



Best Practices — SD-Wan Actions

Jonas Spieckermann
Senior Sales Engineer
Jonas.Spieckermann@watchguard.com

SD-WAN

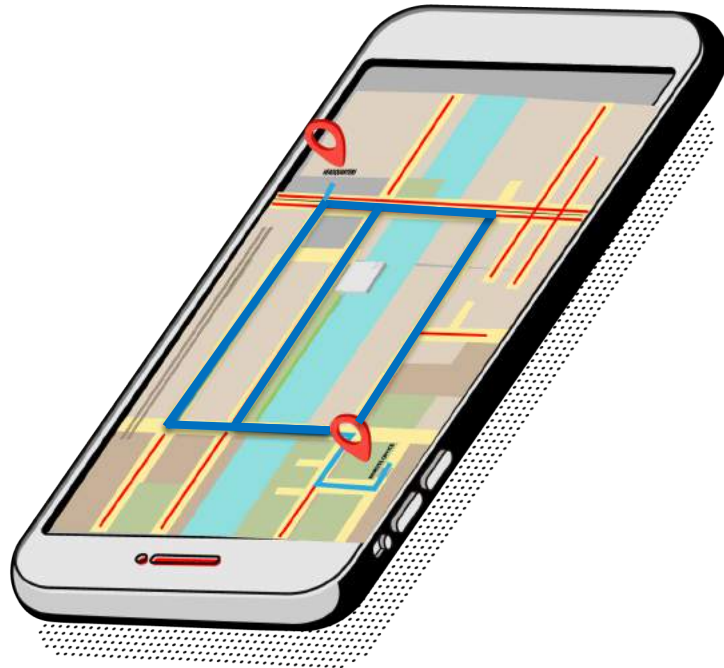
SD-WAN (Software Defined Wide Area Networking) ermöglicht:

- 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.



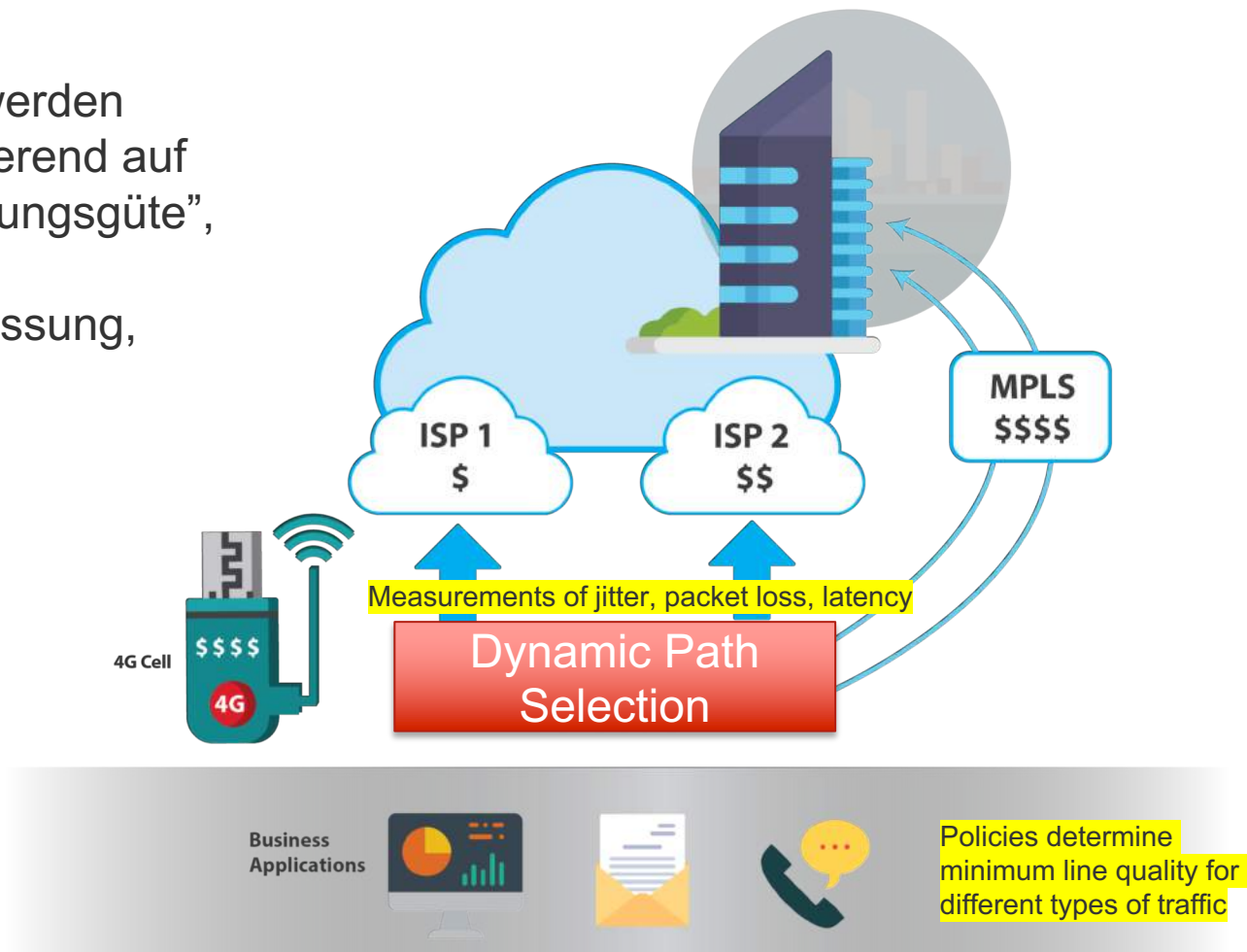
Automatische Leitungswahl für beste Performance.

