- Technical Whitepaper -

configuration examples

of

VPN routers

msm net ingenieurbüro meissner
Am Porstendorferweg 4
07570 Niederpöllnitz - Germany

Table of contents:

1. x509 certificate administration

1.1. Globals to use the certificate administration

Each of the VPN routers of msm net ingenieurbüro meissner is equipped with a complete x509 certificate administration.

Variant 1

With this certificate administration any number of certificate authorities (Root CA) can be created and administered. Furthermore, any number of user certificates can be created. The creation of a user certificate is carried out in such a way that the created user certificate is automatically signed by the related certificate authority (Root CA). That means, a user certificate can be used immediately after its creation. Through the hierarchical connection of certificate authority and user certificate, every business can create and use a simple, independent, valid and – most of all – free of cost PKI.

Variant 2

With this certificate administration any number of requests and certificates (RootCA, SubCA and Ident certificates) can be created and signed. Through the integration of a CryptoSmartcard application (at present eToken of Aladdin) high-security PKI structures can be realized. Extensive export and import functions are realized analogously to variant 1.

Complex CRL applications (creation, import, export, and automatic collection) are integrated in both variants. In the signing of RootCAs of variant 2 the integration of OCSP (Online Certificate Status Protocol) is also realized at the same time.

1.2. Creation of a certificate authority (CA variant 1)

After the successful logon at the VPN router as administrator you change into the menu VPN connections and to the certificate administration there. In the left part of this page you will find indicated all existing certificate authorities. In the right part you are offered further options. Clicking on the key „create certificate authority“, a new page will be opened. There you will be asked to put in all data necessary for the creation of a new certificate authority. All of your inputs will be checked for admissible characters and length before creating a certificate authority. By pressing the „store“ key and your valid inputs, a new certificate authortiy will be set up. The given name used by you for the new certificate authority is now in the list of the certificate authorities. By clicking on the name and pressing the key „certificate authoritiy details“ you can display the root CA. Paging down in this window you will find the line: CA:TRUE.

You can see from this that it is a certificate authority.

1.3. Creation of user certificates

If you want to create a new user certificate, first select one certificate authority from the overview of the certificate authorities in which a new user certificate shall be created. Then click the key „select certificate authority“.

If the certificate authority has been created on this VPN rooter, you can now create a user certificate. If the VPN router is not the same router on which the certificate authority has been created, i.e. it was a certificate import, then some further functions will not be at your disposal. With the selection of a possibly existing certificate you can display this in detail, too. Clicking on „create new certificate“ a new page will appear in which the necessary data for the creation of a user certificate have to be put in. With the storing of the data (their validity is automatically checked) a new user certificate will be created. Within the list of certificates of the certificate authority the name of the new certificate will be found then.

1.4. Revocation of user certificates (variant 1)

Should it be necessary for any reason to revoke a user certificate, then please select the certificate from the list by clicking. As a second step please press the key „revoke selected certificate“.

In the next step you will be asked again if you really want to cancel this certificate. Please confirm if you are sure. The certificate will be revoked then. In the display this can be seen by having a '#' befor the name of the user certificate and the whole line is displayed in red. With the revocation of a certificate a new CRL (Certificate Revocation List) is automatically created. You can display this list by cklicking on the key „certificate revocation list“. You will then see all revoked user certificates of the certificate authority listed with details.

1.5. Export of user certificates (variant 1)

For the use of certificates created by you on other machines, they have to be exported. To do this, please act as follows: Call up the page of the certificate authorities and press „select certificate authority“. Then press „export certificate“. A page will be displayed where you can see all certificates of the certificate authority for the export. Please select those certificates which you want to export and enter the related password. If you have chosen the same password for all certificates, you can also use the related collective function. Having completed your inputs please press the key „next“. In the following window you are then offered all selected certificates for downloading in the PKCS12-format.

Please click with the context-key (right mouse key) on the respective certificate and press „store under...“. All certificates stored in this way can now be imported without problems on the respective target-VPN-router. An import on different systems (e.g. Windows X, Linux,...) in this file format is also possible, since all necessary data for the use of a certificate are enclosed in these files.

