

Cisco, Mikrotik, pfSense VPN site networking with dynamic routing

INSTRUCTIONS

NETWORKS

LAN, WAN, WIRELESS



aqui (level 5)

2019-01-21, updated on 2022-04-04

👁 15804

💬 5

❤ 10

table of contents

General introduction

GRE test environment

Cisco Router Setup (GRE)

Mikrotik RouterOS Setup

default configuration

Interface and IP address configuration

Set IPsec key parameters

Enable dynamic routing with RIPv2 protocol

Is that really safe? Trust is good, control is better !

Advanced site configuration with multiple local LANs or VLANs

Use virtual tunnel interfaces VTI instead of GRE tunnel

VTI test environment

Cisco router setup with VTI and OSPF

pfSense setup with VTI and OSPF

OSPF routing protocol pfSense

OSPF function and routing check

Related Links

General introduction

The following tutorial is a continuation of the existing VPN tutorials here at *Administrator.de* . It describes a heterogeneous VPN site network based on IPsec between Cisco routers and Mikrotik routers. It thus covers a scenario in which a powerful VPN router (Cisco) is used in the head office, but inexpensive Mikrotik routers are used in the external locations, for example for budget reasons.

The highlight of this design is a securely encrypted VPN connection (IPsec in transport mode) over which a GRE tunnel connection is placed.

The use of separate GRE tunnels or tunnel interfaces compared to direct IPsec in tunneling

mode enables the use of dynamic routing protocols such as RIPv2 or OSPF.

The complete elimination of the manual configuration of static routes when using a dynamic routing protocol results in a considerable simplification and error security in routing.

With a large number of branch offices, this makes the installation and management of these remote networks considerably easier.

Furthermore, simple automatic line backup scenarios can be implemented without any manual intervention, for example to secure separate branch offices via a second line or direct backup to another branch office.

Especially in VPN site designs with increased requirements such as remote VoIP telephony, etc., automatic backup and dynamic rerouting result in significantly greater operational security.

Likewise, multicast routing (audio and video streaming) with PIM can be routed to all locations via such a tunnel VPN design.

The aim is to quickly arrive at a functioning and reliable solution for private or company VPNs in the small and medium-sized environment for site networks without much trial and error.

The examples and screenshots presented here can be transferred directly to existing projects, with appropriate adjustment of the IP addressing to your own needs.

The examples can also be used to implement such VPN designs in pure Cisco or pure Mikrotik environments, since the basic configuration steps are identical. The choice of dynamic routing protocol is also free. Those who prefer OSPF can of course use this instead of the RIPv2 presented here. RIPv2 was chosen here because of its ease of configuration. In addition, RIPv2 is often a basic feature component of simple Layer 3 (routing) switches and dedicated routers.

In the links at the end of the tutorial you will find additional information on the topics of VPN and routing.

The configuration is simple and can also be implemented by laypeople. A little basic knowledge about IPsec VPNs in general and Cisco Command Line Interface or Mikrotiks graphical WinBox Config can, as always, do no harm and helps with understanding!

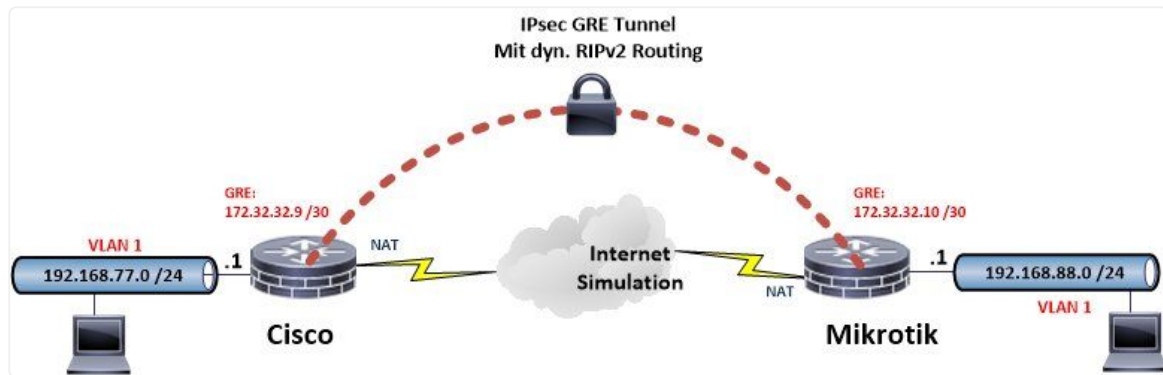
GRE test environment

The Internet is simulated here by separate IP networks of 10 with DHCP address assignment. All VPN routers work with their WAN / Internet port via NAT (Network Address Translation) and an active firewall with each other on this IP network. So just like on the Internet or via the provider under real conditions.

The VPN encryption only uses the current and currently secure AES in a 256-bit variant.

Your own IP addressing and, if necessary, WAN port configs such as xDSL must be adjusted accordingly.

The VPN design looks like this:



The first step of this design deals with the basic configuration of both components. The IP addressing here in the tutorial:

Internet address Cisco = 10.99.1.198

Internet address Mikrotik = 10.1.1.150

GRE tunnel network = 172.31.31.8/30 (Cisco=172.31.31.9, Mikrotik=172.31.31.10)

Local LANs according to the above figure.

The tunnel network is a point-to-point network. This is why /30 networks (30 prefix = 255.255.255.252 subnet mask) with 2 usable host addresses are always used here.

In the second step of the tutorial, a second Mikrotik location is integrated and the Cisco and Mikrotik pages are expanded with additional local VLAN IP networks to show a more realistic setup. More on that later...

Let's go....

Cisco Router Setup (GRE)

The tutorial deliberately does not go into detail about a standard internet setup, which would go beyond the scope of this tutorial. For reasons of clarity, this is assumed or can simply be taken over from the [Cisco Basics Tutorial](#) here. It applies to all Cisco IOS based models. Only the VPN and GRE tunnel configuration in connection with a zone-based firewall are described here, which are necessary for the configuration.

(All config parameters marked in **red** here relate to the extended design in *Chapter 6* for multiple locations and additional local (V)LANs. **These additional local LAN networks can of course** be left out in a simple design with 2 locations and a single local LAN each as shown in the drawing above .

Comments on the Cisco configuration in *black*.) ! hostname cisco_router ! aaa new model ! aaa authentication login default local aaa authorization network default local ! clock timezone CET 1 0 ==> set time to Europe / summer time clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00 ! ip dhcp binding cleanup interval 30

ip dhcp excluded-address 192.168.77.1 192.168.77.100 ==> DHCP IP address pool .101 to .149
ip dhcp excluded-address 192.168.77.150 192.168.77.254 ! ip dhcp pool LAN ==> DHCP server for
local LAN network 192.168.77.0 255.255.255.0 dns-server 192.168.7.254 domain-name
cisco.home.arpa default-router 192.168.77.1 ! ip domain lookup source-interface Ethernet1 ip
domain name cisco.home.arpa ip name-server <DNS IP address> ip inspect log drop-pkt ==>
Logging of the packets blocked by the firewall ! class-map type inspect match-any internet-
allowed

==> Specifying the packets allowed by the Internet through the firewall description Allow access
from the Internet match access-group name WAN_IN class-map type inspect match-any lan-
allowed ==> Specifying the packets allowed by the LAN through the firewall description Local
LAN protocols allow internet match protocol dns match protocol http match protocol https
match protocol imap match protocol smtp extended match protocol sip-tls match protocol
rtsp match protocol ssh match protocol ntp match protocol tcp match protocol udp match
protocol icmp !

policy-map type inspect lan-allowed-policy ==> *Firewall Policy Local LAN to Internet* description
LAN to Internet Policy class type inspect lan-allowed inspect class class-default drop policy-
map type inspect internet-allowed-policy ==> *Firewall Policy Internet to Router* description
Internet to Router Policy class type inspect internet-allowed pass class class-default drop !
zone security lan zone security wan zone-pair security lan-wan source lan destination wan
description Firewall LAN-Internet service-policy type inspect lan-allowed-policy

zone-pair security wan-self source wan destination self
description firewall internet router
service-policy type inspect internet-allowed-policy
!

crypto keyring MTPVN
pre-shared-key address 10.1.1.150 key test123 pre-shared-key address 10.99.1.149 key
secret123 ==> *Second VPN router (see: chapter 6)* ! crypto isakmp policy 10 ==> *Set IPsec key*
parameters encr aes 256 hash sha256 authentication pre-share group 14 ! crypto isakmp
profile Mikrotik-1 ==> *connection parameters Mikrotik-1* description IPsec Mikrotik-1 keyring
MTPVN

match identity address 10.99.1.149 255.255.255.255 crypto isakmp profile Mikrotik-2 ==>
connection parameters Mikrotik-2 (See: Chapter 6) description IPsec Mikrotik-2 keyring MTVPN
match identity address 10.1.1.150 255.255.255.255 ! crypto ipsec transform-set mikrotik esp-
aes 256 esp-sha256-hmac mode **transport** ==> Transport mode since tunnel realized by GRE!!
crypto map mikrotik 10 ipsec-isakmp ==> Router Mikrotik-2 (See: Chapter 6) description IPsec
Mikrotik-2 set peer 10.1.1.150 set transform-set mikrotik set isakmp-profile Mikrotik-2 match
address 107