SD-WAN ist die “Echtzeit Navigation” für Netzwerke



Dynamic Path Selection basierend auf aktuellem Zustand

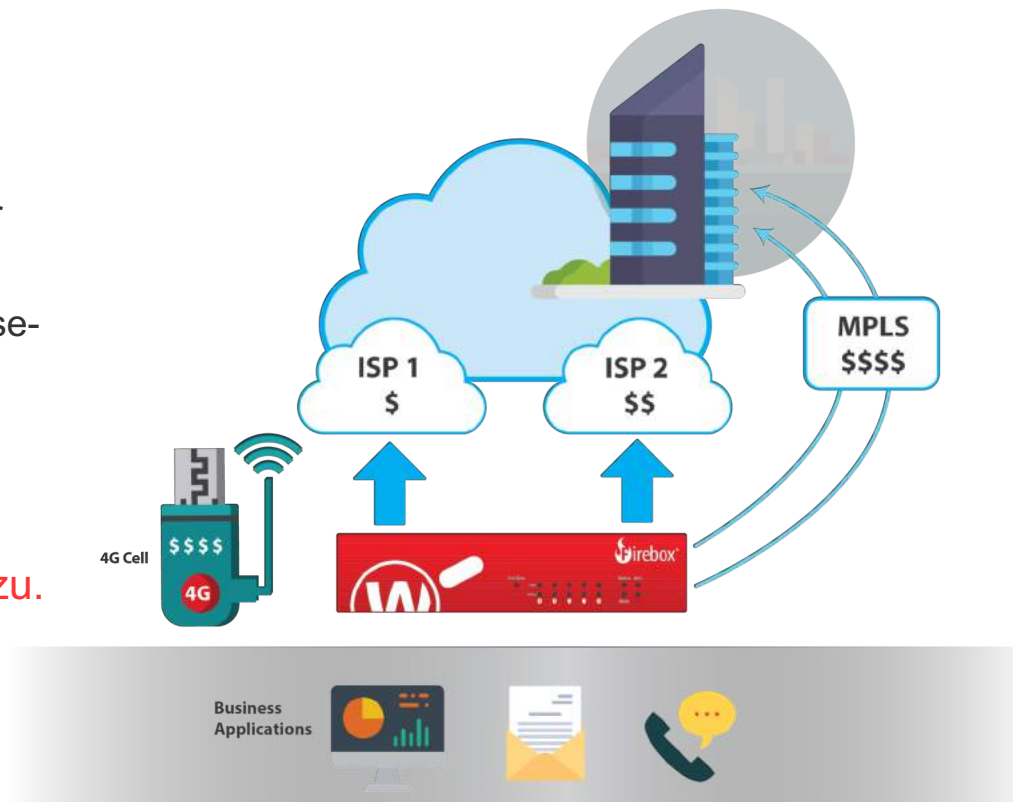
Entscheidungen werden automatisiert basierend auf der aktuellen "Leitungsgüte", ermittelt durch kontinuierliche Messung, durchgeführt



