



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.



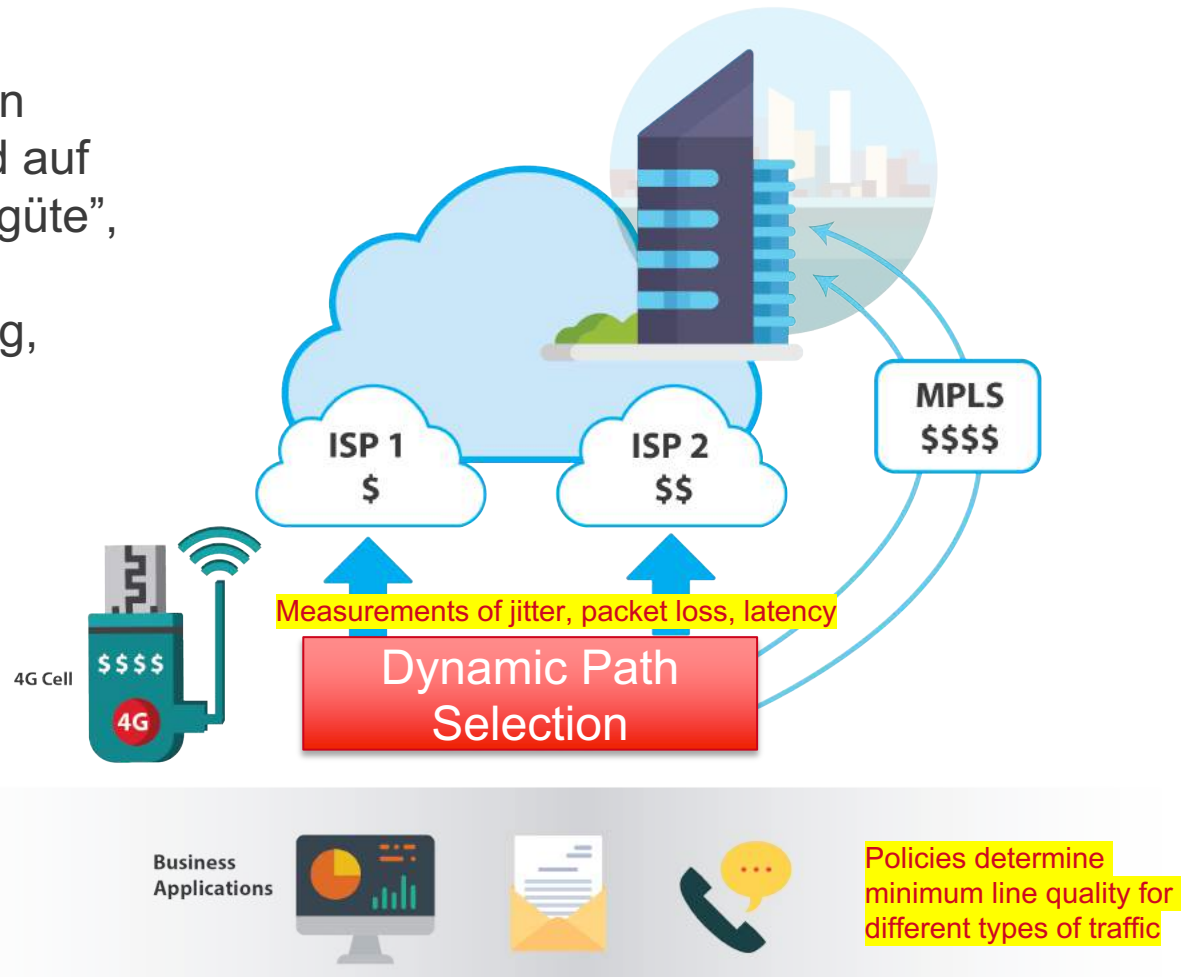
Automatische Leitungswahl für beste Performance.

