- Technical Whitepaper -

Konfigurationsbeispiele

von

VPN Routern

msm net ingenieurbüro meissner
Am Porstendorferweg 4
07570 Niederpöllnitz

Inhaltsverzeichnis:

1. x509 Zertifikatverwaltung

1.1. Grundsätzliches zur Nutzung der Zertifikatverwaltung

Jeder VPN Router von msm net ingenieurbüro meissner ist mit einer kompletten x509 Zertifikatverwaltung ausgestattet.

Variante 1

Mit dieser Zertifikatverwaltung können beliebig viele Zertifizierungsstellen (Root CA) erstellt und administriert werden. Weiterhin können beliebig viele Benutzerzertifikate erstellt werden. Die Erstellung eines Benutzerzertifikates erfolgt derart, dass das erstellte Benutzerzertifikat automatisch zu durch die zugeordnete Zertifizierungsstelle (Root CA) signiert wird. D.h. ein Benutzerzertifikat kann sofort nach der Erstellung verwendet werden. Durch die hierariche Verbindung von Zertifizierungsstelle und Benutzerzertifikat kann sich jedes Unternehmen eine einfache, eigenständige, gültige und vor allem kostenfreie PKI erstellen und betreiben.

Variante2

Mit dieser Zertifikatverwaltung können beliebig viele Request und Zertifikate (RootCA, SubCA und Ident-Zertifikate) erstellt und signiert werden. Durch die Integration einer CryptoSmartcard Applikation (z.Z. eToken von Aladdin) können hochsichere PKI Strukturen realisiert werden. Analog zu der Variante 1 sind umfangreiche Export- und Importfunktionen realisiert.

In beide Varianten sind komplexe CRL Applikationen (Erstellung, Import, Export und automatische Abholung) integriert. In der Signierung von RootCA's der Variante 2 ist gleichzeitig die Integration der OCSP (Online Certificat Status Protocol) realisiert.

1.2. Erstellung einer Zertifizierungsstelle (CA Variante 1)

Nach erfolgreicher Anmeldung am VPN Router als Administrator wechseln Sie in das Menü VPN Verbindungen und dort zu Zertifikatverwaltung. In dieser Seite bekommen Sie im linken Teil alle bestehenden Zertifizierungsstellen angezeigt. Im rechten Teil werden Ihnen weitere Optionen angeboten. Mit dem Klick auf die Taste „Zertifizierungsstelle anlegen“ wird eine neue Seite aufgerufen. In dieser neuen Seite sind Sie aufgefordert, alle Daten für die Erstellung einer neuen Zertifizierungsstelle einzugeben. Alle Eingaben die Sie tätigen werden vor der Erstellung einer Zertifizierungsstelle auf zulässige Zeichen und Länge geprüft. Mit dem Betätigen der Taste „Speichern“ und der Gültigkeit Ihrer Eingaben wird eine neue Zertifizierungsstelle angelegt. In der Liste der Zertifizierungsstellen steht nun der von Ihnen vergebene Name der neuen Zertifizierungsstelle. Mit dem Klick auf den Namen und dem Drücken der Taste „Zertifizierungsstelle Details“ können Sie die Root CA sich anzeigen lassen. Wenn Sie in diesem Fenster nach unten blättern steht dann auch eine Zeile die lautet: CA:TRUE

Daran erkennen Sie, dass es sich um eine Zertifizierungsstelle handelt.

1.3. Erstellung von Benutzerzertifikaten (Variante 1)

Wollen Sie ein neues Benutzerzertifikat erstellen, so wählen Sie zunächst in der Übersicht der Zertifizierungsstellen eine Zertifizierungsstelle aus, in der ein neues Benutzerzertifikat erstellt werden soll. Als nächstes klicken Sie die Taste „Zertifizierungsstelle auswählen“.

Wurde die Zertifizierungsstelle auf diesem VPN Router erstellt können Sie jetzt Benutzerzertifikate erstellen. Ist der VPN Router nicht der Router auf dem die Zertifizierungsstelle erstellt wurde, d.h. es erfolgte ein Zertifikatsimport, stehen Ihnen einige weitere Funktionen nicht zur Verfügung. Mit der Auswahl eines ggf. schon vorhandenen Zertifikates können Sie sich dieses auch im Detail anzeigen lassen. Mit dem Klick auf „Neues Zertifikat erstellen“ erscheint eine neue Seite, in der Sie die benötigten Daten zur Erstellung eines Benutzerzertifikates eingeben. Mit dem Speichern wird bei Gültigkeit der Daten (Prüfung erfolgt automatisch) ein neues Benutzerzertifikat erstellt. In der Liste der Zertifikate der Zertifizierungsstelle steht nun der Name des neuen Zertifikates.

1.4. Sperren eines Benutzerzertifikates (Variante 1)

Sollte es aus irgend einem Grund notwendig sein, dass ein Benutzerzertifikat gesperrt werden muss, so wählen Sie das Zertifikat in der Liste durch anklicken bitte aus. Als zweiten Schritt betätigen Sie bitte die Taste „Ausgewähltes Zertifikat sperren“.