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

WatchGuard fügt SD-WAN als Standard Funktion für alle Firebox Appliances hinzu.



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 externe Schnittstellen
 - (Optional) Loss, latency, und jitter Schwellwerte
 - Failback Methode

SD-WAN Actions

- SD-WAN action (Web UI)

Interfaces

Name: VoIP.SDWAN.Action

Description:

SD-WAN Interfaces

Select the interfaces to include in this SD-WAN action. For useful loss, latency, and jitter metrics, we recommend that you specify targets other than the default gateway. To change a target, edit the [Link Monitor](#) configuration.

INTERFACE NAME	TARGETS
External-1	Ping (4.2.2.1) Ping (8.8.8.8)
External-2	Ping (4.2.2.1) Ping (8.8.8.8)

ADD REMOVE MOVE UP MOVE DOWN

Metrics Settings

Select measurements and specify values that determine when failover occurs to another SD-WAN interface. Failover occurs if the value for any selected measurement is exceeded.

MEASUREMENT	VALUE	UNIT
<input checked="" type="checkbox"/> Loss Rate	5	%
<input checked="" type="checkbox"/> Latency	20	milliseconds
<input checked="" type="checkbox"/> Jitter	10	milliseconds

Fail over if values for all selected measurements are exceeded.

Failback for Active Connections

Select how the Firebox handles failback for active and new connections.

Immediate: Active and new connections use the failback (original) interface

No failback: Active and new connections use the failover interface

Immediate: Active and new connections use the failback (original) interface

Gradual failback: Active connections use the failover interface; new connections use the failback interface

Metrics

Failback

SD-WAN Actions

- SD-WAN action (Policy Manager)

Interfaces

Metrics

Failback

Add SD-WAN Action

Name: Test.SDWAN.action

Description:

SD-WAN Interfaces
Select the interfaces to include in this SD-WAN action. For useful loss, latency, and jitter metrics, we recommend that you specify targets other than the default gateway. To change a target, edit the Link Monitor configuration.

Include	Interface	Targets
<input checked="" type="checkbox"/>	External-1	Ping (Default gateway)
<input checked="" type="checkbox"/>	External-2	Ping (Default gateway)

Move Up
Move Down

Metrics Settings
Select measurements and specify values that determine when failover occurs to another SD-WAN interface. Failover occurs if the value for any selected measurement is exceeded.

Loss Rate 5 %

Latency 20 ms

Jitter 10 ms

Fail over if values for all selected measurements are exceeded.

Failback for Active Connections
Select how the Firebox handles failback for active and new connections.

Immediate failback: Stop all active connections immediately. (selected)

NO failback: Stay on the failover interface even for new connections.

Immediate failback: Stop all active connections immediately.

Gradual failback: Allow active connections to use failover interface.

