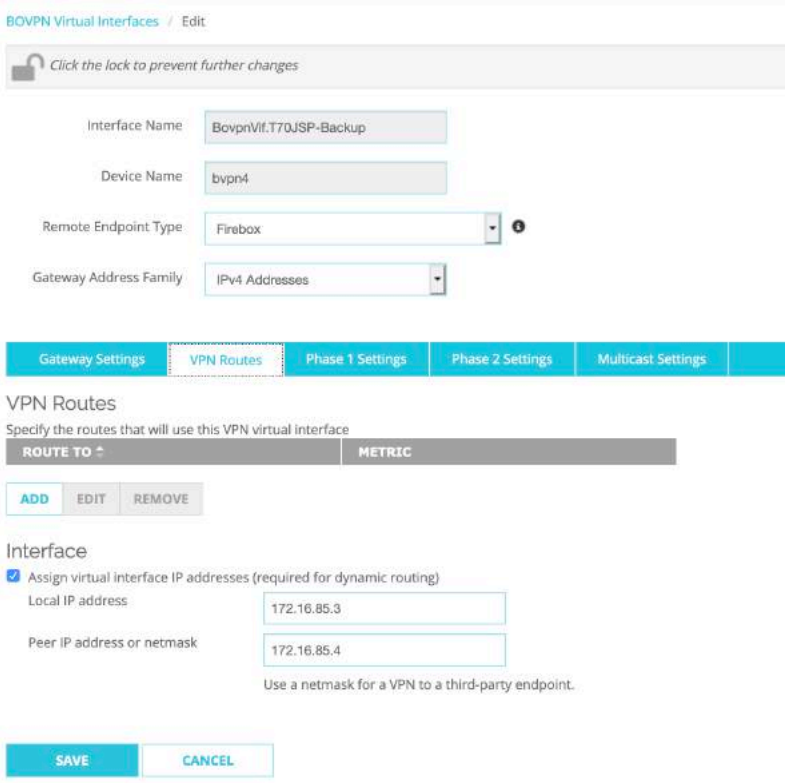


https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/bovpn/manual/bovpn_vif_pbr_c.html

BOVPN Virtual Interface

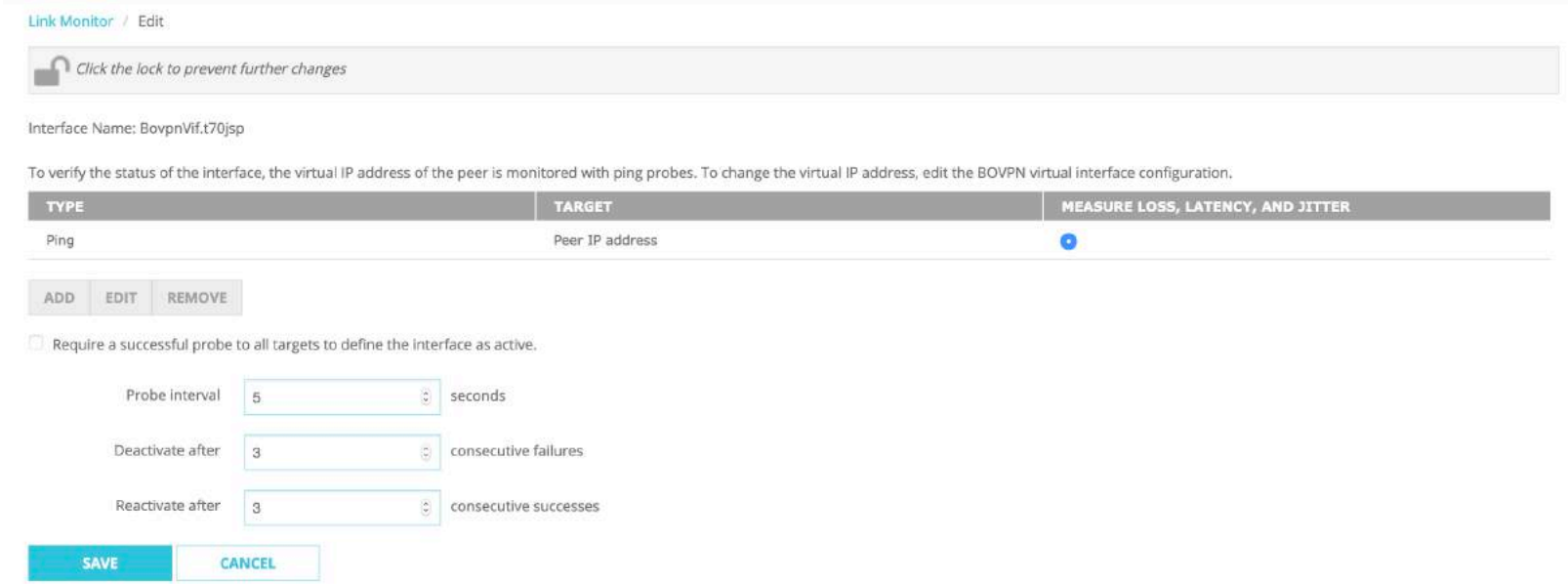
- Konfiguration von 2 BOVPN Virtual Interface Tunneln mit „virtual Interface IP“