SD-WAN ist die “Echtzeit Navigation” für Netzwerke



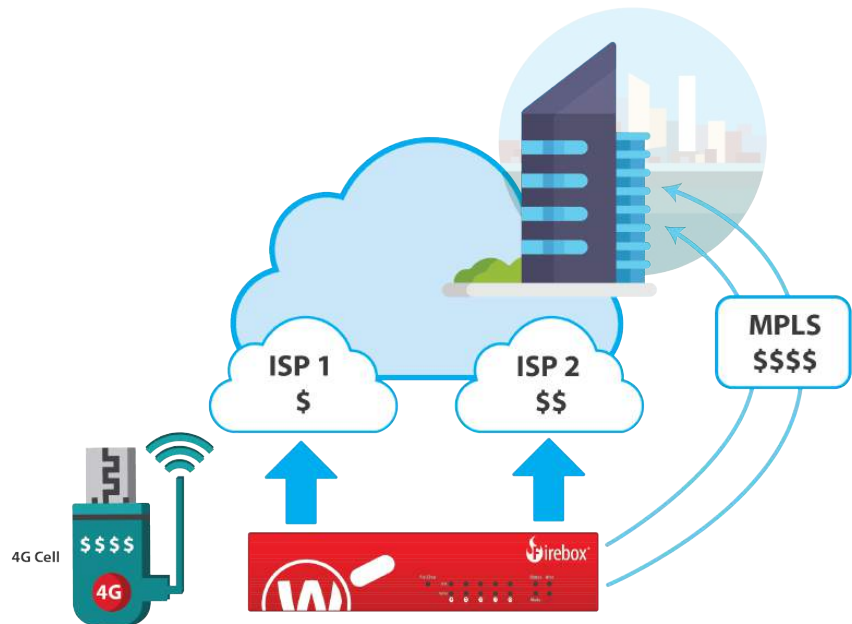
Dynamic Path Selection basierend auf aktuellem Zustand

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)

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
☒ Loss Rate	5 %
☒ Latency	20 milliseconds
☒ 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
☒	External-1	Ping (Default gateway)
☒	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. v

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 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

Network Configuration

Interfaces | Link Aggregation | Bridge | VLAN | Loopback | Bridge Protocols | WINS/DNS | Dynamic DNS | Multi-WAN | **Link Monitor** | SD-WAN | PPPoE

Link Monitor Configuration

External Interfaces:

- External
- External-2

Settings:

☒ Enable Link Monitor for this interface

Select the targets to verify the status of **External**. 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	☐
Ping	4.2.2.1	☒

Add... Edit... Delete

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

Use these settings for **External**:

Probe Interval: 5 Seconds

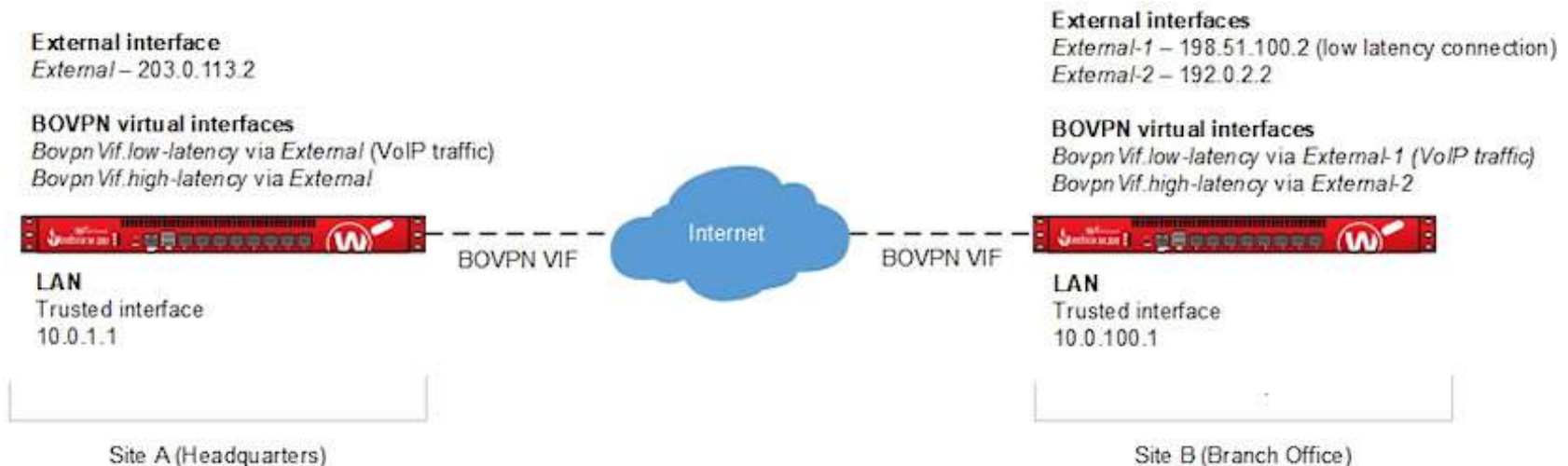
Deactivate After: 3 Consecutive Failures

Reactivate After: 3 Consecutive Successes

OK Cancel Help

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“

BOVPN Virtual Interfaces / Edit

Click the lock to prevent further changes

Interface Name:

Device Name:

Remote Endpoint Type:

Gateway Address Family:

Gateway Settings | **VPN Routes** | Phase 1 Settings | Phase 2 Settings | Multicast Settings

VPN Routes

Specify the routes that will use this VPN virtual interface

ROUTE TO ↑	METRIC
ADD EDIT REMOVE	

Interface

☒ Assign virtual interface IP addresses (required for dynamic routing)

Local IP address:

Peer IP address or netmask:

Use a netmask for a VPN to a third-party endpoint.

