



Redundante VPN-Anbindung

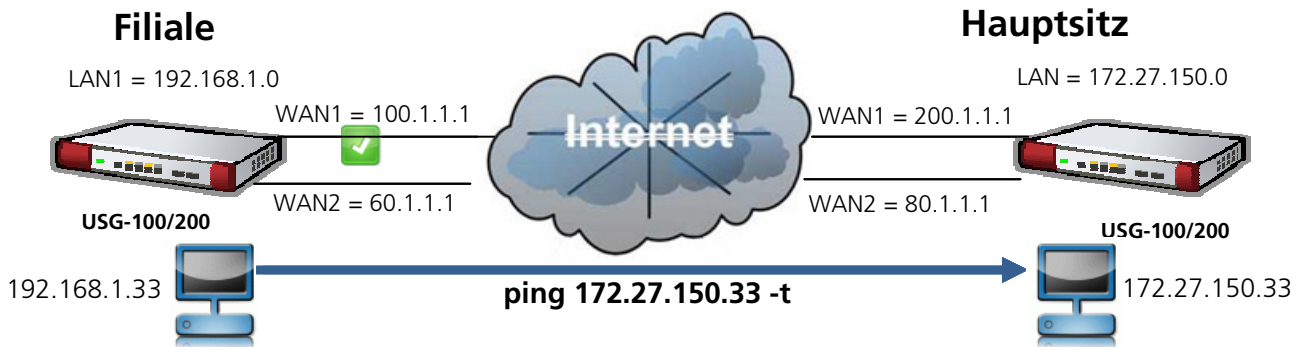
**Konfigurationsbeispiel
ZyXEL ZyWALL USG Serie**

März 2010 / ATA / HAL

AUFBAU

Eine Firma möchte Ihren Hauptsitz mit sämtlichen Nebenstellen über zwei VPN-Leitungen verbinden. Mehrere Wegvarianten sollen die Verbindung permanent sicher stellen.