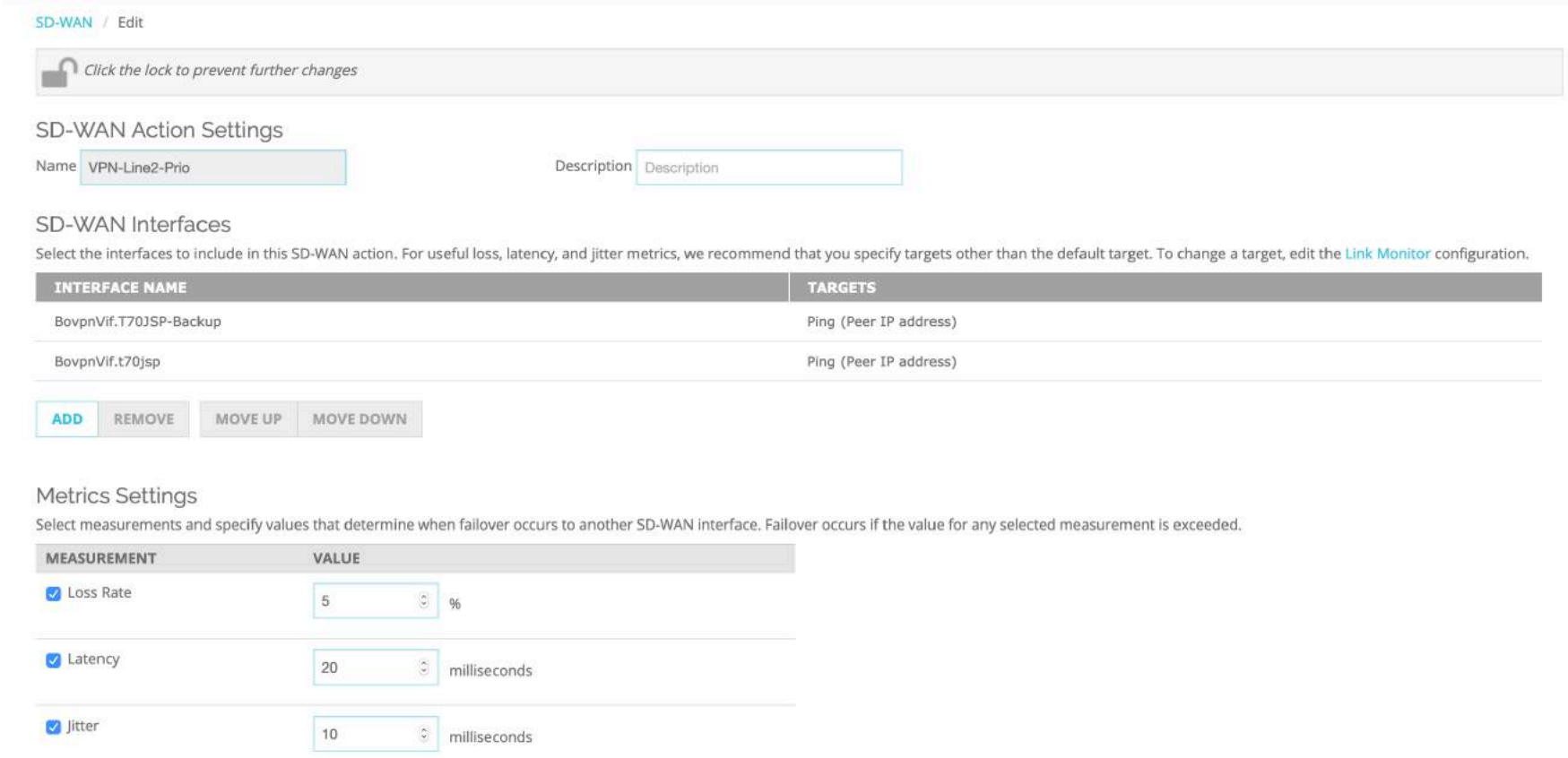


Link Monitor

- Link Monitor für beide VPN Tunnel aktivieren

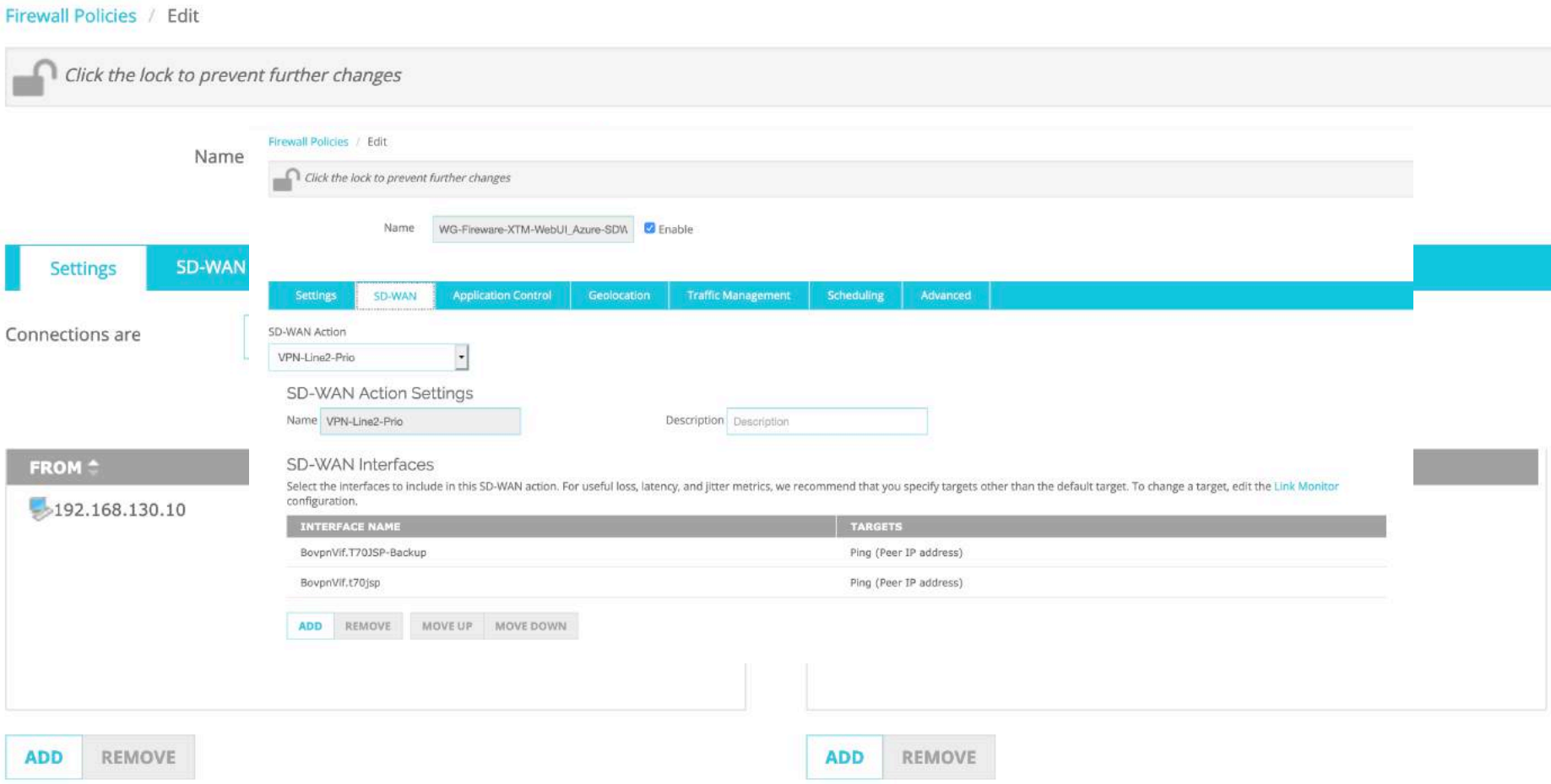