Im nächsten Schritt werden Sie noch einmal gefragt, ob Sie dieses Zertifikat wirklich sperren wollen. Wenn Sie sicher sind bestätigen Sie bitte die Frage. Daraufhin wird das Zertifikat gesperrt. In der Darstellung erkennt man das dadurch, das vor dem Namen des Benutzerzertifikates eine '#' steht und die gesamte Zeile in rot dargestellt wird. Mit dem Sperren eines Zertifikates wird automatisch eine neue CRL (Zertifikatssperrliste) erstellt. Diese Liste können Sie durch einen Klick auf die Taste „Zertifikatssperrliste“ aufrufen. In dieser sehen Sie dann alle gesperrten Benutzerzertifikate der Zertifizierungsstelle mit Details gelistet.

1.5. Export von Benutzerzertifikaten (Variante 1)

Damit Sie die von Ihnen erstellten Zertifikate auch auf anderen Maschinen nutzen können müssen Sie diese exportieren. Dafür gehen Sie wie folgt vor. Rufen Sie die Seite der Zertifizierungsstellen auf und wählen Sie "Zertifizierungsstelle auswählen“. Als nächstes wählen Sie „Zertifikate exportieren“. Darauf bekommen Sie eine Seite angezeigt, in der Ihnen alle Zertifikate der Zertifizierungsstelle zum Export angezeigt werden. Wählen Sie bitte die Zertifikate aus, die Sie exportieren möchten und geben Sie bitte das entsprechende Passwort ein. Sollten Sie für alle Zertifikate das selbe Passwort gewählt haben, so können Sie auch die entsprechende Sammelfunktion verwenden. Haben Sie Ihre Eingaben abgeschlossen, so betätigen Sie bitte die Taste „weiter“. In dem folgenden Fenster bekommen Sie nun alle ausgewählten Zertifikate zum herunterladen im PKCS12- Format angeboten.

Klicken Sie bitte mit der Context-Taste (rechte Maustaste) auf das jeweilige Zertifikat und wählen bitte speichern unter .... . Alle so gespeicherten Zertifikate können nun problemlos auf den jeweiligen Ziel- VPN-Routern importiert werden. Auch ein Import auf anderen Systemen (z.B. Windows X, Linux, ..) ist in diesem Dateiformat möglich, da alle benötigten Daten zur Benutzung eines Zertifikates in diesen Dateien enthalten sind.

1.6. Import von x509 Zertifikaten im pkcs12 - Format (Variante 1)

Für dem Import eines exportierten oder anderen Zertifikates im PKCS12 Format klicken Sie bitte „Fremdzertifikate importieren (PKCS12)“ auf der Seite der Zertifizierungsstellen. Geben Sie bitte die geforderten Daten in das Formular ein und klicken anschließend auf „importieren“. Durch den Import wird eine vollständige Zertifizierungsstelle und das zugeordnete Benutzerzertifikat angelegt. Sie können mehrere Benutzerzertifikate in eine Zertifizierungsstelle importieren. Voraussetzung ist, dass diese Benutzerzertifikate von einer Zertifizierungsstelle signiert worden sind. Ist dies nicht der Fall wird eine neue Zertifizierungsstelle angelegt. Wählen Sie die neu angelegte (Import-) Zertifizierungsstelle aus, so sehen Sie, dass nur ein Teil der Funktionen einer normalen Zertifizierungsstelle zur Verfügung steht. Wenn Sie die Mechanismen der CRL Verwaltung nutzen wollen, so müssen Sie diese noch einrichten.

1.7. Erstellung einer CRL und deren Export (Variante 1)

Jede Zertifizierungsstelle mit der Sie Benutzerzertifikate erstellen können besitzt eine Zertifikatssperrliste (CRL). Diese CRL wird automatisch mit der Generierung der Zertifizierungsstelle erstellt. Beim Anlegen der Zertifizierungsstelle geben Sie den Zyklus in Tagen an, wann eine neue CRL erstellt werden soll. Immer nach Ablauf dieses Zyklus wird automatisch eine neue CRL der Zertifizierungsstelle auf dem VPN Router erstellt.

Weiterhin wird unabhängig von diesem Zyklus eine neue CRL durch die Sperrung eines Benutzerzertifikates erstellt. Die CRL kann von dem erstellenden VPN Router zur weiteren

Verwendung heruntergeladen werden. Dazu gehen Sie wie folgt vor:

- Wählen Sie die Zertifizierungsstelle aus
- Wählen Sie Zertifikatssperrliste
- Wählen Sie Exportieren

Damit wird die Zertifikatssperrliste auf Ihren lokalen Rechner geladen und steht Ihnen zur weiteren Verwendung zur Verfügung.

1.8. Veröffentlichung und Nutzung einer CRL (Variante 1)

Die Zertifikatssperrliste kann auf einem Web-oder Ftpserver im Internet veröffentlicht werden. Dazu wird die CRL auf den Server geladen und in den Content entsprechend eingebunden. Damit alle VPN Router, die Zertifikate der Zertifizierungsstelle der CRL nutzen, die CLR erhalten, muss dies auf diesen VPN Routern eingerichtet werden.