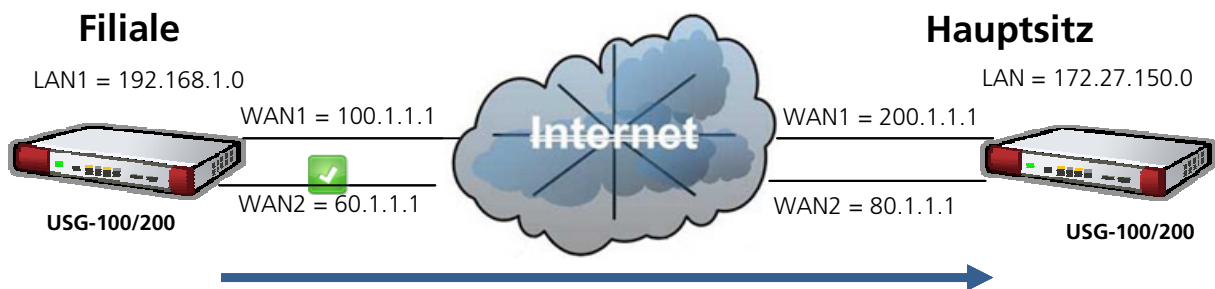
VPN via WAN1



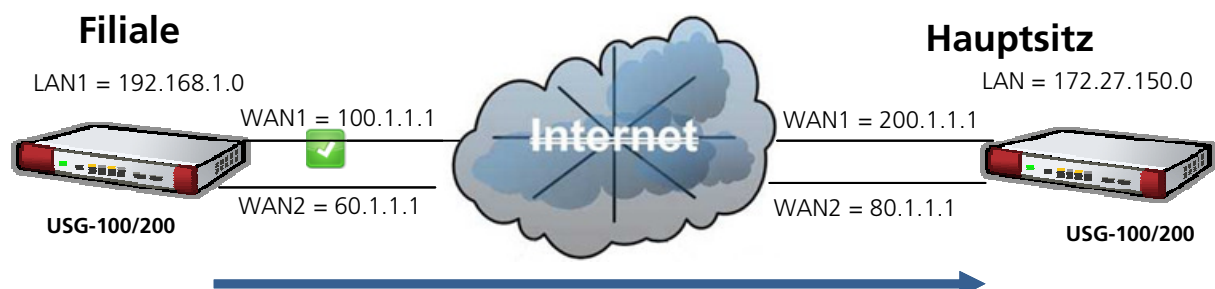
WAN1 Unterbruch



VPN Backup via WAN2



WAN1 übernimmt (nach 60 Sek.) wenn Interface ist wieder UP



VPN-KONFIGURATION IN DER FILIALE

VPN Phase 1 konfigurieren: [configuration](#) > [VPN](#) > [IPSec VPN](#)

VPN Connection **VPN Gateway** Concentrator

Add VPN Gateway

Show Advanced Settings

General Settings

Enable

VPN Gateway Name:

Gateway Settings

My Address

Interface Static -- 0.0.0.0/0.0.0.0

Domain Name / IP

Peer Gateway Address

Static Address

Primary

Secondary

Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: (60-86400 seconds)

Dynamic Address

Authentication

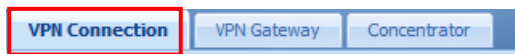
Pre-Shared Key

Certificate (See My Certificates)

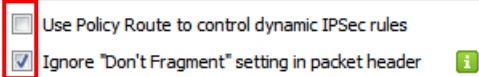
Die Konfiguration der ersten Phase mit **OK** abschliessen. Sie wird in der Liste sichtbar.

4		Filiale	wan1	200.1.1.1, 80.1.1.1	Filiale_Hauptsitz_Netz
---	--	---------	------	---------------------	------------------------

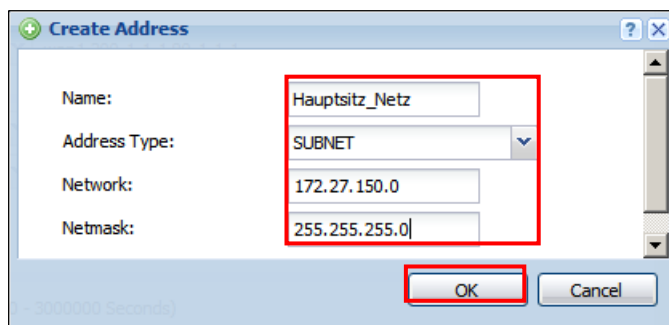
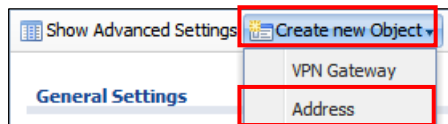
Phase 2 konfigurieren



Global Setting



Der nachfolgende Schritt [Create new Object](#) wird weggelassen, falls die Gegenstelle vorgängig bereits erfasst wurde.



Show Advanced Settings Create new Object ▾

Nailed-Up
 Enable Replay Detection
 Enable NetBIOS broadcast over IPSec

General Settings

Enable

Connection Name:

VPN Gateway

Application Scenario

Site-to-site

Site-to-site with Dynamic Peer

Remote Access (Server Role)

Remote Access (Client Role)

VPN Gateway: wan1 200.1.1.1 80.1.1.1

Policy

Local policy: INTERFACE SUBNET, 192.168.1.0/24

Remote policy: SUBNET, 172.27.150.0/24

Phase 2 Settings

SA Life Time: (180 - 3000000 Seconds)

Related Settings

Add this VPN connection to IPSec_VPN zone.