1.6. Import from x509 certificates in PKCS12 - format

To import an exported or other certificate in the PKCS12-format, please click „import external certificates (PKCS12)“ on the page of the certificate authorities. Please enter the necessary data into the form and click on „import“ then. Through this import a complete certificate authority and the related user certificate is created. You can import several user certificates into one certificate authority on condition that these user certificates have been signed by one certificate authority. If it is not the case, a new certificate authority is created. Selecting the newly created (import) certificate authority you can see that only a part of the functions of a normal certificate authority will be at disposal. If you want to use the mechanisms of the CRL administration, you still have to set up this administration.

1.7. Creation and export of a CRL

Each certificate authority with which you can create user certificates has got one certificate revocation list (CRL). This CRL is automatically created with generation of the certificate authority. When creating a certificate authority, please enter the cycle in days when a new CRL shall be created. At the end of this time a new CRL of the certificate authority will automatically be created on the VPN router.

Regardless of this cycle, a new CRL will be created if a user certificate is revoked. The CRL can be downloaded for further use from the creating VPN router. For that you do as follows:

- Select the certificate authority
- Select certificate revocation list
- Select export.

With it the certificate revocation list will be downloaded on you local processor and is at your disposal for further use.

1.8. Publication and use of a CRL

The certificate revocation list can be published in the internet on a web- or Ftp-server. For that the CRL is loaded on the server and correspondingly integrated into the content. To ensure that all VPN routers using the certificates of the certificate authority of the CRL will receive the CLR, it is necessary to set up such one on the respective VPN routers:

- Select the imported certificate authority,
- Select the certificate revocation list.

Now you have the choice between 2 options for loading the CRL:

1. You can load the CRL directly from your processor.
2. You enter the complete URL to the CRL.

When you configurate the automatic update via the network, you have the services of http, ftp, and

wget at your disposal. This means your URL could look like this:

http://www.msm-net.de/namecertificateauthority.crl

ftp://1.2.3.4/namecertificateauthority.crl

wget://hostname/namecertificateauthority.crl

If you have configurated an update via network, the CRL will be downloaded from the server every hour. This cycle can be changed according to your wishes on request.

It is also possible to import the CRL and set up the URL at the same time.

1.9. Certificate administration variant 2

In variant 2 of the certificate administration, the general administration rules of x509 certificates are in force. That means:

1. Set up request
2. Target-oriented signing of request
3. Export or import certificate in different formats.

In the interests of increased safety requirements compared with variant 1, the automatic password handling of the certificate administration has been dropped and instead a complete cryptosmartcard application has been integrated. This cryptosmartcard application can be used both for the CA administration and for the authentification of the connection locally and on remote machines. The requirements concerned with it are fixed in the respective connection definition. Furthermore, the independent administration structure makes it possible to import, set up, administrate and use within the router system any sub-CA structures.

2. Connection types with examples

2.1. Globals on VPN connections

It is possible to set up 3 different types of VPN connections.

The types are the following:

- bidirectional permanent,
- bidirectional on demand, and
- incoming.

Additionally a connection can be switched to inactive. Bidirectional (permanent and on-demand) connections are connections which can be set up between VPN routers. Incoming connections are connections which can be used between VPN routers as well as VPN routers and mobile clients. With it the following combinations – in excerpts – are possible:

router 1		router 2		use by
ip address	connection type	ipo address	connection type	
static	bidire. perman.	static	bidire. perman.	router to router
static	incoming	dynamic	bidire. perman.	router to router, router 2 i. e. with DSL
static	incoming	dynamic	bidire. on dem.	router to router router 2 i. e. with DSL

Correspondingly the list can also be continued in combinations with mobile clients. In case of connections with dynamic IP addresses, the settings of DPD (dead per detection) should particularly paid attention to! This option can be handled within the expert menu of a connection only. Possible options are:

- hold (recommended for routers with dynamic IP)
- clear (recommended for routeres with static IP and dynamic client).

See also 3.3.

If connections with certificate authentification are set up, then the following is to be considered:

Please select in the connection setup the certificate that is to be used. The subject of the partner certificate has to be entered into the input field beneath. Replacements with '*' are permissible. So the input could be as follows:

C=DE, ST=TH, L=Ort, O=Organistion, OU=*/Emain=*

On VPN routers with variant 2 of the certificate administration, this is one of several options!