==> Everything this ACL defines is IPsec encrypted crypto map mikrotik 15 ipsec-isakmp
description IPsec Mikrotik-1 set peer 10.99.1.149 set transform-set mikrotik set isakmp-profile
Mikrotik-1 match address 108 ! interface Tunnel0 ==> GRE Tunnel Interface description GRE to
Mikrotik-2 ip address 172.31.31.9 255.255.255.252 ip mtu 1400 zone-member security lan
tunnel source 10.99.1.198 tunnel destination 10.1.1.150 tunnel path-mtu-discovery ! interface
Tunnel1 description GRE to Mikrotik-1 ip address 172.31.31.1 255.255.255.252 ip mtu 1400

```
zone-member security lan
tunnel source 10.99.1.198
tunnel destination 10.99.1.149
tunnel path-mtu-discovery ! interface Vlan1 description Local LAN ip address 192.168.77.1
255.255.255.0 ip nat inside ip virtual-reassembly in zone-member security lan ! interface
Vlan10 description Local VLAN-10 ip address 192.168.177.1 255.255.255.0 ip nat inside ip
virtual-reassembly in zone-member security lan ! interface Ethernet 1 description Internet /
WAN connection ip address 10.99.1.198 255.255.255.0 no ip redirects
```

```
no ip unreachable
ip nat outside
zone-member security wan
crypto map mikrotik
!
router rip ==> Dynamic RIP routing with version 2 ! activate version 2 passive-interface default
```

no passive-interface Tunnel0 no passive-interface Tunnel1 network 172.31.0.0 ==> specify networks in classic notation A,B,C network 192.168.77.0 network 192.168.177.0 no auto-summary ==> IMPORTANT ! Activates CIDR masks ! ip route 0.0.0.0 0.0.0.0 10.99.1.254 ==> Default Route Internet ! ip dns server

==> Cisco is DNS Proxy here. (Not applicable with local DNS server!) ip nat inside source list 101 interface Ethernet 1 overload ! ip access-list extended WAN_IN permit icmp any any echo-reply permit icmp any any packet-too-big permit icmp any any time-exceeded permit udp any eq bootps any permit udp any any eq isakmp permit udp any any eq non500-isakmp permit esp any any permit gre any any permit udp any eq domain any permit tcp any eq domain any permit udp any eq ntp any ! access-list 101 deny ip 192.168.77.0 0.0.0.255 172.16.0.0 0.15.255.255

==> VPN traffic in local private IP networks excluded from NAT (tunnel) access-list 101 deny ip 192.168.77.0 0.0.0.255 192.168.0.0 0.0.255.255 access-list 101 deny ip 192.168.177.0 0.0.0.255 172.16.0.0 0.0.16.0.0 0.0.0.255 172.16.0.0 0.0.16.0.0 .255.255 ==> VLAN-10 VPN Traffic dto. excluded from NAT (Tunnel) access-list 101 deny ip 192.168.177.0 0.0.0.255 192.168.0.0 0.0.255.255 access-list 101 permit ip 192.168.77.0 0.0.0.255 any everything others via NAT to the Internet access-list 101 permit ip 192.168.177.0 0.0.0.255 any Dto. for VLAN-10 access-list 107 permit gre host 10.99.1.198 host 10.1.1.150 ==> GRE Traffic (IP 47) encrypted to Mikrotik-2 IPsec ##

`access-list 108 permit gre host 10.99.1.198 host 10.99.1.149 ==> GRE traffic (IP 47) encrypted to Mikrotik-1 IPsec ## ! ntp server ntps1-0.cs.tu-berlin.de source Ethernet 1 ==> Set router time via NTP (reference TU Berlin) ! end`

Mikrotik RouterOS Setup

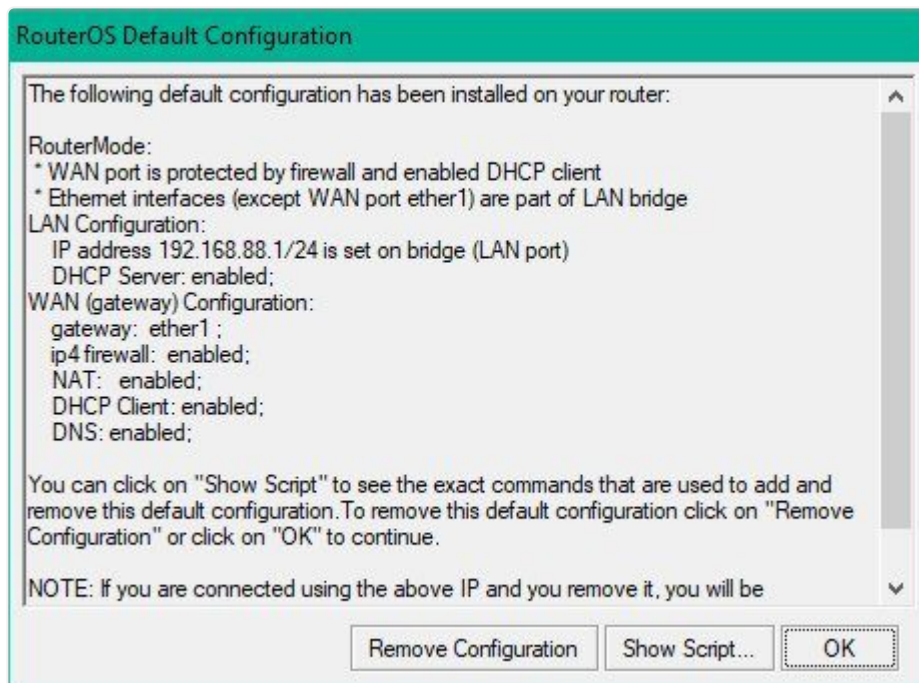
default configuration

The Mikrotik router can remain in the default setup for a basic configuration. In the Mikrotik default setup, port *ether 1* is an Internet port (WAN) with firewall and NAT (IP Address Translation) and works as a DHCP client. It therefore automatically receives an IP address if you plug it into an existing network with DHCP address assignment using this port.

Due to the fact that a secure firewall works on the *ether1* port in the default config, you are absolutely on the *safe* side when it comes to protection from the outside!

You can reset the Mikrotik in the menu item "*System -> Reset Configuration*" and tick "Default Configuration" and "No Backup" with a factory reset with this default configuration.

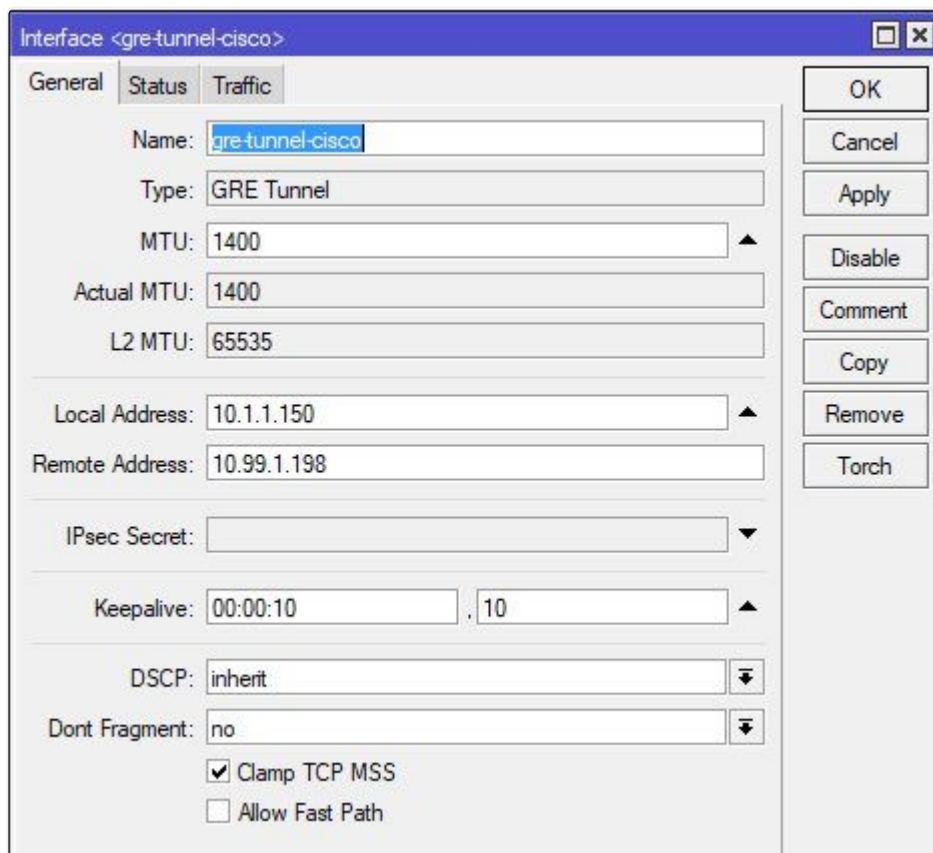
default configuration

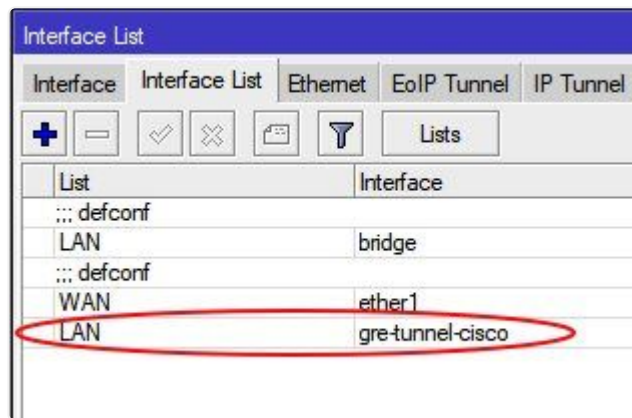


Interface and IP address configuration

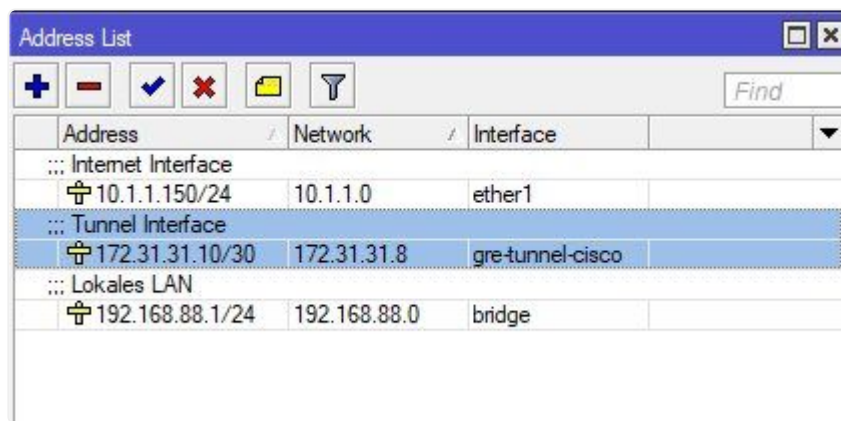
The first step is to set up a tunnel interface under *Interfaces - GRE*.