BOVPN Virtual Interfaces / Edit

Click the lock to prevent further changes

Interface Name:

Device Name:

Remote Endpoint Type:

Gateway Address Family:

Gateway Settings | **VPN Routes** | Phase 1 Settings | Phase 2 Settings | Multicast Settings

VPN Routes

Specify the routes that will use this VPN virtual interface

ROUTE TO ↑	METRIC
ADD EDIT REMOVE	

Interface

☒ Assign virtual interface IP addresses (required for dynamic routing)

Local IP address:

Peer IP address or netmask:

Use a netmask for a VPN to a third-party endpoint.

Link Monitor

- Link Monitor für beide VPN Tunnel aktivieren

Link Monitor / Edit

 Click the lock to prevent further changes

Interface Name: BvpnVif.t70jsp

To verify the status of the interface, the virtual IP address of the peer is monitored with ping probes. To change the virtual IP address, edit the BOVPN virtual interface configuration.

TYPE	TARGET	MEASURE LOSS, LATENCY, AND JITTER
Ping	Peer IP address	

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

SAVE

CANCEL

SD-WAN Actions

SD-WAN / Edit



Click the lock to prevent further changes

SD-WAN Action Settings

Name VPN-Line2-Prio

Description 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 target. To change a target, edit the [Link Monitor](#) configuration.

INTERFACE NAME	TARGETS
BovpnVif.T70JSP-Backup	Ping (Peer IP address)
BovpnVif.t70jsp	Ping (Peer IP address)

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
☒ Loss Rate	5 %
☒ Latency	20 milliseconds
☒ Jitter	10 milliseconds

Firewall-Policies

- Zuweisung der jeweiligen SD-WAN Action in den Policies

Firewall Policies / Edit



Click the lock to prevent further changes

Name

Firewall Policies / Edit



Click the lock to prevent further changes

Name WG-Fireware-XTM-WebUI_Azure-SDW ☒ Enable

Settings

SD-WAN

Settings SD-WAN Application Control Geolocation Traffic Management Scheduling Advanced

SD-WAN Action

VPN-Line2-Prio

SD-WAN Action Settings

Name VPN-Line2-Prio

Description 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 target. To change a target, edit the [Link Monitor](#) configuration.

INTERFACE NAME	TARGETS
BovpnVif.T70JSP-Backup	Ping (Peer IP address)
BovpnVif.t70jsp	Ping (Peer IP address)
ADD REMOVE MOVE UP MOVE DOWN	

FROM

192.168.130.10

[ADD](#)

[REMOVE](#)

[ADD](#)

[REMOVE](#)

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.

Firewall Policies / Edit

 Click the lock to prevent further changes

Name ☒ Enable

Settings SD-WAN Application Control Geolocation Traffic Management Scheduling Advanced

Connections are

Policy Type **Ping**

PORT	PROTOCOL
	ICMP (type: 8, code: 255)