If you want to use PSK for authentification, then please take the following into account:

The router tries to set off the ID via the DNS. If you want to avoid this, please put an @ before the ID inputs (e.g. @192.168.6.254).

2.2. Net to net connection with static ip address over ipsec native with PSK

name	values router 1	values router 2
connection typ	bidirect permanent	bidirect permanent
ESP	equal settings	
IKE	equal settings	
local port/protocol	only for L2TP connection over IPSEC. Values are dependet form WINDOWS version.	
remote port/protocol		
compression	equal settings	
peers ip, FQDN	IP or FQDN 1.1.1.1	IP or FQDN 1.1.1.2
authentification	Pre Shared Key using @192.168.6.254 @192.168.7.254	Pre Shared Key using @192.168.7.254 @192.168.6.254
IPSEC nativ	192.168.6.0/24 192.168.7.0/24	192.168.7.0/24 192.168.6.0/24
GRE over IPSEC		
filterrules	on demand	on demand

2.3. Net-to-net connection with static ip address over ipsec nativ with x509 certificates

name	values router 1	values router 2
connection typ	bidirect permanent	bidirect permanent
ESP	equal settings	
IKE	equal settings	
local port/protocol	only for L2TP connection over IPSEC. Values are dependet form WINDOWS version.	
remote port/protocol		
compression	equal settings	
peers ip, FQDN	IP or FQDN 1.1.1.1	IP or FQDN 1.1.1.2
authentification (certifikate variant 1)	certificate to apply certificate 1 subject certificate 2	certificate to apply certificate 2 subject certificate 1
IPSEC nativ	192.168.6.0/24 192.168.7.0/24	192.168.7.0/24 192.168.6.0/24
GRE over IPSEC		
filterrules	on demand	on demand

2.4. Net-to-net connection with a static and a dynamic ip address

name	values router 1	values router 2
connection typ	incoming	bidirect permanent
ESP	equal settings	
IKE	equal settings	
local port/protocol	only for L2TP connection over IPSEC. Values are dependet form WINDOWS version.	
remote port/protocol		
compression	equal settings	
peers ip, FQDN	IP or FQDN %any	IP or FQDN 1.1.1.2
authentification (certifikate variant 1)	certificate to apply certificate 1 subject certificate 2	certificate to apply certificate 2 subject certificate 1
IPSEC nativ	192.168.6.0/24 192.168.7.0/24	192.168.7.0/24 192.168.6.0/24
GRE over IPSEC		
filterrules	on demand	on demand

2.5. Net-to-net connection with 2 dynamic IP addresses (variant 1, with dynamic DNS)

If you use 2 or more VPN routers at DSL or ISDN interfaces and those do not have permanent IP addresses, it makes sense to register with a DNS service provider and to use from then on the registered FQDN for the configuration. For the dynamic DNS client configuration please select IP service providers within the service menu. In this way you can operate a complete VPN with mobile clients and dynamic IP addresses.

Please see the following table for more details.

name	values router 1	values router 2
connection typ	incoming	bidirect permanent
ESP	equal settings	
IKE	equal settings	
local port/protocol	only for L2TP connection over IPSEC. Values are dependet form WINDOWS version.	
remote port/protocol		
compression	equal settings	
peers ip, FQDN	IP or FQDN fqdnrouter2	IP or FQDN fqdnrouter1

authentification	certificate to apply certificate 1 subject certificate 2	certificate to apply certificate 2 subject certificate 1
IPSEC nativ	192.168.6.0/24 192.168.7.0/24	192.168.7.0/24 192.168.6.0/24
GRE over IPSEC		
filterrules	on demand	on demand

2.6. Net-to-net connection with 2 dynamic IP addresses (variant 2, with ISDN)

name	values router 1	values router 2
connection typ	bidirect permanent	bidirect permanent
ESP	equal settings	
IKE	equal settings	
local port/protocol	only for L2TP connection over IPSEC. Values are dependet form WINDOWS version.	
remote port/protocol		
compression	equal settings	
peers ip, FQDN	vpnrouter1.dyndns.org	vpnrouter2.dyndns.org
authentification	certificate to apply certificate 1 subject certificate 2	certificate to apply certificate 2 subject certificate 1
IPSEC nativ	192.168.6.0/24 192.168.7.0/24	192.168.7.0/24 192.168.6.0/24
GRE over IPSEC		
filterrules	on demand	on demand