Set up the tunnel interface and add it to the "LAN" interface list:





Configure IP addresses on all interfaces:



Set IPsec key parameters

The Mikrotik offers the option to set a separate IPsec policy profile for phases 1 and 2. Of course you can do that if you want.

However, it is easier and clearer to free the already existing default profiles in Mikrotik from old loads (3DES and SHA1) and to set the more modern and secure AES encryption. The default profiles can then simply be retained.

Set IPsec peer profile (phase 1).

IPsec

Policies Policy Proposals Groups Peers Peer Profiles Remote Peers Mode Configs

+ - Y

Name	Hash Algorithms	Encryption Algorithm	DH Group
* default	sha256	aes-128 aes-256	modp2048

IPsec Peer Profile <default>

Name: default

Hash Algorithms: sha256

Encryption Algorithm:

- ☐ des
- ☒ aes-128
- ☒ aes-256
- ☐ camellia-128
- ☐ camellia-256
- ☐ 3des
- ☐ aes-192
- ☐ blowfish
- ☐ camellia-192

DH Group:

- ☐ modp768
- ☐ ec2n155
- ☐ modp1536
- ☐ modp3072
- ☐ modp6144
- ☐ ecp256
- ☐ ecp521
- ☐ modp1024
- ☐ ec2n185
- ☒ modp2048
- ☐ modp4096
- ☐ modp8192
- ☐ ecp384

Proposal Check: obey

Lifetime: 1d 00:00:00

Lifebytes:

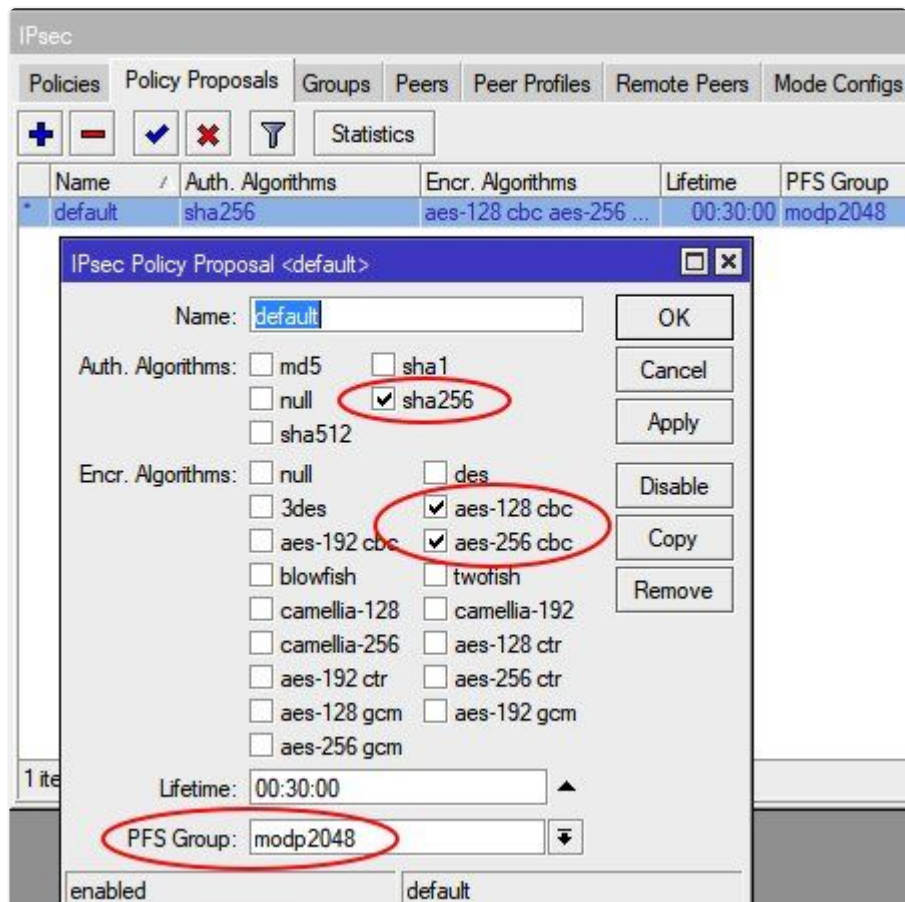
☐ NAT Traversal

DPD Interval: 120 s

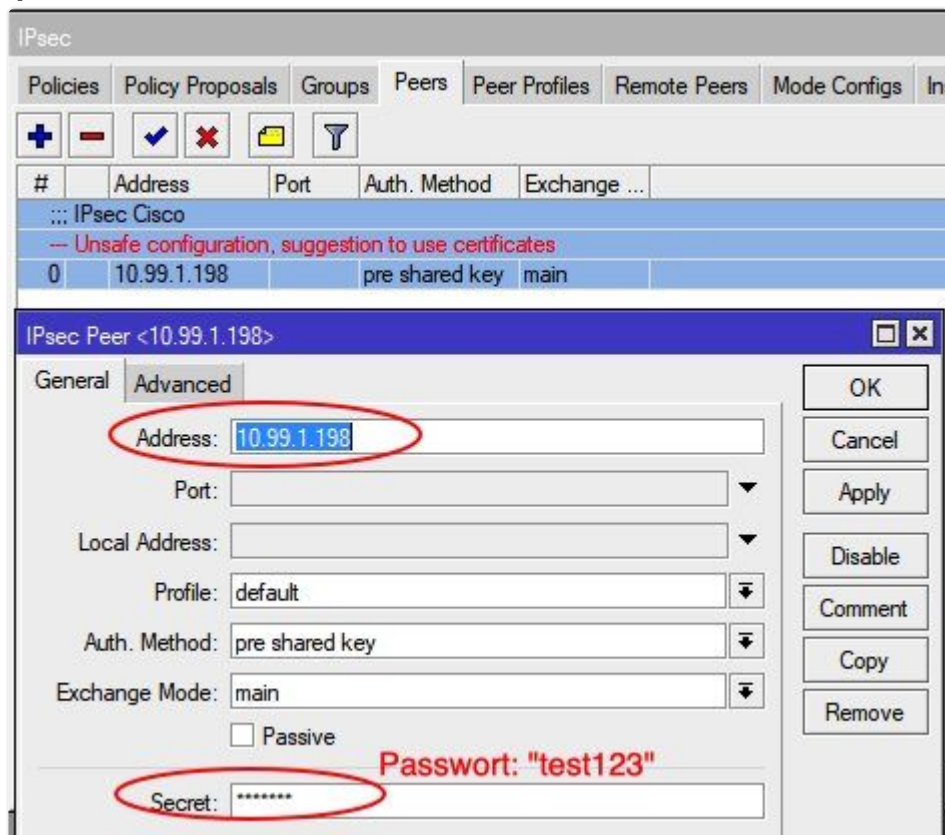
DPD Maximum Failures: 5

default

Set IPsec Policy Profile (Phase 2).

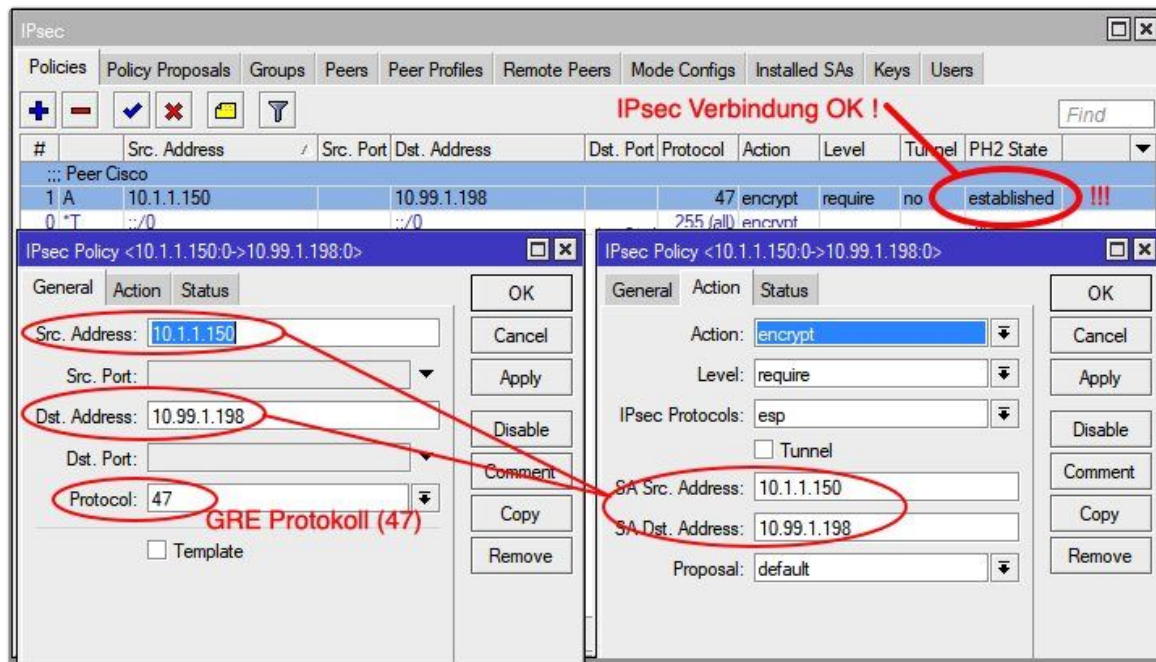


Set up IPsec peer on the Cisco



(For Mikrotik-2 from Chapter 6 the corresponding password: *secret123*)

Set IPsec peer policies



(Adjust the IP peer addresses on the second router (Mikrotik-2, Chapter 6) accordingly!)