SD-WAN Actions



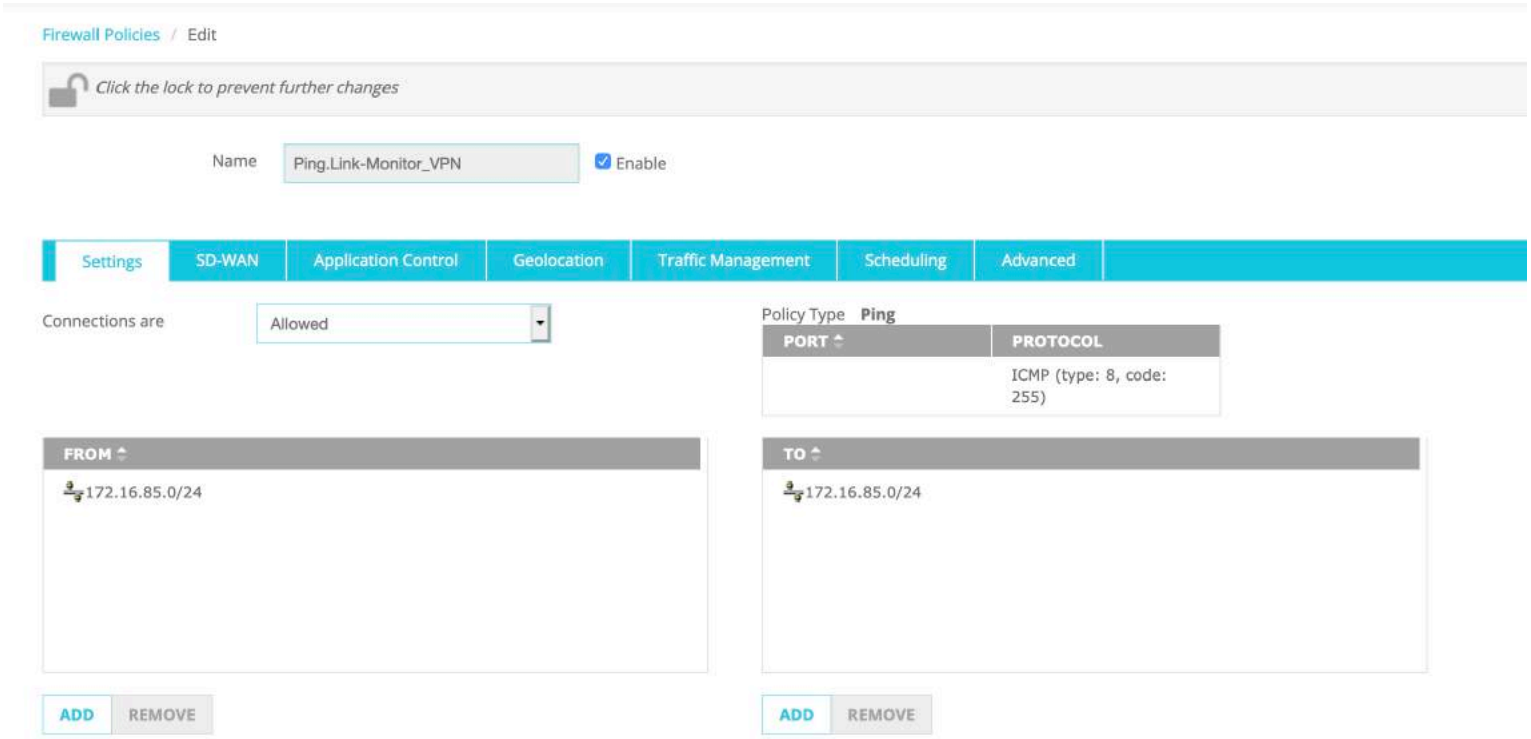
Firewall-Policies

- Zuweisung der jeweiligen