2.7. Net-to-net connection with static IP addresses over ipsec-gre with x509 certificates

name	values router 1	values router 2
connection typ	bidirect permanent	bidirect permanent
ESP	equal settings	
IKE	equal settings	
local port/protocol	only for L2TP connection over IPSEC. Values are dependet form WINDOWS version.	
remote port/protocol		
compression	equal settings	
peers ip, FQDN	IP or FQDN 1.1.1.1	IP or FQDN 1.1.1.2
authentification	Pre Shared Key use @192.168.6.254 @192.168.7.254	Pre Shared Key use @192.168.7.254 @192.168.6.254
IPSEC nativ		
GRE over IPSEC	192.168.6.0/24 192.168.7.0/24 more options on demand	192.168.7.0/24 192.168.6.0/24 more options on demand
filterrules	on demand	on demand

2.8. Remote service connection

The maintenance service shall be carried out by the processor with the IP 192.168.6.10 via router 1 on router 2. Please don not forget that the processor needs a route to 192.168.7.254 via 192.168.6.254 (internal IP router 1)!

name	values router 1	values router 2
connection typ	bidirect permanent	bidirect permanent
ESP	equal settings	
IKE	equal settings	
local port/protocol	only for L2TP connection over IPSEC. Values are dependet form WINDOWS version.	
remote port/protocol		
compression	equal settings	
peers ip, FQDN	IP or FQDN 1.1.1.1	IP or FQDN 1.1.1.2
authentification	certificate to apply certificate 1 subject certificate 2	certificate to apply certificate 2 subject certificate 1

IPSEC nativ	192.168.6.10/32 192.168.7.254/32	192.168.7.254/32 192.168.6.10/32
GRE over Ipsec		
filterrules	on demand	on demand

2.9. Logtunnel connections

Logtunnel connections serve the VPN router for the purpose to store all log data parallel on a log server in a SQL data bank. For this you enter the IP address of the log server (e.g. 192.168.6.2) into the page “Globals“. This address shall be accessible for VPN router 2 via VPN router 1 in the following configuration example.

name	values router 1	values router 2
connection typ	bidirect permanent	bidirect permanent
ESP	equal settings	
IKE	equal settings	
local port/protocol	only for L2TP connection over IPSEC. Values are dependet form WINDOWS version.	
remote port/protocol		
compression	equal settings	
peers ip, FQDN	IP or FQDN 1.1.1.1	IP or FQDN 1.1.1.2
authentification	certificate to apply certificate 1 subject certificate 2	certificate to apply certificate 2 subject certificate 1
IPSEC nativ	192.168.6.2/32 192.168.7.254/32	192.168.7.254/32 192.168.6.2/32
GRE über Ipsec		
filterrules	on demand	on demand

3. Configuration examples and parameters

3.1. Setup parameter

Parameter	Description	Value	Comment	USE
also	Bind all settings from the section	sectionname		
interfaces	Allocation virtual – real interface	<virtual>=<real>|%defaultroute (quoted string)		
forwardcontrol	Whether *setup* should turn IP forwarding on	yes|no		
syslog	To using Syslog-facility	facility.level facilities: auth, authpriv, cron, daemon, kern, lpr, mail, news, syslog, user, uucp and local(0-7) levels: debug, info, notice, warning, err, crit, alert, emerg		
klipsdebug	IPSEC - Debuging	tunnel, tunnel-xmit, pfkey, xform, eroute, spi, radij, esp, ah, ipcomp, verbose (to find in /proc/net/ipsec_klipsdebug) -> spezial: all, none		
plutodebug	IKE - Debuging	raw, crypt, parsing, emitting, control, lifecycle, klips, dns, private, nat_t -> spezial: all, none		
dumpdir	Directory for Core-Dump	Pathname		
dump	Core-Dump	no|yes		
manualstart	Which manually-keyed connections to set up at startup. (Default is none)	Sectionsliste (quoted String)		
pluto	Start Pluto	yes|no		
plutoload	List of loadable connection by Pluto start	Sectionslist (quoted String) -> special: %search (all connection with auto= add|route|start)		
plutostart	List of to loaded connection by Pluto startup	Sectionslist (quoted String) -> special: %search (all connection with auto= route|start)		
plutowait	Should Pluto wait for each negotiation attempt that is part of startup to finish before proceeding with the next?	yes|no (default)		
plutobackgroundload	ignored (old)			
prepluto	Shell command to run before starting Pluto	Path to script		
postpluto	Shell command to run after starting Pluto	Path to script		
fragicmp	Whether a tunnel's need to fragment a packet should be reported back with an ICMP message, in an attempt to make the sender lower his PMTU estimate.	yes (default) |no		
no_eroute_pass	limited version from 'packetdefault', is ignored if 'packetdefault' define	yes -> packetdefault=pass no -> packetdefault=drop		
opportunistic	opportunistic encryption	yes | no (default)		
hidetos	Whether a tunnel packet's TOS field should be set to 0 rather than copied from the user packet inside.	yes (default) |no		