FROM

 172.16.85.0/24

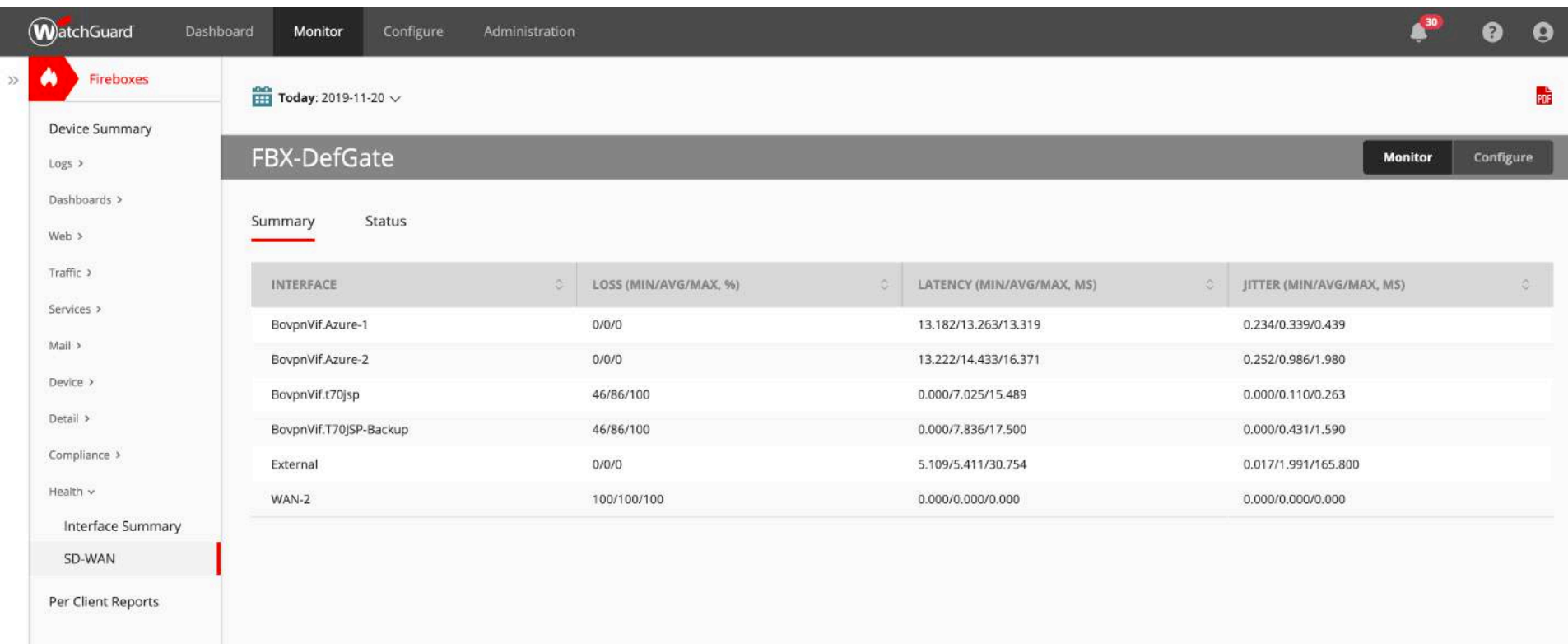
TO

 172.16.85.0/24

ADD REMOVE **ADD REMOVE**

Kontrolle der SD-WAN Nutzung

- WatchGuard Cloud stellt den SD-WAN Status langfristig dar



WatchGuard Dashboard Monitor Configure Administration

Fireboxes

Today: 2019-11-20

FBX-DefGate Monitor Configure

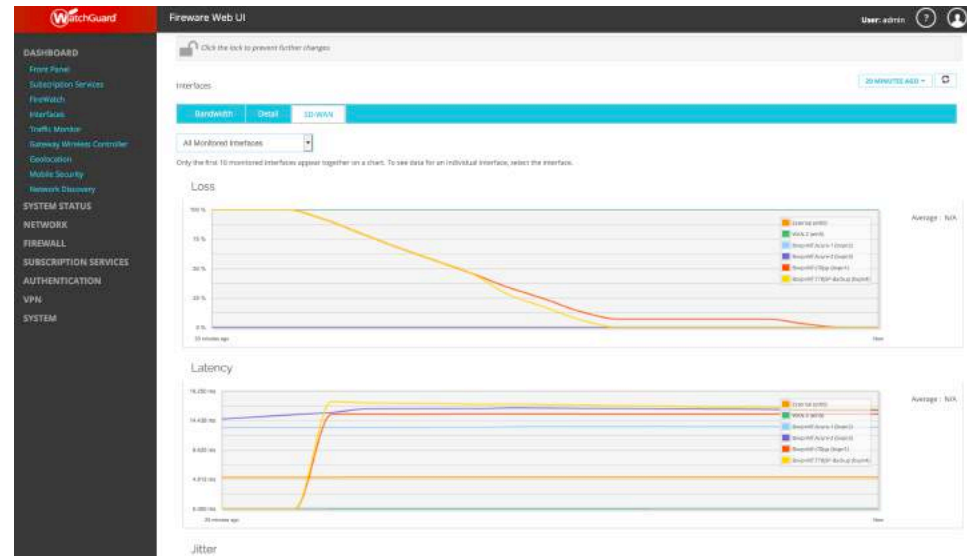
Summary Status

INTERFACE	LOSS (MIN/AVG/MAX, %)	LATENCY (MIN/AVG/MAX, MS)	JITTER (MIN/AVG/MAX, MS)
BvvpnVif.Azure-1	0/0/0	13.182/13.263/13.319	0.234/0.339/0.439
BvvpnVif.Azure-2	0/0/0	13.222/14.433/16.371	0.252/0.986/1.980
BvvpnVif.t70jsp	46/86/100	0.000/7.025/15.489	0.000/0.110/0.263
BvvpnVif.t70JSP-Backup	46/86/100	0.000/7.836/17.500	0.000/0.431/1.590