SD-WAN Action in den Policies



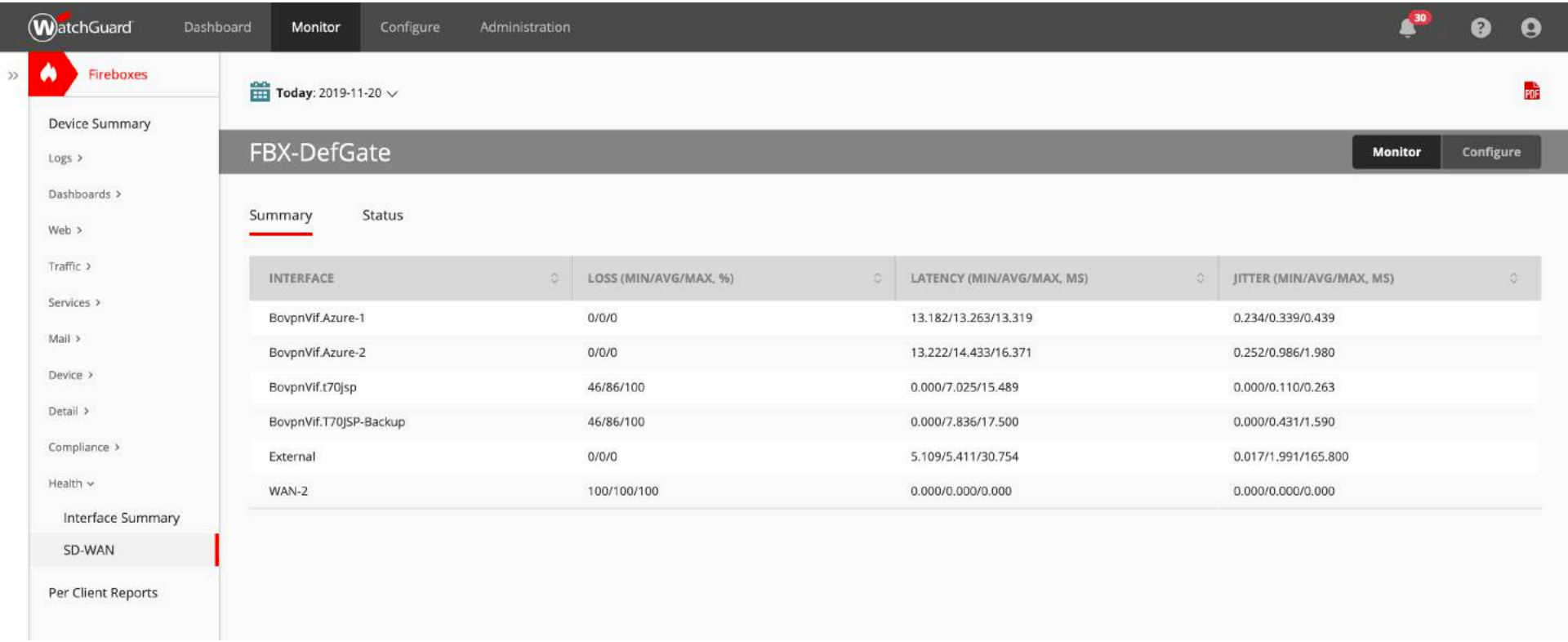
Regel für Link-Monitor

- Achtung: Wenn keine „Default VPN Regel“ genutzt wird, so muss Ping zwischen den virtual Interface IPs erlaubt sein, damit der Link Monitor funktioniert.