If the status changes to "Established" in phase 2, the IPsec connection is OK and the tunnel is active. In return, the Cisco router then displays the *QM_IDLE* status with ***show crypto isakmp sa***.

```
cisco_router#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
10.99.1.198  10.1.1.150  QM_IDLE       2002  ACTIVE
10.1.1.150   10.99.1.198  QM_IDLE       2001  ACTIVE
```

Enable dynamic routing with RIPv2 protocol

In general, any dynamic routing protocol can be used here. A distance vector protocol such as OSPF is also an option here if required.

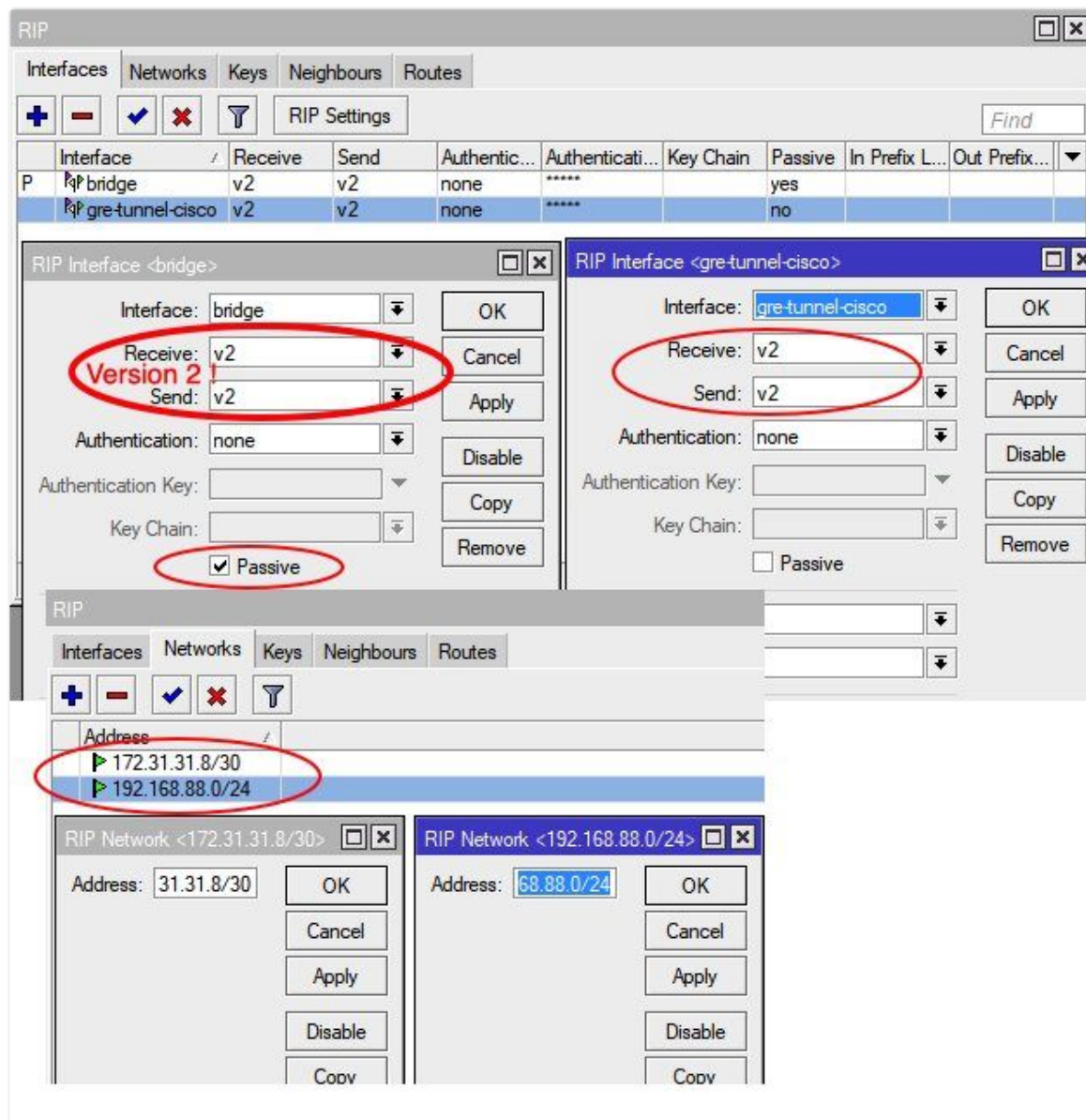
For the sake of simplicity, the tutorial describes a simple next-hop protocol such as the well-known [RIP](#) (Routing Information Protocol) in version 2.

RIP is also very widely available in KMU models of L3 switches and routers as well as in almost all firewalls. OSPF rather more in the high-end area. (If you are interested (PM), the tutorial can be expanded to include an OSPF chapter.)

It is very important that **version 2** of RIP is activated without fail!!!

Only RIPv2 can use [CIDR Subnet Masks](#) Work around subnets, i.e. with variable subnet masks. These modern CIDR masks, which are used everywhere today, finally replace the old division into fixed network classes, which was abolished in 1993.

Activate RIPv2 on the Mikrotik and enter local IP networks:



The "Passive" parameter on the LAN interface means that the router does not send any RIPv2 updates here and therefore does not pass on any routing data in the LAN. He should also only do it in the WAN (VPN)!

Anyone who operates other RIPv2 routers here in the LAN naturally does NOT activate passive mode here!

In addition, it is possible to provide the RIPv2 routing updates with a password to prevent unauthorized routers in the network from sending fake (false) routing updates in order to manipulate the data traffic.

Routing updates are then only accepted with remote sites that have the same passwords. A security feature.

Control of the routing table and IP connection

Route List						
Routes						
Next Hops						
Rules						
VRF						
Find						
all						
▼						
	Dest. Address	Gateway	Distance	Routing Mark	Pref. Source	
AS	0.0.0.0/0	10.1.1.254 reachable ether1	1			
DAC	10.1.1.0/24	ether1 reachable	0		10.1.1.150	
DAC	172.31.31.8/30	gre-tunnel-cisco reachable	0		172.31.31.10	
DAr	192.168.77.0/24	172.31.31.9 reachable gre-tunnel-cisco	120			
DAC	192.168.88.0/24	bridge reachable	0		192.168.88.1	

(DAC = Connected IP networks, DAr = dynamically learned via RIPv2)

Distance : 0=local, 1=static, 120=learned with RIPv2)

Routing table check on the Cisco router:

```
cisco_router#sh ip rou
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from
PfR
```

Gateway of last resort is 10.99.1.254 to network 0.0.0.0

```
S*    0.0.0.0/0 [254/0] via 10.99.1.254
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      10.99.1.0/24 is directly connected, Ethernet1
L      10.99.1.198/32 is directly connected, Ethernet1
      172.31.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.31.31.8/30 is directly connected, Tunnel0
L      172.31.31.9/32 is directly connected, Tunnel0
      192.168.77.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.77.0/24 is directly connected, Vlan1
L      192.168.77.1/32 is directly connected, Vlan1
R      192.168.88.0/24 [120/1] via 172.31.31.10, 00:00:01, Tunnel0
```

```
cisco-router#sh ip rip database
172.31.0.0/16    auto-summary
172.31.31.8/30  directly connected, Tunnel0
192.168.77.0/24 auto-summary
192.168.77.0/24 directly connected, Vlan1
192.168.88.0/24 auto-summary
```



```
192.168.88.0/24
[1] via 172.31.31.10, 00:00:19, Tunnel0
```

120/1 also shows the networks learned from the Mikrotik via RIPv2 ("R").

A ping from a local LAN to the remote local LAN now verifies that VPN site networking is working correctly.

Is that really safe? Trust is good, control is better !

Haven't any configuration errors been made? Is the data really secure and encrypted?

Latent doubts (almost) always remain if you do not explicitly look at the data traffic of the locations.