Parameter	Description	Value	Comment	USE
uniqueids	Whether a particular participant ID should be kept unique, with any new (automatically keyed) connection using an ID from a different IP address deemed to replace all old ones using that ID	yes|no		
packetdefault	Verfahrensweise für Packete, die in ein virtuelles IPSEC-Interface gelangen und keine eroute haben	pass|drop|reject		
overridemtu	Value that the MTU of the ipsec*n* interface(s) should be set to, overriding IPsec's (large) default.	Integer (MTU-Wert)		
nocrsend	Send none Certificate-Request by connection establishment	yes|no		
strictcrlpolicy	Stricly check user-certifikates per CRL	yes|no (If yes, it must exist a valid CRL. If no and CRL with revoked Certificates is exist)		
crlcheckinterval	Interval time for CRL check	Integer (long) (seconds)		
nat_traversal	Enable NAT-T patches (ESP in UDP)	yes|no		
keep_alive	Time between keepalive -packetes	Integer (Seconds)		
force_keepalive	Enforce keepalive -packetes	yes|no		
disable_port_floating		yes|no		
virtual_private	system global 'private net list'	Expl.: virtual_private=%v4:10.0.0.0/8,%v4:172.16.0.0/12,%v4:192.168.0.0/16,%v4:!192.168.2.0/24,%v4:!192.168.15.128/25		
xauth	Authentification User/Password with PAM (/etc/pam.d/pluto)	yes|no		

3.2. **Connection globals**

Parameter	Description	Value	Comment	USE
also	Include option from the actual sections.	Sectionname		
type	Connection typ	tranport|tunnel|passthrough(only manual-mode)		
authby	Authentification per	secret|rsasig		
_plutodevel	only for develop			
left-/right	Address	<ipadress>|%any|%opportunistic		
left-/rightsubnet	Net to tunneling	left=<netadress>|%defaultroute right=<netadress>|%any|%vhost vhost: %no (no virtual IP, accept public IP) %dhcp (accept DHCP SA of affected IP [not impl] %ike = accept affected IKE Config Mode IP [not impl] %priv = accept system-wide private net list %v4:x = accept ipv4 in list 'x' %v6:x = accept ipv6 in list 'x' %all = accept all ips [only for testing]		
left-/rightprotoport	Protocol/port for IPSEC-SA	<Protokollname/-nummer>/(<Portnummer>) %any als Wildcard		
leftnexthop	Route IPSEC-packetes via ...	<ipadress>|%defaultroute|%direct		
leftfirewall	If host connection firewalled, create a forward rules	yes|no		
leftupdown	By change the conncetion status start the script	Pfath to script + argumentes (quoted String)		
esp	Encryptions-/Authentifications - algorithmen	enc-auth(!) enc: 3des|cast128|aes(128..256)| blowfish(128..256)| twofish(128..256)| serpent(128..256) auth: md5|sha|sha2_256|sha2_512 !: exclusive, don't to agree to another mode		
ah	Authentifications - algorithmen	auth(!) auth: md5|sha|sha2_256|sha2_512 !: exclusive, don't to agree to another mode		