- Wählen Sie die importierte Zertifizierungsstelle aus
- Wählen Sie Zertifikatssperrliste

Nun stehen Ihnen 2 Möglichkeiten zum laden der CRL zur Verfügung:

1. Sie können die CRL direkt von Ihrem Rechner laden

2. Sie geben die komplette URL zu der CRL ein.

Wenn Sie das automatische Update über Netzwerk konfigurieren, so stehen Ihnen die Dienste http, ftp und wget zur Verfügung. Dies bedeutet Ihre URL könnte wie folgt aussehen:

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

ftp://1.2.3.4/zertifizierungsstellenname.crl

wget://hostname/zertifizierungsstellenname.crl

Haben Sie ein Update über Netzwerk konfiguriert, so wird stündlich die CRL von dem Server geladen. Auf Anforderung kann dieser Zyklus beliebig verändert werden.

Sie können die CRL auch importieren und gleichzeitig die URL einrichten.

1.9. Zertifikatadministration in der Variante 2

In der Variante 2 der Zertifikatsverwaltung gelten die allgemeinen Administrationsregeln von x509 Zertifikaten. Dies heisst:

1. Request erstellen
2. Request zielorientiert signieren
3. Zertifkate exportieren bzw. importieren in verschiedenen Formaten

Im Interesse von erhöhten Sicherheitsanforderungen gegenüber der Variante 1 entfällt das automatische Passworthandling der Zertifikatsadministration und es wurde eine komplette Cryptosmartcardapplikation integriert. Die Cryptosmartcardapplikation kann für die CA Administration als auch zur Verbindungsauthendifizierung lokal und auf remote Maschinen genutzt werden. Dies entsprechenden Anforderungen werden in der jeweiligen Verbindungsdefinition getroffen. Weiterhin ist es durch die freie Administrationsstruktur möglich beliebige Sub-CA Strukturen zu importieren, zu erstellen, zu administrieren und in dem Routersystem zu nutzen.

2. Verbindungsarten mit Beispielen

2.1. Grundsätzliches zu VPN Verbindungen

Es ist möglich 3 verschiedene Arten von VPN Verbindungen einzurichten.

Die Arten sind:

- bidirektional permanent,

- bidirektional on demand und

- eingehend.

Zusätzlich kann eine Verbindung noch inaktiv geschalten werden. Bidirektionale (permanet und on demand) Verbindungen sind Verbindungen die zwischen VPN Routern aufgebaut werden können. Eingehende Verbindungen sind Verbindungen, die zwischen VPN Routern sowie VPN Routern und mobilen Client genutzt werden können. Damit ergeben sich auszugsweise nachfolgende Kombinationen:

Router1		Router 2		Anwendung bei
IP Adresse	Verbindungsart	IP Adresse	Verbindungsart	
fest	bidire. perman.	fest	bidire. perman.	Router zu Router
fest	eingehend	dynam.	bidire. perman.	Router zu Router, Router2 z.B. mit DSL
fest	eingehend	dynam.	bidire. on dem.	Router zu Router Router2 z.B. mit DSL

Entsprechend lässt sich die Liste in Kombinationen auch mit mobilen Clients fortsetzen. Werden Verdindungen mit dynamischen IP Adressen betrieben, so ist insbesondere auf die Einstellungen von DPD (dead peer detection) zu achten! Diese Option kann nur im Expertenmenü einer Verbindung bearbeitet werden. Mögliche Optionen sind:

- hold (zu empfehlen für Router mit dynamischer IP)

- clear (zu empfehlen für Router mit statischer IP und dynamischen Client)

Siehe hierzu auch 3.3.

Werden Verbindungen mit Zertifikatauthentifizierung eingerichtet, so ist folgendes zu beachten:

In der Verbindungseinrichtung wählen Sie bitte das zu verwendende Zertifikat aus. In dem darunter stehenden Eingabefeld muß das Subject des Partnerzertifikates eingetragen werden. Ersetzungen durch '*' sind dabei zulässig. Somit könnte folgende Eingabe erfolgen:

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

Auf VPN-Router mit Variante 2 der Zertifikatverwaltung ist dies eine von mehreren Möglichkeiten!

Wollen Sie PSK zur Authentifikation verwenden, so sollten Sie folgendes beachten:

Der Router versucht die ID über den DNS auszulösen. Wenn Sie dies vermeiden wollen setzen Sie ein @ vor die ID Einträge. (z.B. @192.168.6.254)

2.2. Netzwerk zu Netzwerk Verbindung mit statischen IP Adressen über ipsec nativ mit PSK

Feldname	Wert Router1	Wert Router 2
Verbindungstyp	bidirektional permanent	bidirektional permanent
ESP	Gleiche Einstellungen	
IKE	Gleiche Einstellungen	
Local Port/Protokoll	Gilt nur für L2TP Verbindungen über IPSEC und ist abhängig von verwendeten Windows	
Remote Port/Protokoll		
Kompression	Sollte gleich eingestellt sein	
Partner IP, FQDN	IP oder FQDN 1.1.1.1	IP oder FQDN 1.1.1.2
Authendifizierung	Pre Shared Key verwenden @192.168.6.254 @192.168.7.254	Pre Shared Key verwenden @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 über Ipsec		
Filterregel	Nach Anforderung	Nach Anforderung