External	0/0/0	5.109/5.411/30.754	0.017/1.991/165.800
WAN-2	100/100/100	0.000/0.000/0.000	0.000/0.000/0.000

Interface Summary
SD-WAN
Per Client Reports

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

SD-WAN Status

Click the lock to prevent further changes

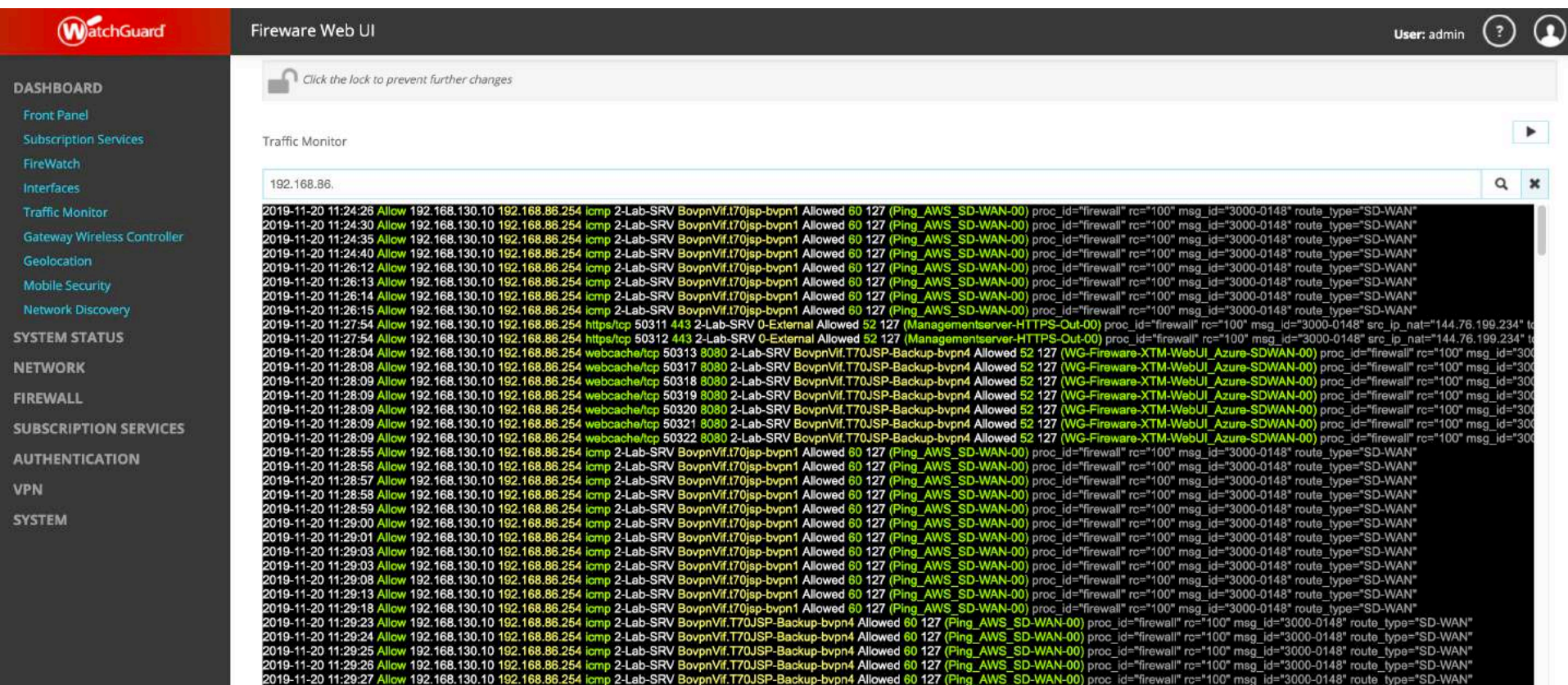
SD-WAN Status

FORCE FAILBACK | MANUAL GRADUAL FAILBACK | MANUAL IMMEDIATE FAILBACK

ACTION	MODE	INTERFACES	FAILBACK OPTION
Global MWAN	Fallover	External WAN-2	Immediate failback
Test-SDWAN	Fallover	External WAN-2	Immediate failback
VPN_Line1-Prio	Fallover	BovpnVif.t70jsp BovpnVif.T70JSP-Backup	Immediate failback
VPN-Line2-Prio	Fallover	BovpnVif.T70JSP-Backup BovpnVif.t70jsp	Immediate failback