OK Cancel Help

SD-WAN Actions

■ SD-WAN interfaces

- Zur Messung der Interface Performance Daten sollte das *link monitor* Ziel angepasst werden
- Die *link monitor* Einstellungen befinden sich in Fireware v12.3 hier:
 - Web UI: **Network > Link Monitor**
 - Policy Manager: **Network > Configuration > Link Monitor**
- Die *link monitor* Konfiguration ermöglicht das Messen von loss, latency und jitter für ein Ziel.

TYPE	TARGET	MEASURE LOSS, LATENCY, AND JITTER
Ping	4.2.2.1	<input checked="" type="radio"/>
Ping	8.8.8.8	<input type="radio"/>

SD-WAN Actions

■ SD-WAN & BOVPN virtual interface

- Loss, latency, and jitter Messung erfolgt nur bei externen Schnittstellen
 - Diese sind nicht wirksam bei BOVPN virtual interfaces
- Eine *SD-WAN action* kann genutzt werden um die in der Policy behandelten Verbindungen in das virtual interface zu routen. Folgende Anforderung ist gegeben:
 - Failover/Failback über die *SD-WAN action* wird für BOVPN virtual interfaces nicht unterstützt.
 - *Link monitor* kann nicht für BOVPN virtual interfaces genutzt werden
 - loss, latency oder jitter kann nicht für BOVPN virtual interfaces gemessen werden

SD-WAN Actions

■ Failover

- *SD-WAN actions* unterstützen den Modus Failover (round robin, interface overflow, und routing table werden nicht unterstützt)
- Verwendung von loss, latency, oder jitter:
 - Ein Failover findet statt, wenn ein einzelner Schwellwert oder wenn alle Schwellwerte überschritten sind (konfigurationsabhängig).
- Ohne Verwendung von loss, latency oder jitter:
 - Failover bei Schnittstellenausfall
 - Schnittstellenausfall = link monitor Fehler
 - Alle Verbindungen nutzen die Failover Schnittstelle

SD-WAN Actions

■ Failback

- Der Failback findet nach einer der 3 Optionen statt:
 - **No failback** – Alle Verbindungen verbleiben auf der jetzt aktiven Schnittstelle
 - **Immediate** – Alle Verbindungen verwenden die ursprüngliche Schnittstelle
 - **Gradual** – Aktive Verbindungen nutzen die Failover Schnittstelle. Neue Verbindungen nutzen die ursprüngliche Schnittstelle.
- Default: **Immediate failback**
- Einstellungsabhängig können Failback Aktionen manuell in FSM oder Web-UI durchgeführt werden.

SD-WAN Actions

- Failback (Web UI)

SD-WAN Status

FORCE FAILBACK MANUAL GRADUAL FAILBACK MANUAL IMMEDIATE FAILBACK

ACTION	MODE	INTERFACES	FAILBACK OPTION
Global MWAN	Failover	External-1 External 2	Immediate failback
VoIP.SD-WAN.action	Failover	External 2 External-1	Gradual failback
Test.SD-WAN.action	Failover	External-1 External 2	No failback

SD-WAN Actions

- Failback (FSM)

The screenshot shows the Firebox System Manager interface for SD-WAN configuration. The main area displays a table of actions with columns for Action, Mode, Interfaces, and Failback option. A 'Force Failback' button is visible next to the VoIP.SD-WAN.action entry. The Refresh Interval is set to 5 seconds, and a Pause button is present at the bottom.

Action	Mode	Interfaces	Failback option
Global MWAN	Failover	External-1 External 2	Immediate failback
VoIP.SD-WAN.action	Failover	External 2 External-1	Gradual failback
Test.SD-WAN.action	Failover	External-1 External 2	No failback

Refresh Interval: 5 seconds

Pause

SD-WAN Actions

Eine *SD-WAN action* wird der Policy im Tab SD-WAN zugewiesen.