2.3. Netzwerk zu Netzwerk Verbindung mit statischen IP Adressen über ipsec nativ mit x509

Feldname	Wert Router1	Wert Router 2
Verbindungstyp	bidirektional permanent	bidirektional permanent
ESP	Gleiche Einstellungen	
IKE	Gleiche Einstellungen	
Local Port/Protokoll	Gilt nur für L2TP Verbindungen über IPSEC und ist abhängig von verwendeten Windows	
Remote Port/Protokoll		
Kompression	Sollte gleich eingestellt sein	
Partner IP, FQDN	IP oder FQDN 1.1.1.1	IP oder FQDN 1.1.1.2
Authendifizierung (Bei Zertifikatvariante 1)	Zertifikat verwenden Zertifikat1 Subject Zertifikat2	Zertifikat verwenden Zertifikat2 Subject Zertifikat1
Ipsec nativ	192.168.6.0/24 192.168.7.0/24	192.168.7.0/24 192.168.6.0/24
GRE über Ipsec		
Filterregel	Nach Anforderung	Nach Anforderung

2.4. Netzwerk zu Netzwerk Verbindung mit einer statischen und einer dynamischen IP Adresse

Feldname	Wert Router1	Wert Router 2
Verbindungstyp	eingehend	bidirektional permanent
ESP	Gleiche Einstellungen	
IKE	Gleiche Einstellungen	
Local Port/Protokoll	Gilt nur für L2TP Verbindungen über IPSEC und ist abhängig von verwendeten Windows	
Remote Port/Protokoll		
Kompression	Sollte gleich eingestellt sein	
Partner IP, FQDN	IP oder FQDN %any	IP oder FQDN 1.1.1.2
Authendifizierung (Bei Zertifikatvariante 1)	Zertifikat verwenden Zertifikat1 Subject Zertifikat2	Zertifikat verwenden Zertifikat2 Subject Zertifikat1
Ipsec nativ	192.168.6.0/24 192.168.7.0/24	192.168.7.0/24 192.168.6.0/24
GRE über Ipsec		
Filterregel	Nach Anforderung	Nach Anforderung

2.5. Netzwerk zu Netzwerk Verbindung mit 2 dynamischen IP Adressen (Variante 1, mit dynamischen DNS)

Betreiben Sie 2 oder mehrere VPN Router an DSL oder ISDN Schnittstellen und haben diese keine festen IP Adressen, so macht es Sinn sich bei einem DNS Dienstleister zu registrieren und in der Folge die registrierten FQDN für die Konfigurartion zu nutzen. Für die dyn. DNS Client Konfiguration wählen Sie bitte im Servicemenu IP Dienstleister aus. Auf diese Art und Weise können Sie ein komplettes VPN mit mobilen Clients und dynamischen IP Adressen betreiben.

Für weitere Details

sehen Sie bitte die folgende Tabelle.

Feldname	Wert Router1	Wert Router 2
Verbindungstyp	bidirektional permanent	bidirektional permanent
ESP	Gleiche Einstellungen	
IKE	Gleiche Einstellungen	
Local Port/Protokoll	Gilt nur für L2TP Verbindungen über IPSEC und ist abhängig von verwendeten Windows	
Remote Port/Protokoll		
Kompression	Sollte gleich eingestellt sein	

Partner IP, FQDN	IP oder FQDN fqdnrouter2	IP oder FQDN fqdnrouter1
Authendifizierung	Zertifikat verwenden Zertifikat1 Subject Zertifikat2	Zertifikat verwenden Zertifikat2 Subject Zertifikat1
Ipsec nativ	192.168.6.0/24 192.168.7.0/24	192.168.7.0/24 192.168.6.0/24
GRE über Ipsec		
Filterregel	Nach Anforderung	Nach Anforderung

2.6. Netzwerk zu Netzwerk Verbindung mit 2 dynamischen IP Adressen (Variante 2, mittels ISDN)

Feldname	Wert Router1	Wert Router 2
Verbindungstyp	bidirektional permanent	bidirektional permanent
ESP	Gleiche Einstellungen	
IKE	Gleiche Einstellungen	
Local Port/Protokoll	Gilt nur für L2TP Verbindungen über IPSEC und ist abhängig von verwendeten Windows	
Remote Port/Protokoll		
Kompression	Sollte gleich eingestellt sein	
Partner IP, FQDN	vpnrouter1.dyndns.org	vpnrouter2.dyndns.org
Authendifizierung	Zertifikat verwenden Zertifikat1 Subject Zertifikat2	Zertifikat verwenden Zertifikat2 Subject Zertifikat1
Ipsec nativ	192.168.6.0/24 192.168.7.0/24	192.168.7.0/24 192.168.6.0/24
GRE über Ipsec		
Filterregel	Nach Anforderung	Nach Anforderung

2.7. Netzwerk zu Netzwerk Verbindung mit statischen IP Adressen über ipsec-gre mit x509

Feldname	Wert Router1	Wert Router 2
Verbindungstyp	bidirektional permanent	bidirektional permanent
ESP	Gleiche Einstellungen	
IKE	Gleiche Einstellungen	
Local Port/Protokoll	Gilt nur für L2TP Verbindungen über IPSEC und ist abhängig von verwendeten Windows	
Remote Port/Protokoll		
Kompression	Sollte gleich eingestellt sein	
Partner IP, FQDN	IP oder FQDN 1.1.1.1	IP oder FQDN 1.1.1.2
Authendifizierung	Pre Shared Key verwenden @192.168.6.254 @192.168.7.254	Pre Shared Key verwenden @192.168.7.254 @192.168.6.254
Ipsec nativ		192.168.7.0/24 192.168.6.0/24
GRE über Ipsec	192.168.6.0/24 192.168.7.0/24 weitere Optionen n. Bedarf	192.168.7.0/24 192.168.6.0/24 weitere Optionen n. Bedarf
Filterregel	Nach Anforderung	Nach Anforderung

2.8. Remote Wartungsverbindungen

Die Wartung soll von dem Rechner mit der IP 192.168.6.10 über den Router1 auf dem Router2 durchgeführt werden. Vergessen Sie bitte nicht, das der Rechner eine Route zu 192.168.7.254 über 192.168.6.254 (interne IP Router1) benötigt.