Connectivity Check

Enable Connectivity Check ⓘ

Check Method:

Check Period: (5-30 Seconds)

Check Timeout: (1-10 Seconds)

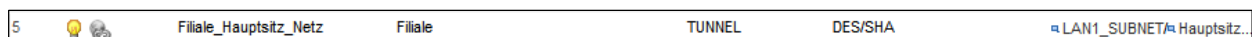
Check Fail Tolerance: (1-10)

Check This Address Domain Name or IP Address

Check the First and Last IP Address in the Remote Policy

Log

Nach Abschluss der zweiten Phase wird die komplette VPN-Regel in der Liste sichtbar.



Die VPN-Konfiguration in der Filiale ist abgeschlossen.

Konfiguration der VPN Regel im Hauptsitz

VPN-Phase 1 konfigurieren

Konfiguration > VPN > IPSec VPN



Add VPN Gateway ? X

Show Advanced Settings

General Settings

Enable

VPN Gateway Name:

Gateway Settings

My Address

Interface Static -- 0.0.0.0/0.0.0.0

Domain Name / IP

Peer Gateway Address

Static Address

Primary

Secondary

Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: (60-86400 seconds)

Dynamic Address

Authentication

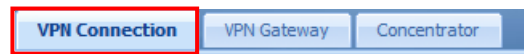
Pre-Shared Key

Certificate (See My Certificates)

Die Konfiguration der ersten Phase mit **OK** abschliessen. Sie wird in der Liste sichtbar.

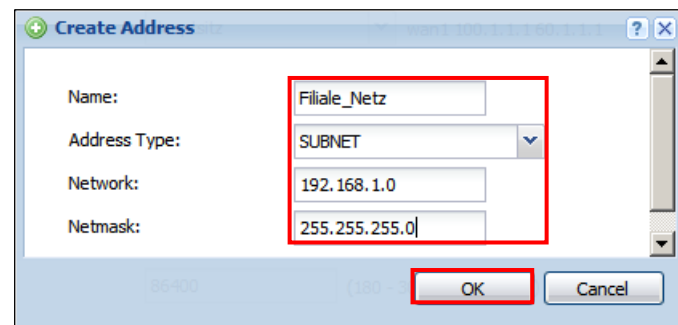
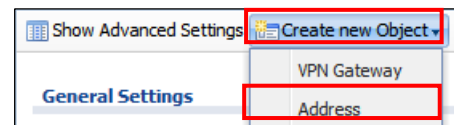
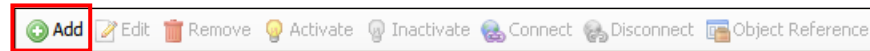
4	Hauptsitz	wan1	100.1.1.1, 60.1.1.1	Filiale_Hauptsitz_Netz
---	-----------	------	---------------------	------------------------

Phase 2 konfigurieren



Global Setting

- Use Policy Route to control dynamic IPSec rules
- Ignore "Don't Fragment" setting in packet header i



Nailed-Up
 Enable Replay Detection
 Enable NetBIOS broadcast over IPSec

Show Advanced Settings Create new Object ▾

General Settings

Enable

Connection Name:

VPN Gateway

Application Scenario

Site-to-site

Site-to-site with Dynamic Peer

Remote Access (Server Role)

Remote Access (Client Role)

VPN Gateway: wan1 100.1.1.1 60.1.1.1

Policy

Local policy: SUBNET, 172.27.150.0/24

Remote policy: SUBNET, 192.168.1.0/24

Phase 2 Settings

SA Life Time: (180 - 3000000 Seconds)

Related Settings

Add this VPN connection to IPSec_VPN zone.

Connectivity Check

Enable Connectivity Check ⓘ

Check Method:

Check Period: (5-30 Seconds)

Check Timeout: (1-10 Seconds)

Check Fail Tolerance: (1-10)