3.3 connection - auto-keyed parameter

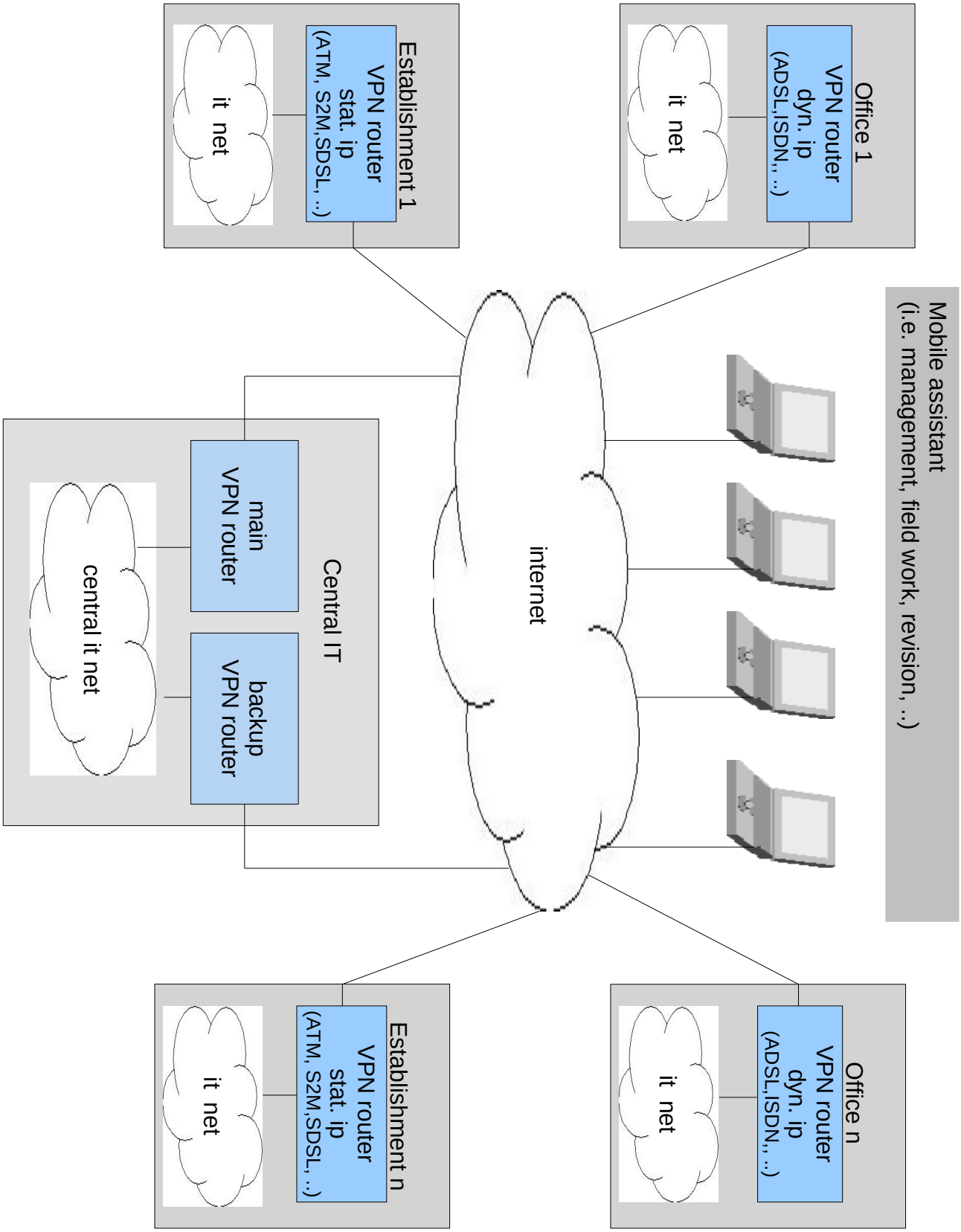
Parameter	Description	Value	Comment	USE
auto	Operation by startup	add|route|start|ignore		
keyexchange	Methode to keyexchange	ike		
auth	Protocol for authentification	esp|ah		
pfs	Perfect Forward Secrecy of keys	yes|no		
pfsgroup	PFS-Gruppe, if pfs=yes	modp(768,1024,1536,2048,3072,4096,6144,8192)		
keylife	how long a particular instance of a connection (a set of encryption/authentication keys for user packets) should last, from successful negotiation to expiry	Ganzzahl, followed from s(seconds)|m(minutes)|h(hours), max 24h		
rekey	Whether a connection should be renegotiated when it is about to expire.	yes|no		
rekeymargin	How long before connection expiry or keying-channel expiry should attempts to negotiate a replacement begin.	Integer, followed s(Seconds)| m(Minutes)|h(Hours)		
rekeyfuzz	Maximum percentage by which rekeymargin should be randomly increased to randomize rekeying intervals (important for hosts with many connections).	Integer% (value with percent character)		
dpddelay	Set the delay (in seconds) between Dead Peer Dectection	Integer (Seconds)		
dpdtimeout	Set the length of time	Integer (Seconds)		
dpdaction	When a DPD enabled peer is declared dead, what action should be taken.	hold|clear|restart		
aggrmode	Use aggressive mode ISAKMP negotiation.	yes|no		
xauth	(not used from us)			
compress	whether IPComp compression of content is proposed on the connection (link-level compression does not work on encrypted data, so to be effective, compression must be done *before* encryption)	yes|no (default)		
keyingtries	How many attempts (a whole number or %forever) should be made to negotiate a connection, or a replacement for one, before giving up (default %forever).	The value %forever means ``never give up'' (obsolete: this can be written 0)		
ikelifetime	how long the keying channel of a connection (buzzphrase: ``ISAKMP SA'') should last before being renegotiated	Integer, followed s(seconds)| m(minutes)|h(hours), max 8h		
disablearrivalcheck	Whether KLIPS's normal tunnel-exit check (that a packet emerging from a	yes|no (default)		