Feldname	Wert Router1	Wert Router 2
Verbindungstyp	bidirektional permanent	bidirektional permanent
ESP	Gleiche Einstellungen	
IKE	Gleiche Einstellungen	
Local Port/Protokoll	Gilt nur für L2TP Verbindungen über IPSEC und ist abhängig von verwendeten Windows	
Remote Port/Protokoll		
Kompression	Sollte gleich eingestellt sein	
Partner IP, FQDN	IP oder FQDN 1.1.1.1	IP oder FQDN 1.1.1.2
Authendifizierung	Zertifikat verwenden	Zertifikat verwenden

	Zertifikat1 Subject Zertifikat2	Zertifikat2 Subject Zertifikat1
Ipsec nativ	192.168.6.10/32 192.168.7.254/32	192.168.7.254/32 192.168.6.10/32
GRE über Ipsec		
Filterregel	Nach Anforderung	Nach Anforderung

2.9. Logtunnelverbindungen

Logtunnelverbindungen dienen dem VPN Router dazu, dass alle Logeinträge parallel auf einem Logserver in einer SQL Datebank gespeichert werden. Dazu geben Sie in der Seite Allgemein die IP Adresse des Logservers ein. (z.B. 192.168.6.2). Diese Adresse soll in dem folgendem Konfigurationsbeispiel für den VPN Router2 über den VPN Router1 erreichbar sein.

Feldname	Wert Router1	Wert Router 2
Verbindungstyp	bidirektional permanent	bidirektional permanent
ESP	Gleiche Einstellungen	
IKE	Gleiche Einstellungen	
Local Port/Protokoll	Gilt nur für L2TP Verbindungen über IPSEC und ist abhängig von verwendeten Windows	
Remote Port/Protokoll		
Kompression	Sollte gleich eingestellt sein	
Partner IP, FQDN	IP oder FQDN 1.1.1.1	IP oder FQDN 1.1.1.2
Authendifizierung	Zertifikat verwenden Zertifikat1 Subject Zertifikat2	Zertifikat verwenden Zertifikat2 Subject Zertifikat1
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		
Filterregel	Nach Anforderung	Nach Anforderung

3. Konfigurationsoptionen von VPN Verbindungen

3.1. Setup Parameter

Parameter	Beschreibung	Wert	Kommentar	USE
also	Bindet alle Angaben einer anderen Sektion in die aktuelle mit ein	Name eine anderen Sektion		
interfaces	Zuordung(en) virtuelles – reales Interface	<virtual>=<real>| %defaultroute (quoted string)		
forwardcontrol	Soll Forwarding aktiviert werden, falls noch nicht aktiv	yes|no		
syslog	Zu benutende 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 (zu finden 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	Verzeihnis für Core-Dump	Pfadangabe		
dump	Core-Dump	no|yes		
manualstart	Zu startende Verbindungen im manual mode	Sektionsliste (quoted String)		
pluto	Soll Pluto gestartet werden	yes|no		
plutoload	Verbindungen, die Pluto beim Start laden soll	Sektionslist (quoted String) -> spezial: %search (alle Verbindungen mit auto= add|route|start)		
plutostart	Verbindungen, die Pluto beim Start starten soll	Sektionslist (quoted String) -> spezial: %search (alle Verbindungen mit auto= route|start)		
plutowait	Soll Pluto warten, bis eine Verbindung fertig ausgehandelt ist, bis die nächste gestartet wird.	yes|no		
plutobackgroundload	ignored (veraltet)			
prepluto	shell-command, das vor dem Start von Pluto ausgeführt werden soll	Pfad zu Script		
postpluto	shell-command, das nach dem Start von Pluto ausgeführt werden soll	Pfad zu Script		
fragicmp	Sollen fragmentierte Packete an Sender gemeldet werden, so das dieser die PMTU reduzieren kann	yes|no		