The screenshot shows the 'Firewall Policies / Edit' interface. The 'Name' field is set to 'SIP-ALG' and the 'Enable' checkbox is checked. The 'SD-WAN' tab is selected, and the 'SD-WAN Action' dropdown menu is open, showing options: 'None', 'None', 'VoIP.SD-WAN.action' (highlighted), and 'Create new'. The 'SAVE' and 'CANCEL' buttons are visible at the bottom.

SD-WAN Actions

■ Konfigurationsübernahme

- Migration von Fireware v12.2.1 oder früher:
 - Policy-based routing ohne failover wird in eine SD-WAN action mit einer einzelnen Schnittstelle umgewandelt
 - Policy-based routing mit failover wird in eine SD-WAN action mit mehreren Schnittstellen migriert.
- Policy Manager ermöglicht weiterhin die Konfiguration von policy-based routing (Abwärtskompatibilität zu älteren Fireware OS Versionen)

The screenshot shows a configuration window with the following elements:

- A checked checkbox labeled "Route outbound traffic using".
- A dropdown menu currently set to "Policy Based Routing" with a small downward arrow. To its right, the text "(Fireware OS v12.2.x or lower)" is displayed.
- An "Interface" label followed by a dropdown menu set to "External-1".
- A second dropdown menu with three options: "Policy Based Routing" (highlighted in blue), "SD-WAN Based Routing", and "traffic".



Link Monitor Verbesserungen

Link Monitor Verbesserungen

- *Link monitor* Einstellungen finden sich jetzt unter:
 - Web UI – **Network > Link Monitor**
 - Policy Manager – **Network > Configuration > Link Monitor**
- In der Web UI kann *link monitor* nun auch ohne *multi-WAN* genutzt werden
 - Z.B. wenn die Konfiguration nur eine externe Schnittstelle umfasst.
 - Im Policy Manager ist dies nicht möglich.

Link Monitor Verbesserungen

- Web UI

Link Monitor

LINK MONITOR	INTERFACE NAME	TARGETS
Yes	External-1	Ping (8.8.8.8) Ping (4.2.2.1)
Yes	External-2	Ping (8.8.8.8) Ping (4.2.2.1)

CONFIGURE

Link Monitor / Edit

Interface Name: External-1

Enable link monitor for this interface

Select the targets to monitor to verify the status of External-1. If you add custom targets, the default gateway target is replaced. Otherwise, the default gateway target is used.

TYPE	TARGET	MEASURE LOSS, LATENCY, AND JITTER
Ping	8.8.8.8	<input type="radio"/>
Ping	4.2.2.1	<input type="radio"/>

ADD EDIT REMOVE

Require a successful probe to all targets to define the interface as active.