A quick check of whether the VPN data is really securely encrypted over public networks (Internet) is never wrong and creates trust in this solution! The Cisco router displays the security:

```
cisco_router#sh crypto isakmp policy
Global IKE policy
Protection suite of priority 10
    encryption algorithm:  AES - Advanced Encryption Standard (256
bit keys).
    hash algorithm:        Secure Hash Standard 2 (256 bit)
    authentication method: Pre-Shared Key
    Diffie-Hellman group:  #14 (2048 bit)
    lifetime:              86400 seconds, no volume limit
```

And also the Mikrotik in his log...:

Jan/21/2019 18:39:13	memory	ipsec, info	respond new phase 1 (Identity Protection): 10.1.1.150[500]<=>10.99.1.198[500]
Jan/21/2019 18:39:15	memory	ipsec, info	ISAKMP-SA established 10.1.1.150[500]-10.99.1.198[500]
Jan/21/2019 18:39:22	memory	ipsec, info	spi:2fc82cb916d5e3e8f250a5e3419cce7
Jan/21/2019 18:39:22	memory	ipsec, info	ISAKMP-SA established 10.1.1.150[500]-10.99.1.198[500]
Jan/21/2019 18:39:40	memory	ipsec, info	spi:2b6a67123dc11fe2:c258316035e77e10
Jan/21/2019 18:39:40	memory	interface, info	gre-tunnel-cisco link up

As usual, a Wireshark sniffer trace provides the last certainty that the data is secure:

Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe						
Anzeigefilter anwenden ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
23	24...	10.99.1.199	10.1.1.150	ISAKMP	430	Identity Protection (Main Mode)
24	25...	10.99.1.198	10.1.1.150	ISAKMP	150	Informational
25	25...				60	<Ignored>
26	26...	10.99.1.198	10.1.1.150	ESP	138	ESP (SPI=0x0d988191)

> Frame 26: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0						
> Ethernet II, Src: da:33:c1:64:ca:fe (da:33:c1:64:ca:fe), Dst: Routerbo_66:76:64 (d4:ca:6d:66:76:64)						
> Internet Protocol Version 4, Src: 10.99.1.198, Dst: 10.1.1.150						
▼ Encapsulating Security Payload						
ESP SPI: 0x0d988191 (228098449)						
ESP Sequence: 9						

0000	d4 ca 6d 66 76 64 da 33 c1 64 ca fe 08 00 45 c0	..mfvd-3..d....E..
0010	00 7c 00 09 00 00 fe 32 a3 c7 0a 63 01 c6 0a 012....c....
0020	01 96 0d 98 81 91 00 00 00 09 42 ee 05 42 44 78B..BDx
0030	8b ae 8f 4d 48 5d cd 78 df 03 23 01 62 5f c2 bf	...MH]..x..#..b..
0040	5f d8 25 20 3d 63 0f 76 aa 1b 15 58 b1 03 f6 df	..% =c.v...X....
0050	b6 99 cb 78 e4 c0 ce 77 55 29 e4 6d cb 86 af b6	...x...w U)..m....
0060	1b 18 24 38 85 de 9d 42 49 34 ce 5c 9a f9 54 6b	..\$8...B I4:\...Tk
0070	3e e7 7f 75 53 08 aa 78 1f aa ff 38 14 cf be d2	>...uS...x...8....
0080	fd 97 e1 12 fa 3c 4d 94 92 2e<M... ..

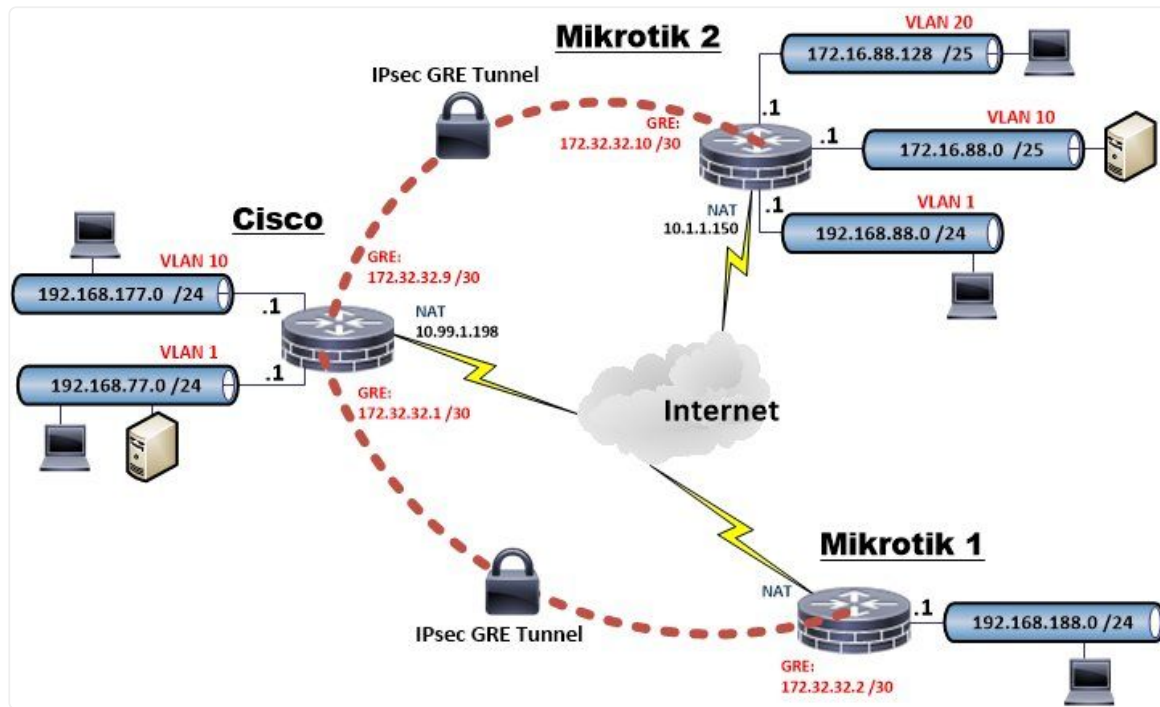
The **ESP** package transports the encrypted data between the 2 locations!

Works as designed...! 👍

Advanced site configuration with multiple local LANs or VLANs

A more practice-oriented VPN site design is one that also considers multiple local (V)LANs, as the majority of SMB networks are segmented these days. Bigger ones anyway. Due to the introduction of VoIP, this has to be the case in order to keep voice data away from productive networks.

The example describes 3 locations and can be extended to any other location. The configuration steps are always the same.



The configuration commands to be extended for the Cisco router for a second location and another local LAN (VLAN 10) are **marked in red above**.

For the basic VLAN configuration of the Mikrotiks you will find a separate, detailed [VLAN_Tutorial](#) here in the forum !

Only the RIP routing process has to be activated and the additional local IP networks and interfaces entered there in the RIP routing.

Use virtual tunnel interfaces VTI instead of GRE tunnel

An alternative to the traditional use of GRE tunnels with dynamic routing shown above is the more modern approach with VTI tunnels. Current IPsec implementations usually also support VTI interfaces. This makes it much easier to configure an IPsec LAN to LAN connection with dynamic routing protocols and, for example, parallel multicast routing. As already seen above with the GRE tunnels, VTI interfaces behave like normal network interfaces.

The demo setup here uses the same internet test infrastructure as above. The more modern OSPF instead of RIPv2 is used here as a dynamic routing protocol to show both configuration options.

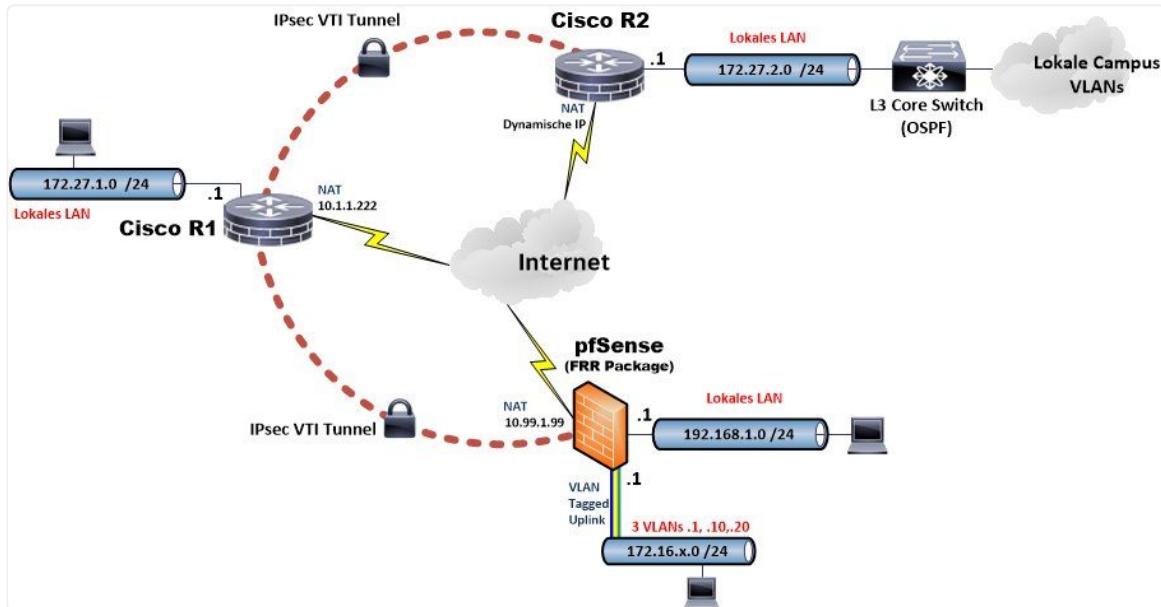
In the pfSense, the routing package *Quagga-OSPF* or alternatively the *FRR* Package to be installed. Here in the example FRR was used. Ultimately it doesn't matter because the configs of the two packages are almost identical.

At Mikrotik, VTI support is currently still a request for future firmware and is therefore currently not supported in this variant.

The basic configuration with IPs, zone-based firewall, etc. remains in place on the Cisco Config, which is why only the changed IPsec configurations are listed here for the sake of clarity.

Here we go...