Parameter	Beschreibung	Wert	Kommentar	USE
no_eroute_pass	Eingeschränkte Version von 'packetdefault', wird ignoriert wenn 'packetdefault' definiert	yes -> packetdefault=pass no -> packetdefault=drop		
opportunistic				
hidetos	Soll der TOS-Wert des getunnelten Paketes versteck werden?	yes|no (falls no, wird der TOS-Wert des zu tunnelntel Packetes im ESP/AH Packet übernommen)		
uniqueids	Eindeutiger Partner-ID	yes|no (falls yes, wird eine bestehende Verbindung zu einem Partner mit der selben ID wie die des Partners der neuen Verbindung gelöscht)		
packetdefault	Verfahrensweise für Packete, die in ein virtuelles IPSEC-Interface gelangen und keine eroute haben	pass|drop|reject		
overridemtu	Legt die PMTU der virtuellen IPSEC-Interface fest	Ganzahl (MTU-Wert)		
nocrsend	Soll beim Verbindungsaufbau kein Certificate-Request gesendet werden	yes|no (für Partner, die keine Authentifizierung per Zertifikat unterstützen, und die Authentifizierung abbrechen)		
strictcrlpolicy	konsequente Prüfung der Identzertifikate per CRL	yes|no (falls yes, muß eine gültige CRL exsistieren. falls no, und CRL mit gesperrten Zertifikaten ist vorhanden, wird dies beachtet?)		
crlcheckinterval	????????????????????	Ganzahl (long) (Sekunden)		
nat_traversal	Einschalten des NAT-T patches (ESP in UDP)	yes|no		
keep_alive	Zeit zischen keepalive -Packeten	Ganzzahl (Sekunden)		
force_keepalive	Erzwinge keepalive -Pakete	yes|no		
disable_port_floating	??????????????	yes|no		
virtual_private	systemweite 'private net list'	Bsp.: 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	Authentifikation User/Password gegen PAM (/etc/pam.d/pluto)	yes|no		

3.2.Connection generell

Parameter	Beschreibung	Wert	Komentar	USE
also	bindet Optionen der Sektion in aktuelle Sektion ein	Sektionsname		
type	Verbindungstyp	tranport|tunnel| passthrough(only manual-mode)		
authby	Authentifizierung per	secret|rsasig		
_plutodevel	?????????????			
left-/right	Adresse	<ipadress>|%any| %opportunistic		
left-/rightsubnet	Zu tunnelntes Netzwerk	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	Auswahl von Protokoll/Port für IPSEC-SA	<Protokollname/-nummer>/(<Portnummer>) %any als Wildcard		
leftnexthop	Route IPSEC-Packete via ...	<ipadress>|%defaultroute| %direct		
leftfirewall	Wenn der Host Verbindungen firewalled, wird eine Forward-Regel erstellt	yes|no		
leftupdown	Script, das gestartet werden soll, wenn sich der Verbindungsstatus ändert	Pfad zum Script + Argumente (quoted String)		
esp	Verschlüsslungs-/Authentifikations - 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 !: exlusive, akzeptiere keine anderen Verfahren		
ah	Authentifikations - Algorithmen	auth(!) auth: md5|sha|sha2_256| sha2_512 !: exlusive, akzeptiere keine anderen Verfahren		

3.3 connection - Auto-Keyed Parameter

Parameter	Beschreibung	Wert	Komentar	USE
auto	Operation bei Startup	add|route|start|ignore		
keyexchange	Methode des Schlüßelaustauschen	ike		
auth	Protokoll für Authentifikation	esp|ah		
pfs	Perfect Forward Secrecy of keys	yes|no		
pfsgroup	PFS-Gruppe, wenn pfs=yes	modp(768,1024,1536,2048,3072,4096,6144,8192)		
keylife	Lebenszeit der Authentifikations-/Verschlüsslungsschlußel für IPSec	Ganzzahl, gefolgt von s(Sekunden)|m(Minuten)|h(Stunden), max 24h		
rekey	Soll vor dem Ablauf der Lebenszeit der Schlüßel, ein erneuter Schlüßelaustausch erfolgen?	yes|no		
rekeymargin	wie lange vor dem Ablauf der Schlüßel soll der erneute Schlüßelaustausch erfolgen	Ganzzahl, gefolgt von s(Sekunden)|m(Minuten)|h(Stunden)		
rekeyfuzz	Prozentzahl mit der der wiederholte Schlüßelaustausch zufällig verlängert wird. (Ergebins darf keylife nicht überschreiten)	Ganzahl% (mit Prozentzeichen)		
dpddelay	Wartezeit zwichen Packeten	Ganzahl (Sekunden)		
dpdtimeout	Timeout für Warten auf Antwortpacket	Ganzahl (Sekunden)		
dpdaction	Aktion, wenn Verbindung tot ist	hold|clear		
aggrmode	erlaube aggressiv mode, sonst main mode	yes|no		
xauth	????????????? (nicht von uns verwendet)			
compress	Kompremierung der Nutzerdaten	yes|no (no = niemals Kompremieren, IKE-Proporsal ablehnen, yes = wenn möglich)		
keyingtries	Anzahl Versuche des Verbindungsaufbaus	Ganzzahl (0 = gib niemals auf)		
ikelifetime	Lebenszeit der IKE-Schlüßel	Ganzzahl, gefolgt von s(Sekunden)|m(Minuten)|h(Stunden), max 8h		
disablearrivalcheck	???????	yes|no		
ike	Verschlüsslungs-/Authentifikations - Algorithmen Bitlänge DH	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, akzeptiere keine anderen Verfahren		
lifetime	veraltet für 'keylife'			
rekeystart	veraltet für 'rekeymargin'			