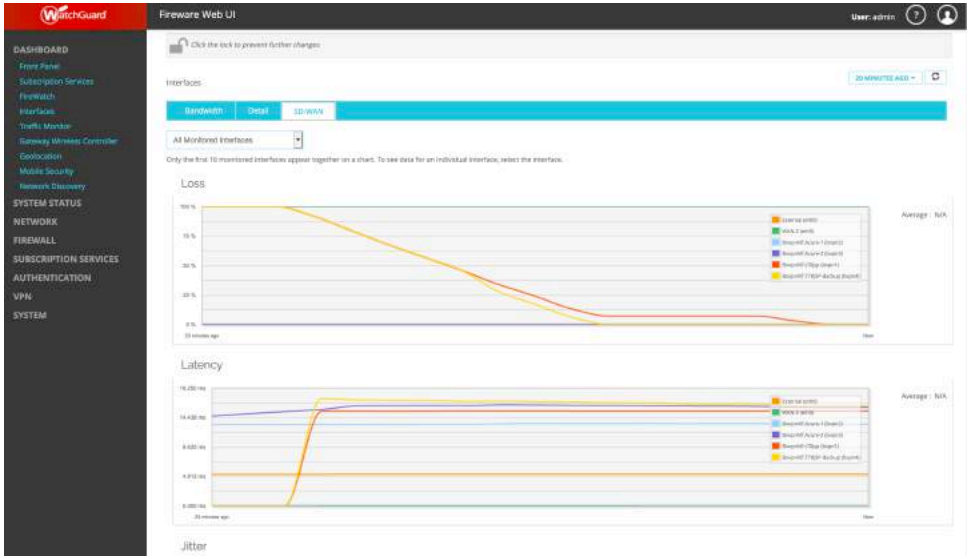
Kontrolle der SD-WAN Nutzung

- WatchGuard Cloud stellt den SD-WAN Status langfristig dar

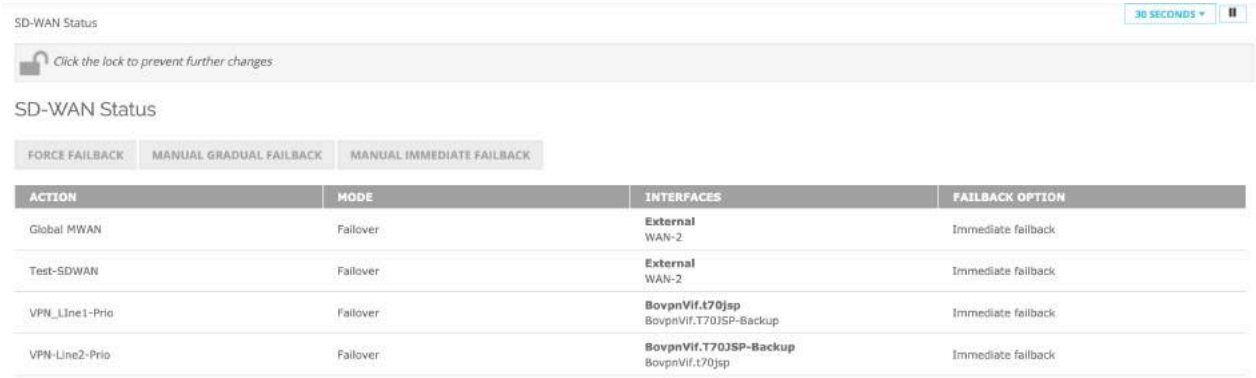


Kontrolle der SD-WAN Nutzung

- Dashboards zu SD-WAN in der Web-UI
  - Auch Firewatch mit Blick auf Interface (In) / (Out)