VTI test environment



Cisco router setup with VTI and OSPF

Cisco Router 1 (R1):

```
!  
crypto keyring ROUTER1  
pre-shared-key address 0.0.0.0 0.0.0.0 key secret123  
pre-shared-key hostname CiscoR2 key secret1234  
!  
crypto isakmp policy 5  
encr aes 256  
hash sha256  
authentication pre-share  
group 14  
!  
crypto isakmp policy 10  
encr aes  
authentication pre-share  
group 2  
!  
crypto isakmp profile DVTI  
description Dynamic VPN Tunnel  
keyring ROUTER1  
match identity address 0.0.0.0  
virtual-template 3  
crypto isakmp profile CISCO_R2  
description Dynamic VPN Tunnel Cisco R2  
keyring ROUTER1
```

```
self-identity user-fqdn CiscoR1
match identity user-fqdn CiscoR2
virtual-template 2
!
crypto ipsec transform-set VTISSET esp-aes esp-sha-hmac
mode tunnel
!
crypto ipsec profile CISCO_R2
set transform-set VTISSET
set isakmp-profile CISCO_R2
!
crypto ipsec profile DVTI
set transform-set VTISSET
set isakmp-profile DVTI
!
interface
Loopback1 ip address 172.27.27.1 255.255.255.255
!
interface Virtual-Template2 type tunnel
description Tunnel Interface Cisco-R2
ip unnumbered Loopback1
ip ospf network point-to-point
tunnel source 10.1.1.222
tunnel mode ipsec ipv4
tunnel destination dynamic
tunnel protection ipsec profile CISCO_R2
!
interface Virtual-Template3 type tunnel
description Dynamic VTI Tunnel
ip unnumbered Loopback1
ip mtu 1400 <== (must be set to 1400 for pfSense otherwise OSPF link MTU mismatch!)
ip ospf network point-to-point
tunnel source 10.1.1.222
tunnel mode ipsec ipv4
tunnel destination dynamic
tunnel protection ipsec profile DVTI
!
interface Vlan1
description Local LAN
ip address 172.27.1.254 255.255.255.0
ip nat inside
!
interface <WAN>
description Internet Port
```

```
ip address 10.1.1.222 255.255.255.0
ip nat outside
!
router ospf 1
router-id 172.27.27.1
passive-interface default
no passive-interface Virtual-Template2
no passive-interface Virtual-Template3
network 172.27.1.0 0.0.0.255 area 0
network 172.27.27.1 0.0.0.0 area 0
!
end
```

Cisco Router 2 (R2):

```
!
crypto keyring ROUTER2
pre-shared-key hostname CiscoR1 key secret1234
!
crypto isakmp policy 5
encr aes 256
hash sha256
authentication pre-share
group 14
!
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
!
crypto isakmp profile ROUTER1
description IPsec Tunnel Router-1
keyring ROUTER2
self-identity user-fqdn CiscoR2
match identity user-fqdn CiscoR1
!
crypto ipsec transform-set VTISSET esp-aes esp-sha-hmac
mode tunnel
!
crypto ipsec profile ROUTER1
set transform-set VTISSET
set isakmp-profile ROUTER1
!
!
interface
```

```
Loopback1 ip address 172.27.27.5 255.255.255.255
!
interface Tunnel1
description VPN Tunnel Router-1
ip unnumbered Loopback1
tunnel source <WAN Interface>
tunnel mode ipsec ipv4
tunnel destination 10.1.1.222
tunnel protection ipsec profile ROUTER1
!
interface <WAN>
description Internet Port
ip address <Dynamic>
ip nat outside
!
interface Vlan1
description Local LAN
ip address 172.27.2.254 255.255.255.0
ip nat inside
!
router ospf 1
router-id 172.27.27.5
passive-interface default
no passive-interface Tunnel1
no passive-interface Vlan1
network 172.27.2.0 0.0.0.255 area 0
network 172.27.27.5 0.0.0.0 area 0
!
end
```

pfSense setup with VTI and OSPF

The pfSense has a normal standard setup, which is not discussed further in the tutorial. Basic configurations for pfSense can be found in the links below.

Only on the third OPT port are 3 Vlan's 1, 10 and 20 connected via a VLAN switch in order to "fill" the OSPF routing table a little.

A normal LAN to LAN tunnel with phase 1 and phase 2 is set up via the IPsec VPN:

Phase 1:

General Information	
Disabled	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.
Key Exchange version	IKEv1 Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.
Internet Protocol	IPv4 Select the Internet Protocol family.
Interface	WAN Select the interface for the local endpoint of this phase1 entry.
Remote Gateway	10.1.1.222 Enter the public IP address or host name of the remote gateway.
Description	Cisco R1 VTI A description may be entered here for administrative reference (not parsed).

Phase 1 Proposal (Authentication)	
Authentication Method	Mutual PSK Must match the setting chosen on the remote side.
Negotiation mode	Main Aggressive is more flexible, but less secure.
My identifier	My IP address
Peer identifier	Peer IP address
Pre-Shared Key	geheim123 Enter the Pre-Shared Key string. This key must match on both peers. This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise. Generate new Pre-Shared Key

Phase 1 Proposal (Encryption Algorithm)	
Encryption Algorithm	AES Algorithm
Key length	128 bits
Hash	SHA1
DH Group	2 (1024 bit)
Delete	
Note: Blowfish, 3DES, CAST128, MD5, SHA1, and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.	
Add Algorithm	+ Add Algorithm

Phase 2:

ATTENTION: What is special here is the phase 2 mode, which must be set to **(routed) VTI**!

General Information	
Disabled	<input type="checkbox"/> Disable this phase 2 entry without removing it from the list.
Mode	Routed (VTI)
Local Network	Address Type Local point-to-point IPsec interface tunnel network address.
Remote Network	Address Type Remote point-to-point IPsec interface tunnel network address.
Description	Cisco R1 VTI A description may be entered here for administrative reference (not parsed).

2 Host IP Adressen im gleichen IP Netzwerk

Loopback IP Cisco R1

Phase 2 Proposal (SA/Key Exchange)

Protocol ESP
 Encapsulating Security Payload (ESP) is encryption, Authentication Header (AH) is authentication only.

Encryption Algorithms

☒ AES Auto

☐ AES128-GCM Auto

☐ AES192-GCM Auto

☐ AES256-GCM Auto

☐ Blowfish Auto

☐ 3DES

☐ CAST128
 Note: Blowfish, 3DES, and CAST128 provide weak security and should be avoided.

Hash Algorithms ☐ MD5 ☒ SHA1 ☐ SHA256 ☐ SHA384 ☐ SHA512 ☐ AES-XCBC

Note: MD5 and SHA1 provide weak security and should be avoided.

PFS key group 2 (1024 bit)
 Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Lifetime 3600
 Specifies how often the connection must be rekeyed, in seconds

If you have done everything correctly, the IPsec overview looks like this:

IPsec Tunnels									
	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions	
<div><input type="checkbox"/></div> <div>Disable</div> <div></div>	V1	WAN 10.1.1.222	main	AES (128 bits)	SHA1	2 (1024 bit)	Cisco R1 VTI	<div></div> <div></div> <div></div>	
			Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	P2 actions
<div><input type="checkbox"/></div> <div>Disable</div> <div></div>			vti	172.27.27.2	172.27.27.1	ESP	AES (auto)	SHA1	<div></div> <div></div> <div></div>
<div><div>+</div>Add P2</div>									

If all the settings are correct, the VTI tunnel to the Cisco is set up without errors ("established"):

IPsec Status									
IPsec ID	Description	Local ID	Local IP	Remote ID	Remote IP	Role	Reauth	Algo	Status
con1000: #1	Cisco R1 VTI	10.99.1.99	10.99.1.99	10.1.1.222	10.1.1.222	IKEv1 initiator	26768 seconds (07:26:08)	AES_CBC HMAC_SHA1_96 PRF_HMAC_SHA1 MODP_1024	ESTABLISHED 1402 seconds (00:23:22) ago Disconnect

IPsec ID	Local subnets	Local SPI(s)	Remote subnets	Times	Algo	Stats	
con1000: #1	0.0.0.0/0	Local: c0d916fd Remote: 2f3e38ef	0.0.0.0/0	Rekey: 1646 seconds (00:27:26) Life: 2198 seconds (00:36:38) Install: 1402 seconds (00:23:22)	AES_CBC HMAC_SHA1_96 MODP_1024 IPComp: none	Bytes-In: 13,570 (13 KiB) Packets-In: 165 Bytes-Out: 21,128 (21 KiB) Packets-Out: 153	Disconnect

OSPF routing protocol pfSense

The *Quagga-OSPF* or the *FRR* package must first be installed via the pfSense package management in order to activate the OSPF routing. Which one you take is purely a matter of taste. The config of both OSPF packages in the pfSense GUI is very similar. Here in the example *FRR* was used.

Enable OSPF with logging

Services / FRR / OSPF / OSPF

OSPF Interfaces Areas [Global Settings] [BFD] [BGP] [OSPF6] Status

General Options

Enable ☒ Enable OSPF Routing

Log Adjacency Changes ☒ If set to yes, adjacency changes will be written via syslog.










Router ID 172.27.27.2 (Lokale VTI IP pfSense)
Specify the Router ID. RID is the highest logical (loopback) IP address configured on a router.
For more information on router identifiers see [wikipedia](#).

SPF Hold Time
Set the SPF holdtime in milliseconds. The minimum time between two consecutive shortest path first calculations.
(0-60000, Default: 1000)

SPF Delay
Set SPF delay in milliseconds. The delay between receiving an update to the link state database and starting the shortest path first calculation.
(0-600000, Default: 200)

Enable SNMP AgentX ☐ Enable agentx support for accessing FRR Zebra data via SNMP with the net-snmp package.