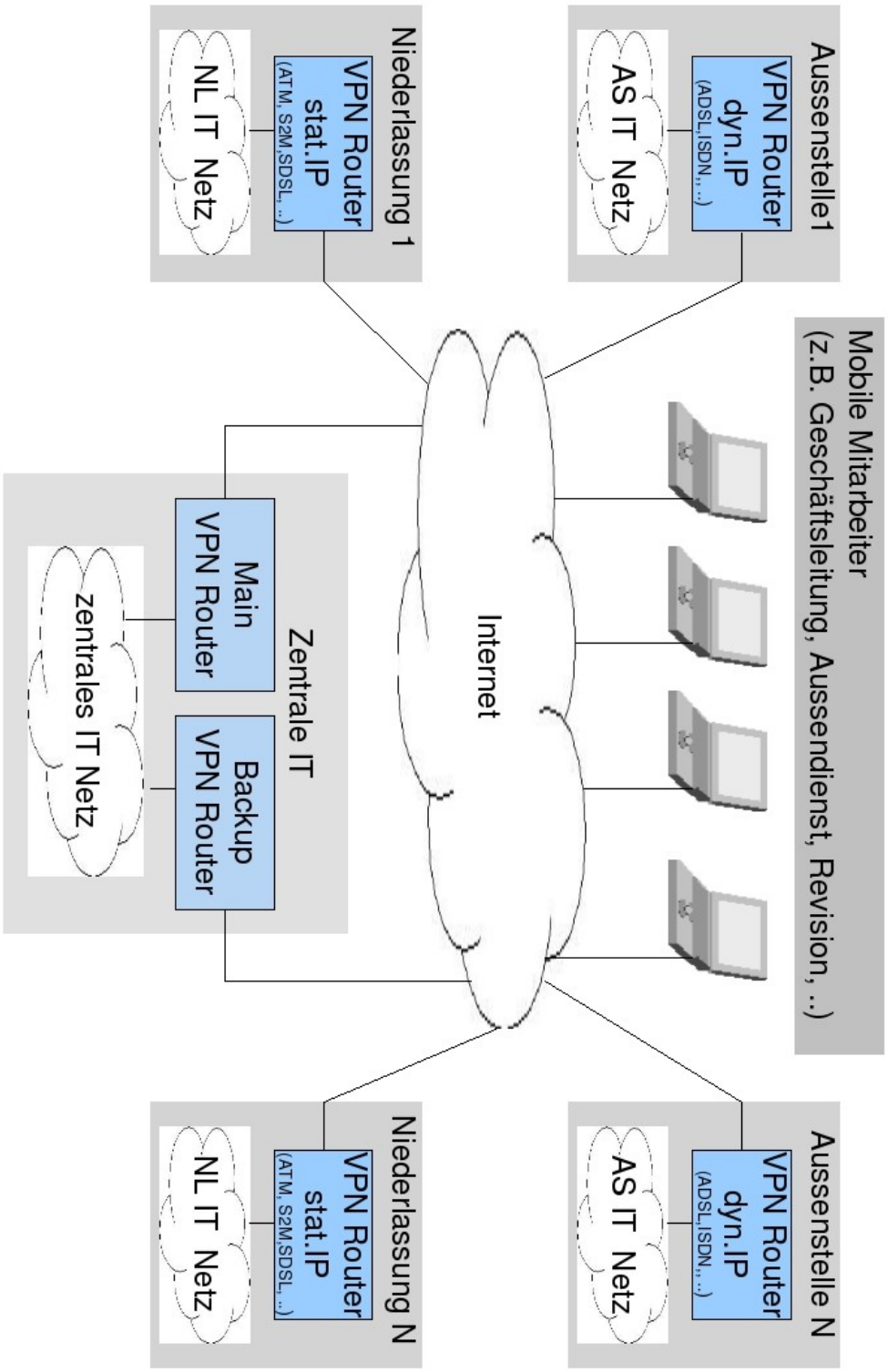
Parameter	Beschreibung	Wert	Komentar	USE
rekeytries	Anzahl der erneuten Schlüßelaustausch-Versuche	Ganzzahl (0 = gib niemals auf)		
left-/rightrsasigkey	Festlegen des RSA public keys, bzw. wie zu ermitteln	<rsakey>|%cert|%none|%dnsondemand|%dnsonload		
left-/rightrsasigkey2	Festlegen des RSA public keys, bzw. wie zu ermitteln (nützlich für Keyupdate)	<rsakey>|%cert|%none|%dnsondemand|%dnsonload		
left-/rightid	ID's der Partner	<ip>|<fqdn>|@<user_fqdn>|<distinguished name>		
left-/rightcert	zu verwendentes Zertifikat (PEM-Format)	<Pfadangabe relativ zu /etc/ipsec.d/>		
rightca	zu verwendentes CA-Zertifikat zur Authentifikation des Zertifikates	<distinguished name>|%same|(wenn nicht spezifizier, alle verfügbaren CA's)		
rightsubnetwithin	Remote-Subnetz mus im Netz angegebenen Netz liegen	<net adress>		