Parameter	Description	Value	Comment	USE
	tunnel has plausible addresses in its header) should be disabled.			
ike	Encryptions-/Authentifications - Algorithmen Bitlenght DH (Diffi Hellmann)	enc-auth(-dh)(!) enc: 3des|cast128|aes(128..256)|blowfish(128..256)|twofish(128..256)|serpent(128..256) auth: md5|sha|sha2_256|sha2_512 dh: modp(768,1024,1536,2048,3072,4096,6144,8192) !: exlusive, don't to agree to another mode		
lifetime	old for 'keylife'			
rekeystart	old for 'rekeymargin'			
rekeytries	Counter of rekeying.	Integer (0 = never ending)		
left-/rightrsasigkey	The left/right participant's public key for RSA signature authentication	<rsakey>|%cert|%none|%dnsondemand|%dnsonload		
left-/rightrsasigkey2	If present, a second public key	<rsakey>|%cert|%none|%dnsondemand|%dnsonload		
left-/rightid	Peers ID	<ip>|<fqdn>|@<user_fqdn>|<distinguished name>		
left-/rightcert	Certificate to use (PEM-Format)	<path relativ to /etc/ipsec.d/>		
rightca	CA-Certificate for use to authentification from the Certificates	<distinguished name>|%same|(wenn nicht spezifizier, alle verfügbaren CA's)		
rightsubnetwithin	Remote-subnet	<net adress>		