Assign interfaces and OSPF area: (Here for the sake of simplicity everything in the backbone area 0)

Services / FRR / OSPF / Interfaces ?					
OSPF	Interfaces	Areas	[Global Settings]	[BFD]	[BGP] [OSPF6] Status
Interface	Description	Metric	Area	Authentication	
opt4	VTI Tunnel R1		0		 
lan	LAN		0		 
opt1	VLAN1		0		 
opt2	VLAN10		0		 
opt3	VLAN20		0		 

OSPF function and routing check

Cisco R1:

```
Router-1#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address
Interface				
172.27.27.5	0	FULL/ -	00:00:37	172.27.27.5
Virtual-Access2				
172.27.27.2	0	FULL/ -	00:00:35	172.27.27.2
Virtual-Access1				

```
Router-1#sh ip routes
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS

level-2

ia - IS-IS inter area, * - candidate default, U - per-user static

route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

a - application route

+ - replicated route, % - next hop override, p - overrides from

PfR

Gateway of last resort is 10.1.1.254 to network 0.0.0.0

```
S* 0.0.0.0/0 [1/0] via 10.1.1.254
   10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   10.1.1.0/24 is directly connected, Vlan99
L   10.1.1.222/32 is directly connected, Vlan99
   172.16.0.0/24 is subnetted, 3 subnets
O   172.16.1.0 [110/1100] via 172.27.27.2, 00:07:14, Virtual-
Access1
```


Detailed FRR Status

- Zebra Routes
- Zebra IPv6 Routes
- OSPF General
- OSPF Neighbors
- OSPF Routes

Zebra Routes

Display 100 of 24 items
Filter expression: Filter

```

pfsense:~# ssh home.arpa> show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

K>* 0.0.0.0/0 [0/0] via 10.99.1.254, 00:35:07
K>* 10.1.1.222/32 [0/0] via 10.99.1.254, 00:35:07
C>* 10.99.1.0/24 [0/1] is directly connected, re1, 00:35:07
O  172.16.1.0/24 [110/100] is directly connected, re0, 00:35:07
C>* 172.16.1.0/24 [0/1] is directly connected, re0, 00:35:07
K>* 172.16.7.254/32 [0/0] via 10.99.1.254, 00:35:07
O  172.16.10.0/24 [110/100] is directly connected, re0.10, 00:35:07
C>* 172.16.10.0/24 [0/1] is directly connected, re0.10, 00:35:07
O  172.16.20.0/24 [110/100] is directly connected, re0.20, 00:35:07
C>* 172.16.20.0/24 [0/1] is directly connected, re0.20, 00:35:07
O>* 172.27.1.0/24 [110/11] via 172.27.27.1, ipsec1000 onlink, 00:31:50 — Cisco R1
O>* 172.27.2.0/24 [110/1011] via 172.27.27.1, ipsec1000 onlink, 00:32:01 — Cisco R2
C>* 172.27.27.0/30 [0/1] is directly connected, ipsec1000, 00:35:07
O>* 172.27.27.1/32 [110/11] via 172.27.27.1, ipsec1000 onlink, 00:32:01 — Cisco R1
O>* 172.27.27.5/32 [110/1011] via 172.27.27.1, ipsec1000 onlink, 00:32:01 — Cisco R2
O  192.168.1.0/24 [110/100] is directly connected, re2, 00:35:07
C>* 192.168.1.0/24 [0/1] is directly connected, re2, 00:35:07

```

Last but not least the firewall routing table:

IPv4 Routes					
Destination	Gateway	Flags	Use	Mtu	Netif
default	10.99.1.254	UGS	1177	1500	re1
10.1.1.222	10.99.1.254	UGHS	447	1500	re1
10.99.1.0/24	link#2	U	3	1500	re1
10.99.1.99 (WAN)	link#2	UHS	0	16384	lo0
127.0.0.1	link#4	UH	38	16384	lo0
172.16.1.0/24	link#1	U	170	1500	re0
172.16.1.1 (VLAN 1)	link#1	UHS	0	16384	lo0
172.16.7.254	10.99.1.254	UGHS	116	1500	re1
172.16.10.0/24	link#8	U	0	1500	re0.10
172.16.10.1 (VLAN 10)	link#8	UHS	0	16384	lo0
172.16.20.0/24	link#9	U	0	1500	re0.20
172.16.20.1 (VLAN 20)	link#9	UHS	0	16384	lo0
172.27.1.0/24 (Cisco R1)	172.27.27.1	UG1	0	1400	ipsec1000
172.27.2.0/24 (Cisco R2)	172.27.27.1	UG1	0	1400	ipsec1000
172.27.27.1 (Cisco R1)	link#10	UH	5	1400	ipsec1000
172.27.27.1/32	172.27.27.1	UG1	0	1400	ipsec1000
172.27.27.2	link#10	UHS	0	16384	lo0
172.27.27.5/32 (Cisco R2)	172.27.27.1	UG1	0	1400	ipsec1000
192.168.1.0/24	link#3	U	2483	1500	re2
192.168.1.1 (LAN)	link#3	UHS	0	16384	lo0

A ping check of the respective local interfaces of all 3 devices then runs successfully.

Related Links

Note on the Mikrotik GRE implementation !:

[https://administrator.de/knowledge/routeros-7-1beta6-gre-tunnel-funktion ...](https://administrator.de/knowledge/routeros-7-1beta6-gre-tunnel-funktion-...)

Cisco router basic configuration:

[https://administrator.de/wissen/cisco-880-890-router-Configuration-adsl- ...](https://administrator.de/wissen/cisco-880-890-router-Configuration-adsl-...)

RIP protocol overview:

https://de.wikipedia.org/wiki/Routing_Information_Protocol

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_rip/configurat ...](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_rip/configurat...)

<https://wiki.mikrotik.com/wiki/Manual:Routing/RIP>

OSPF VPN routing with WireGuard:

[https://administrator.de/tutorial/merkzettel-vpn-installation-mit-wiregu ...](https://administrator.de/tutorial/merkzettel-vpn-installation-mit-wiregu...)

OSPF with Mikrotik and pfSense/OPNsense via GRE:

<https://aspel.github.io/2018-11-19/ospf-over-gre-tunnel-with-ipsec-micro ...>

Simple IPsec tunnel config with pfSense firewall (no dynamic routing !):

<https://administrator.de/content/detail.php?id=437826&token=307#comm ...>

Location coupling with VTI and Cisco routers:

<https://www.administrator.de/content/detail.php?id=332230&token=14#c ...>

Location coupling with VTI Cisco and pfSense Firewall:

<https://administrator.de/forum/2921-kaskadierung-fritzbox-ipsec-tunnel-6 ...>

Transport IPv6 over v4 GRE Tunnel Interface with OSPF (Cisco):

<https://administrator.de/content/detail.php?id=630607&token=121#comm ...>

Classic Cisco IKEv1 location coupling on pfSense Firewall:

<https://administrator.de/content/detail.php?id=636683&token=689#comm ...>

Heterogeneous IPsec VPN site coupling from different manufacturers:

<https://administrator.de/wissen/ipsec-vpn-praxis-standort-kupplung-cisco ...>

Connect FritzBox VPN to Linux StrongSwan:

<https://administrator.de/contentid/1174573041#comment-1232746577>

Site Site to Site IPsec VPN with pfSense Firewall and Mikrotik Router with dynamic IP:

<https://administrator.de/content/detail.php?id=501151&token=508#comm ...>

OT: Mikrotik L2TP VPN for mobile clients:

<https://administrator.de/content/detail.php?id=562927&token=111#comm ...>

OT: Mikrotik OpenVPN Config Details:

<https://administrator.de/content/detail.php?id=359367&token=695#comm ...>

OT: DS-Lite connection with pfSense:

<https://cybercyber.org/m-net-ds-lite-verbinding-mit-pfsense.html>

OT: Make AirPrint printers and other Bonjour/mDNS services accessible:

<https://administrator.de/contentid/2382190660#comment-2394690003>

Content-Key: 398932

Url: <https://administrator.de/contentid/398932>

Ausgedruckt am: 06.04.2022 um 15:04 Uhr

5 comments



ITgustel 04/02/2020 at 13:36:42

Hello, could you add a DHCP relay to the example?

I am currently failing (in a Mikrotik to Mikrotik VPN) to get a working relaying.



aqui 03.04.2020 updated at 09:37:54

Clear !

Please be patient so I can test the watertightness.

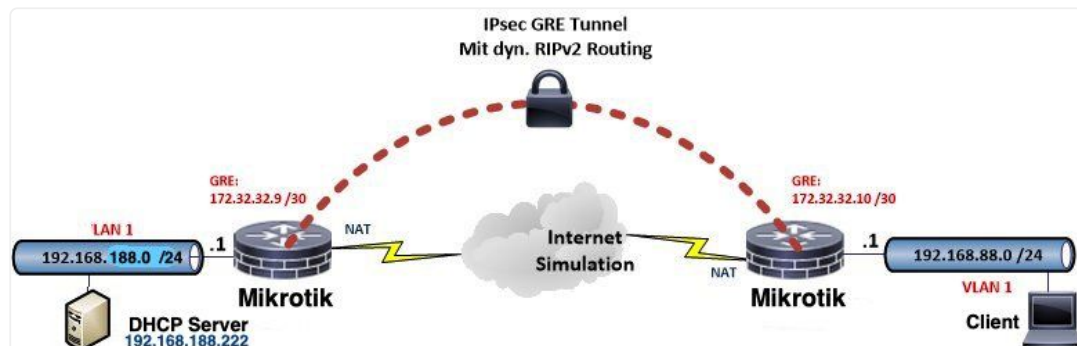
One more question about your setup:

Do you use a DHCP server on or at a central Mikrotik to supply other networks with IPs or do you have an external, central DHCP server such as a Windows DHCP at a main location?