3.4. connection – Manual-Keyed-Parameter

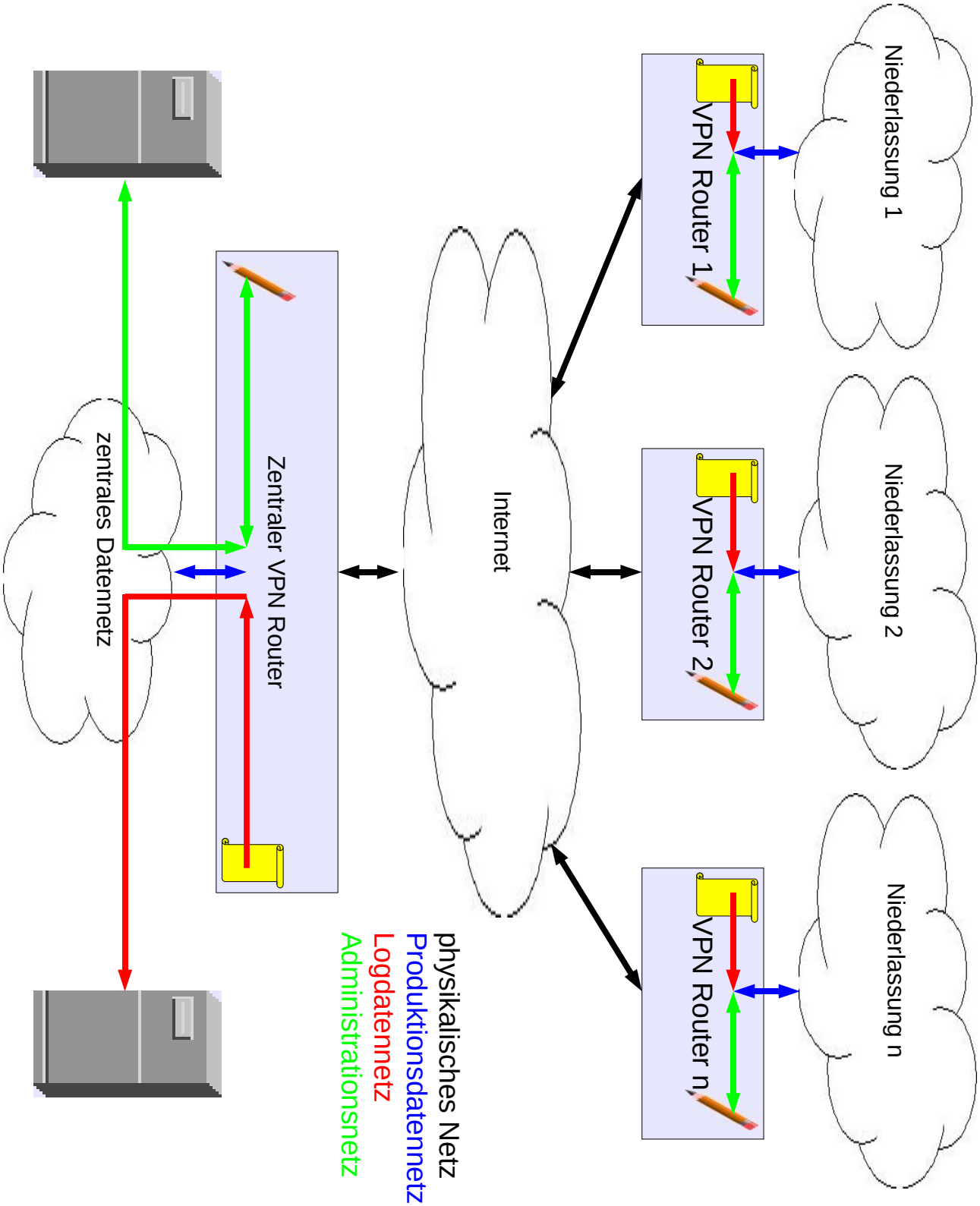
Parameter	Beschreibung	Wert	Komentar	USE
spibase	SPI-Basiswert, niederwertigstes Bit zeigt Richrung (in/out) an (exclusiv oder 'spi')	Hexzahl (3 Stellen, letze muß 0 sein) 0x..0 (empfohlen 0x100-0xff0)		
spi	Benutze SPI-Nummer für alls SA's (exclusiv oder 'spibase')	Hexzahl (3 Stellen) 0x... (empfohlen 0x100-0xfff)		
left-/rightespspi	Überschreibe automatishe ESP SA -Zuweisung mit Wert ...	Hexzahl 0x...		
left-/rightahspi	Überschreibe automatishe AH SA -Zuweisung mit Wert ...	Hexzahl 0x...		
(left/right/-)espenckey	Verschlüsslungs-Schlüßel, kann für beide Richtungen seperate festlegt werden	gültiger Schlüßel (Bitlänge) in hex-Form: 0x...		
(left/right/-) espauthkey	Authentifikations-Schlüßel, kann für beide Richtungen seperate festlegt werden	gültiger Schlüßel (Bitlänge) in hex-Form: 0x...		
espreplay_window	Antwortfenster	Ganzzahl zwischen 0..64		
(left/right/-)ahkey	Authentifikations-Schlüßel, kann für beide Richtungen seperate festlegt werden	gültiger Schlüßel (Bitlänge) in hex-Form: 0x...		
ahreplay_window	Antwortfenster	Ganzzahl zwischen 0..64		

4. Topologie Strukturgramme (Beispiele)

4.1 Zentralisiertes VPN (Topologie)



4.2 Logische Topologie eines zentralisierten VPN



4.2 Zentralisierte Administration