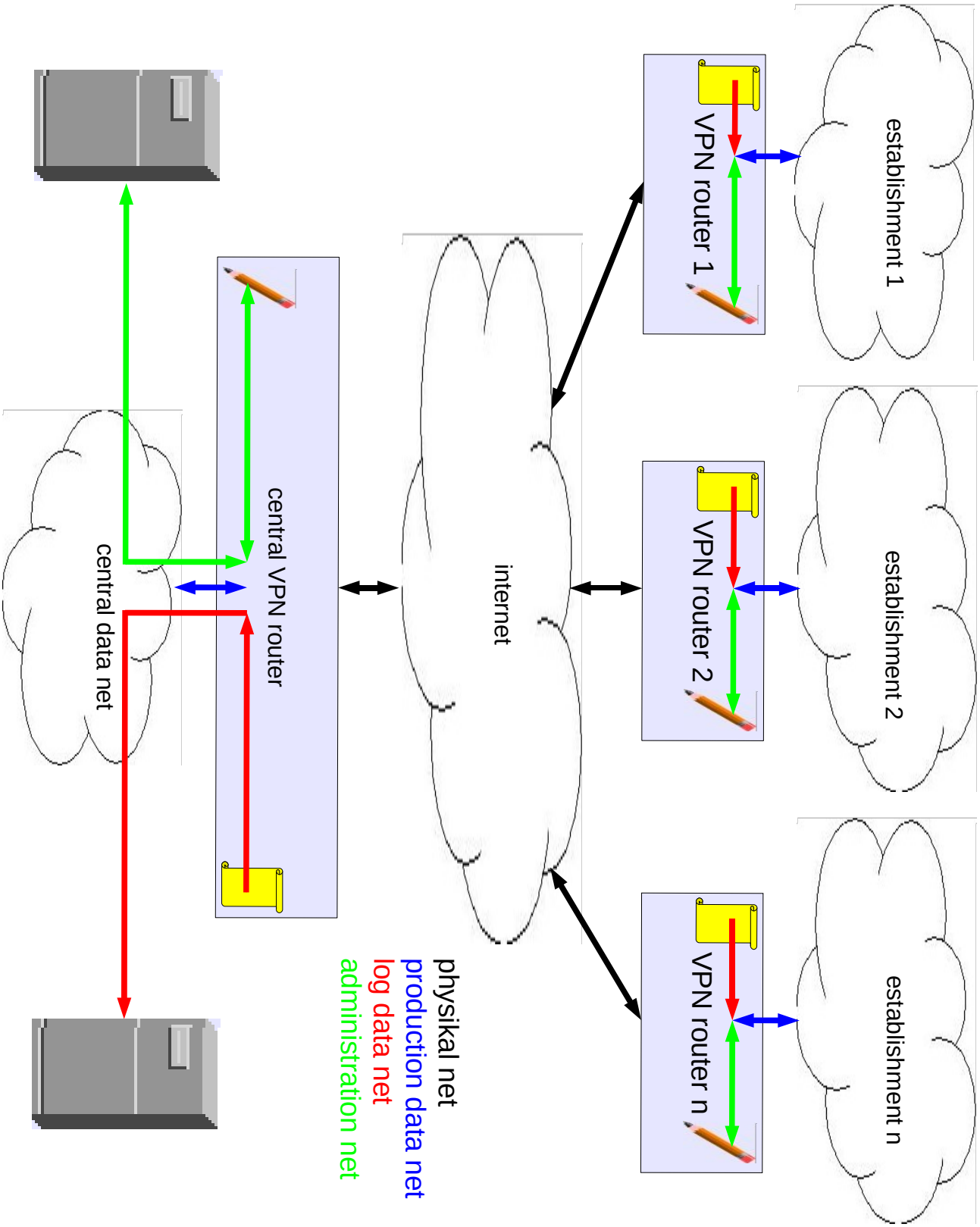
3.4. connection – manual-keyed-parameter

Parameter	Description	Value	Comment	USE
spibase	The base number for the SPIs to be used for the connection (in/out)(excl. or 'spi')	numbers in the range 0x100-0xff0		
spi	Use SPI-number for all SA's (excl.or 'spibase')	Hexzahl (3 Stellen) 0x... (empfohlen 0x100-0xfff)		
left-/rightespspi	SPI to be used for the leftward/rightward ESP SA, overriding automatic assignment using spi or spibase	Hexzahl 0x...		
left-/rightahspi	SPI to be used for the leftward/rightward AH SA, overriding automatic assignment using spi or spibase	Hexzahl 0x...		
(left/right/-)espenckey	ESP encryption key	valid key (Bitlenght) in hex-form: 0x...		
(left/right/-) espauthkey	ESP authentication key	valid key (Bitlenght) in hex-form: 0x...		
espreplay_window	ESP replay-window setting	Integer between 0..64		
(left/right/-)ahkey	AH authentication key	valid key (Bitlenght) in hex-form: 0x...		
ahreplay_window	AH replay-window setting	Integer between 0..64		

4. Topologie structurgram (example)
4.1. Centralizesed VPN (topologie)



4.2. Logical topologie from a centralizesed VPN



4.3. Centralizesed administration