Check This Address Domain Name or IP Address

Check the First and Last IP Address in the Remote Policy

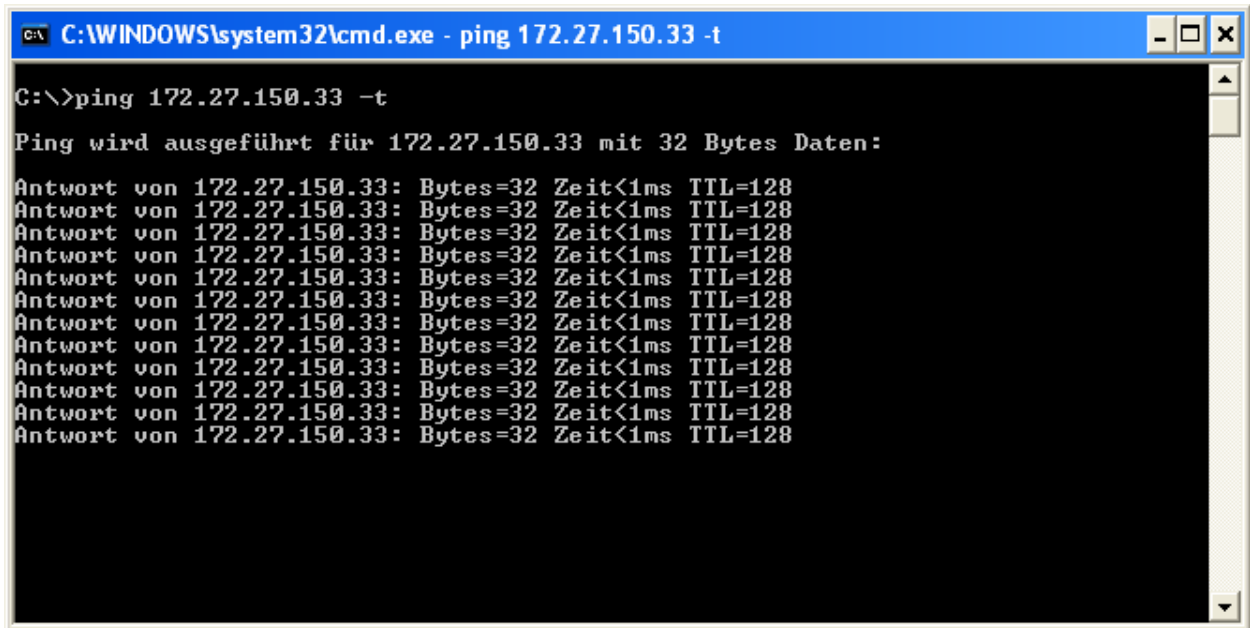
Log

5
🔧
Hauptsitz_Filiale_Netz
Hauptsitz
TUNNEL
DES/SHA
LAN1_SUBNET Filiale_Netz

DURCHFÜHRUNG UND TESTS

Ein hilfreicher Befehl im DOS-Fenster ist Ping.

Start > Ausführen > CMD



```
C:\WINDOWS\system32\cmd.exe - ping 172.27.150.33 -t

C:\>ping 172.27.150.33 -t

Ping wird ausgeführt für 172.27.150.33 mit 32 Bytes Daten:

Antwort von 172.27.150.33: Bytes=32 Zeit<1ms TTL=128
Antwort von 172.27.150.33: Bytes=32 Zeit<1ms TTL=128
Antwort von 172.27.150.33: Bytes=32 Zeit<1ms TTL=128
Antwort von 172.27.150.33: Bytes=32 Zeit<1ms TTL=128
Antwort von 172.27.150.33: Bytes=32 Zeit<1ms TTL=128
Antwort von 172.27.150.33: Bytes=32 Zeit<1ms TTL=128
Antwort von 172.27.150.33: Bytes=32 Zeit<1ms TTL=128
Antwort von 172.27.150.33: Bytes=32 Zeit<1ms TTL=128
Antwort von 172.27.150.33: Bytes=32 Zeit<1ms TTL=128
Antwort von 172.27.150.33: Bytes=32 Zeit<1ms TTL=128
Antwort von 172.27.150.33: Bytes=32 Zeit<1ms TTL=128
Antwort von 172.27.150.33: Bytes=32 Zeit<1ms TTL=128
```