Kontrolle der SD-WAN Nutzung

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



The screenshot displays the WatchGuard Fireware Web UI interface. The left sidebar contains navigation menus for DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, and SYSTEM. The main content area is titled 'Traffic Monitor' and shows a list of network events. The top of the interface includes the WatchGuard logo, 'Fireware Web UI', a user login 'User: admin', and a lock icon with the text 'Click the lock to prevent further changes'.

The Traffic Monitor table lists events with columns for time, action, source IP, destination IP, port, protocol, and details. The details column shows the specific interface used for each event.

Time	Action	Source IP	Destination IP	Port	Protocol	Details
2019-11-20 11:24:26	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:24:30	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:24:35	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:24:40	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:26:12	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:26:13	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:26:14	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:26:15	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:27:54	Allow	192.168.130.10	192.168.86.254	50311	https/tcp	50311 443 2-Lab-SRV 0-External Allowed 52 127 (Managementserver-HTTPS-Out-00) proc_id="firewall" rc="100" msg_id="3000-0148" src_ip_nat="144.76.199.234" to
2019-11-20 11:28:04	Allow	192.168.130.10	192.168.86.254	50313	webcache/tcp	50313 8080 2-Lab-SRV BvovpnVif.T70JSP-Backup-bvovpn4 Allowed 52 127 (WG-Fireware-XTM-WebUI_Azure-SDWAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:28:08	Allow	192.168.130.10	192.168.86.254	50317	webcache/tcp	50317 8080 2-Lab-SRV BvovpnVif.T70JSP-Backup-bvovpn4 Allowed 52 127 (WG-Fireware-XTM-WebUI_Azure-SDWAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:28:09	Allow	192.168.130.10	192.168.86.254	50318	webcache/tcp	50318 8080 2-Lab-SRV BvovpnVif.T70JSP-Backup-bvovpn4 Allowed 52 127 (WG-Fireware-XTM-WebUI_Azure-SDWAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:28:09	Allow	192.168.130.10	192.168.86.254	50319	webcache/tcp	50319 8080 2-Lab-SRV BvovpnVif.T70JSP-Backup-bvovpn4 Allowed 52 127 (WG-Fireware-XTM-WebUI_Azure-SDWAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:28:09	Allow	192.168.130.10	192.168.86.254	50320	webcache/tcp	50320 8080 2-Lab-SRV BvovpnVif.T70JSP-Backup-bvovpn4 Allowed 52 127 (WG-Fireware-XTM-WebUI_Azure-SDWAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:28:09	Allow	192.168.130.10	192.168.86.254	50321	webcache/tcp	50321 8080 2-Lab-SRV BvovpnVif.T70JSP-Backup-bvovpn4 Allowed 52 127 (WG-Fireware-XTM-WebUI_Azure-SDWAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:28:55	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:28:58	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:28:59	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:29:00	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:29:01	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:29:03	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:29:03	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:29:08	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:29:13	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:29:18	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:29:23	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:29:24	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:29:25	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:29:26	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"
2019-11-20 11:29:27	Allow	192.168.130.10	192.168.86.254	80	icmp	2-Lab-SRV BvovpnVif.T70JSP-Bvovpn1 Allowed 60 127 (Ping_AWS_SD-WAN-00) proc_id="firewall" rc="100" msg_id="3000-0148" route_type="SD-WAN"

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

BOVPN Virtual Interfaces

 Click the lock to prevent further changes

NAME ↕	EDITABLE	GATEWAY ADDRESS FAMILY
BovpnVif.t70jsp	Yes	IPv4
BovpnVif.Azure-1	Yes	IPv4
BovpnVif.Azure-2	Yes	IPv4
BovpnVif.T70JSP-Backup	Yes	IPv4

[ADD](#) [EDIT](#) [REMOVE](#) [ENABLE](#) [DISABLE](#) [REPORT](#)



Live Demo



Vielen Dank!



***NOTHING GETS
PAST **RED.*****