Probe interval seconds

Deactivate after consecutive failures

Reactivate after consecutive successes

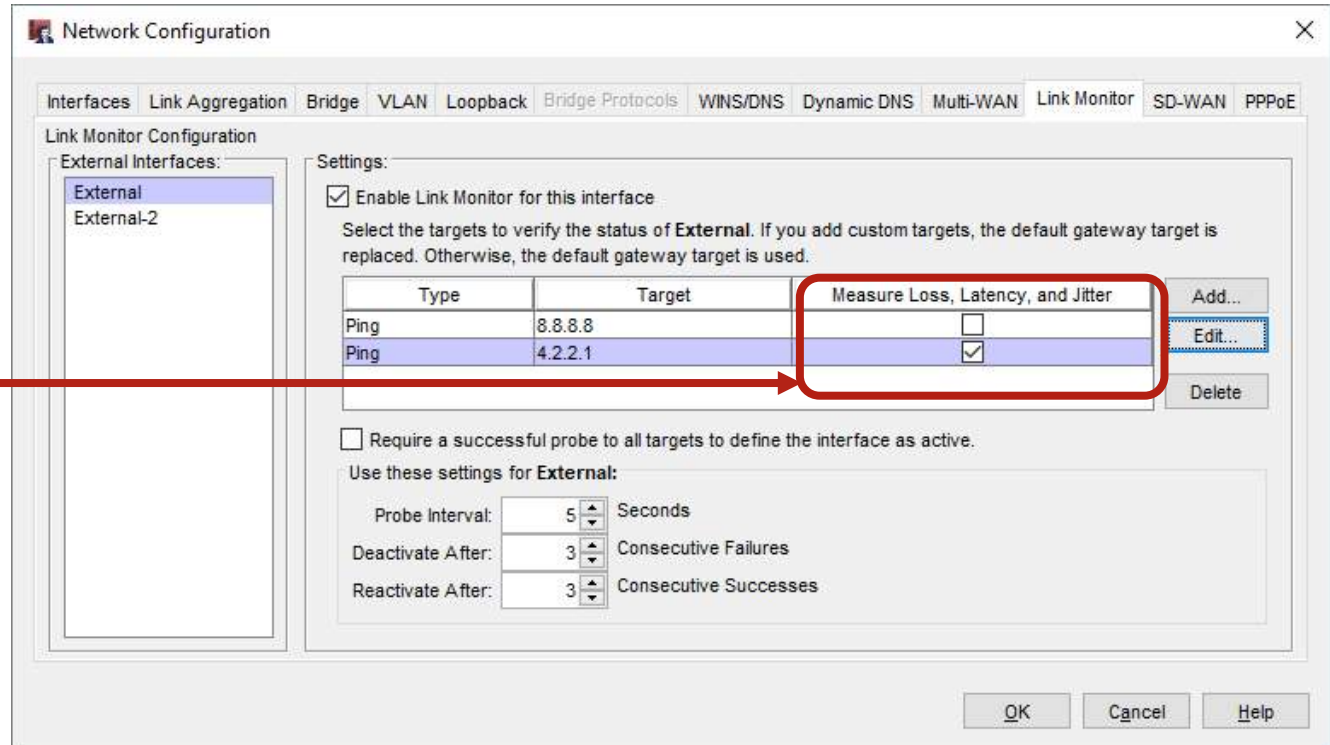
Select to measure loss, latency, and jitter for one target



Link Monitor Verbesserungen

- Policy Manager

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



Link Monitor Verbesserungen

- Wird *link monitor* aktiviert ist zunächst das Default Gateway der Schnittstelle das Ziel
 - Für belastbare Daten ist eine Veränderung auf ein anderes Ziel empfohlen.
 - Wird ein neues Ziel hinzugefügt ersetzt es das Default Gateway als Ziel
 - Werden alle eigenen Ziele entfernt, wird das Default Gateway erneut hinzugefügt

Link Monitor Verbesserungen

TYPE	TARGET	MEASURE LOSS, LATENCY, AND JITTER
Ping	Default gateway	<input checked="" type="radio"/>

ADD EDIT REMOVE

Add Link Monitor Target ×

Type

Target

OK CANCEL

TYPE	TARGET	MEASURE LOSS, LATENCY, AND JITTER
Ping	4.2.2.1	<input checked="" type="radio"/>

ADD EDIT REMOVE

Link Monitor Verbesserungen

- DNS Ziele werden mit Version 12.3 unterstützt

Add Link Monitor Target ×

Type

Target

Query domain

TYPE	TARGET	MEASURE LOSS, LATENCY, AND JITTER
Ping	8.8.8.8	<input checked="" type="radio"/>
Ping	4.2.2.1	<input type="radio"/>
DNS	host.example.com@192.0.2.2	<input type="radio"/>

Link Monitor Verbesserungen

- Bis zu 3 *link monitor* Ziele können verwendet werden.

TYPE	TARGET	MEASURE LOSS, LATENCY, AND JITTER
Ping	8.8.8.8	<input checked="" type="radio"/>
TCP	198.51.100.2:80	<input type="radio"/>
DNS	host.example.com@192.0.2.2	<input type="radio"/>



Live Demo



Danke