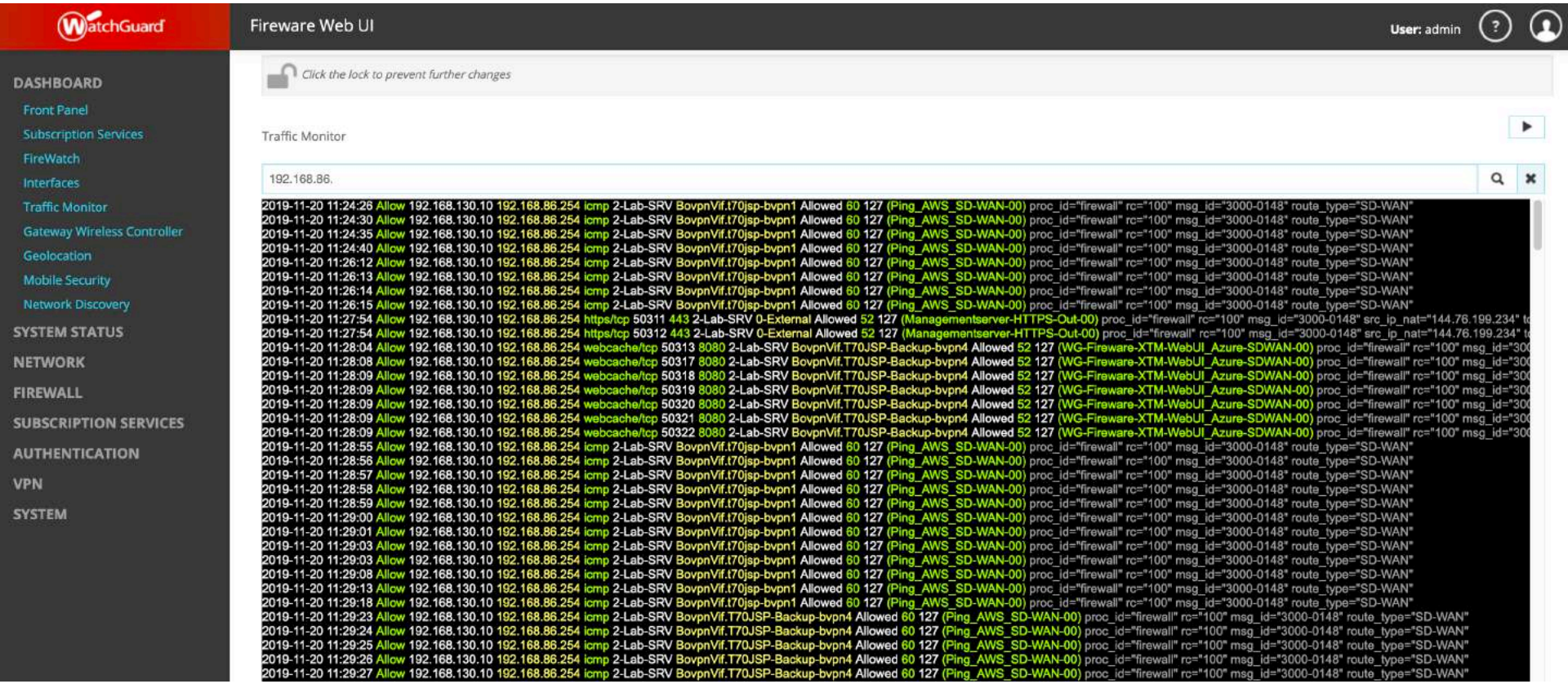
- Status zu SD-WAN in der Web-UI



ACTION	MODE	INTERFACES	FAILBACK OPTION
Global MWAN	Failover	**External** WAN-2	Immediate failback
Test-SDWAN	Failover	**External** WAN-2	Immediate failback
VPN_LIne1-Prio	Failover	**BovpnVif.t70jsp** BovpnVif.T70JSP-Backup	Immediate failback
VPN-Line2-Prio	Failover	**BovpnVif.T70JSP-Backup** BovpnVif.t70jsp	Immediate failback

Kontrolle der SD-WAN Nutzung

- Traffic Monitor stellt die genutzte Schnittstelle in jeder Logmeldung dar.



Auslösen eines Failovers

- Eine einfache Möglichkeit SD-WAN Failover zu testen ist das deaktivieren eines der BOVPN Virtual Interfaces.
  - Im Traffic Log wird der Failover und Failback sofort sichtbar

Live Demo

Vielen Dank!

NOTHING GETS PAST RED.

WatchGuard