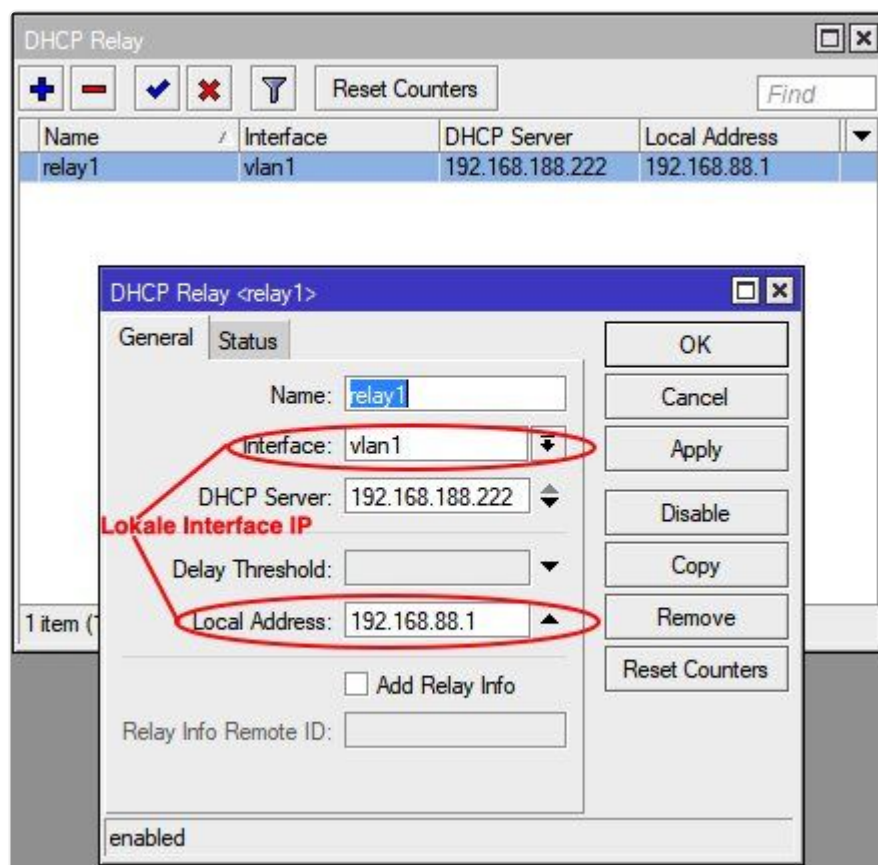


aqui 03.04.2020 updated at 18:24:42

So, the solution is relatively simple and works absolutely error-free:
test design and config is identical to above.



Setup of the DHCP relay on the client side router (vlan1 IP segment):



The client interface, the interface IP address and the IP address of the DHCP server must be specified here!

Config of the DHCP server (here ISC-DHCP):

```
# Konfigurations Datei fuer ISC dhcpd
#
ddns-update-style none;
authoritative;
ping-check true;
option domain-name "dhcptest.home.arpa";
option domain-name-servers 192.168.7.254, 192.168.188.1 ;
default-lease-time 600;
max-lease-time 7200;

# DHCP Log Messages senden.
log-facility local7;

# DHCP Ranges fuer die lokalen LAN Subnetze
subnet 192.168.188.0 netmask 255.255.255.0 {
    range 192.168.188.100 192.168.188.150;
    option routers 192.168.188.1;
}
subnet 192.168.88.0 netmask 255.255.255.0 {
    range 192.168.88.100 192.168.88.150;
    option domain-name "subnet88.home.arpa";
    option routers 192.168.88.1;
}
subnet 192.168.99.0 netmask 255.255.255.0 {
    range 192.168.99.100 192.168.99.150;
    option domain-name "subnet99.home.arpa";
    option routers 192.168.99.1;
}
```

Output of the DHCP lease file:

```
lease 192.168.88.149 {
    starts 5 2020/04/03 15:43:08;
    ends 5 2020/04/03 15:53:08;
    tstp 5 2020/04/03 15:53:08;
    cltt 5 2020/04/03 15:43:08;
    binding state free;
    hardware ethernet 00:23:5a:4f:01:22;
    uid "\001\000#Z?\001\000";
    set vendor-class-identifier = "MSFT 5.0";
}
```

Checks DHCP Client (HP Windows 10 Laptop):

```
C:\Windows>ipconfig -all
```

```
Windows-IP-Konfiguration
```

```

Hostname . . . . . : Laptop
Primäres DNS-Suffix . . . . . :
```

```
Knotentyp . . . . . : Hybrid
IP-Routing aktiviert . . . . . : Nein
WINS-Proxy aktiviert . . . . . : Nein
DNS-Suffixsuchliste . . . . . : subnet88.home.arpa
```

Ethernet-Adapter LAN-Verbindung:

```
Verbindungsspezifisches DNS-Suffix: subnet88.home.arpa
Beschreibung. . . . . : Intel(R) 82567LM Gigabit
Network Connection
Physische Adresse . . . . . : 00-23-5A-4F-01-22
DHCP aktiviert. . . . . : Ja
Autokonfiguration aktiviert . . . : Ja
Verbindungslokale IPv6-Adresse . :
fe80::f488:debb:2cdf:f237%18(Bevorzugt)
IPv4-Adresse . . . . . : 192.168.88.149(Bevorzugt)
Subnetzmaske . . . . . : 255.255.255.0
Lease erhalten. . . . . : Freitag, 3. April 2020
17:34:19
Lease läuft ab. . . . . : Freitag, 3. April 2020
17:48:13
Standardgateway . . . . . : 192.168.88.1
DHCP-Server . . . . . : 192.168.188.222
DHCPv6-IAID . . . . . : 234890074
DHCPv6-Client-DUID. . . . . : 00-01-00-01-1B-A5-E8-14-00-
23-5A-4F-01-22
DNS-Server . . . . . : 172.16.7.254
192.168.188.1
NetBIOS über TCP/IP . . . . . : Aktiviert
```

Now you have something to craft over the weekend! 😊

Conclusion:

Works as designed! 😊



tikay event 05/16/2020 at 23:55:26

Hello [@aqui](#) ,

I've been busy doing hardware tests for the last few days, as I'll soon be building the whole thing for a data center interconnect. We have a direct L2 connection between the two data centers, but my supervisor insists on encryption and I need a routing protocol.

No problem so far, it's not the first time I've built something like this. So far on LANCOM, but since I have to reach something close to gigabit, LANCOM is out.

I've tried countless different things (Cisco, Huawei, Mikrotik, OPNsense*), but always in the tunnel variant and loopback interfaces on both sides instead (LANCOM took out the transport mode and it never really worked with that).

*please never never again

I did the Mikrotik test with two RB750Gr3 (vulgo hEX) and got about a third of the IPSec throughput specified online. So from the 470Mbit that Mikrotik measured pure, I get 170Mbit. Measured with iPerf in TCP mode with 20GB of data, partly with adjusted MTU to 1360 or 1380 bytes. My configuration was adapted to the hardware acceleration of the hEX.

Do you know what throughput you can achieve with transport mode? You save yourself a pass through the router. Since we probably have different devices, the ratio of the real to the microtic reading would also make sense here.

I've now ordered two more RB4011...!\$\$!"\$\$!"\$ with which I want to test whether I can get to the gigabit mark. [Regards](#)

@tikayevent

PS: I use OSPF instead of RIP, but I guess that won't matter.



aqui 05/17/2020 updated at 12:01:23 p.m

You save yourself a pass through the router.

Well, not quite, the IP forwarding decision is also made somewhere, so routing is also done and it's the same in terms of encryption. You only save the additional tunnel overhead and have fewer MTU problems.

But to answer the question: I currently have no practical values with iPerf3 etc. and am orienting myself to the official product-related IPsec throughput figures from Mikrotik. In general, you should always make sure that there is IPsec acceleration in hardware on the platform:

https://wiki.mikrotik.com/wiki/Manual:IP/IPsec#Hardware_acceleration

With your 4011s, this is the case for all crypto suites! So you're not doing anything wrong with that.

You can see the expected IPsec throughput figures [HERE](#).

In any case, you will always reach the gigabit mark with frame sizes between 512 and 1400 bytes. With smaller frame sizes, it then, as usual, comes to a halt.

I'm using OSPF instead of RIP, but I guess that won't matter.

No, just the opposite. OSPF is better. Less overhead, faster convergence. I'll expand on that in the tutorial in due course. 😊

More from aqui



How to properly back up ESXi VMs?

aqui - 26 comments



IKEv2 VPN Server for Windows and Apple Clients with Raspberry Pi

aqui - 1 comment



Link Aggregation (LAG) in the network

aqui - 15 comments



Notepad: VPN installation with Wireguard

aqui - 21 comments

hotly debated



IPv6 Privacy Extensions does not work

Marcus78 - 65 comments



My PC "laughs at me"!



dm-magic - 42 comments



New acquisition, modem Fritzbox telephone separately, wiring
wusa88 - 32 comments



DHCP madness TPLink switches VLANs
felix94 - 27 comments



Windows 11 or the fairy tale of Rumpelstiltskin!
1Werner1 - 27 comments



Microsoft wants to give Linux a "Windows Subsystem".
kgborn - 22 comments



Outdoor and fireproof server cabinet
ButterBot - 21 comments



Protection against ransomware - create a subnet
fishrain - 20 comments



Outlook Contacts Update business cards for existing contacts
Quercus - 19 comments



Calculation in report in Access
jhausstein - 17 comments



Which licenses should I purchase?
MrRoyal - 16 comments



Website cannot be reached from the internal network
finn.h - 16 comments