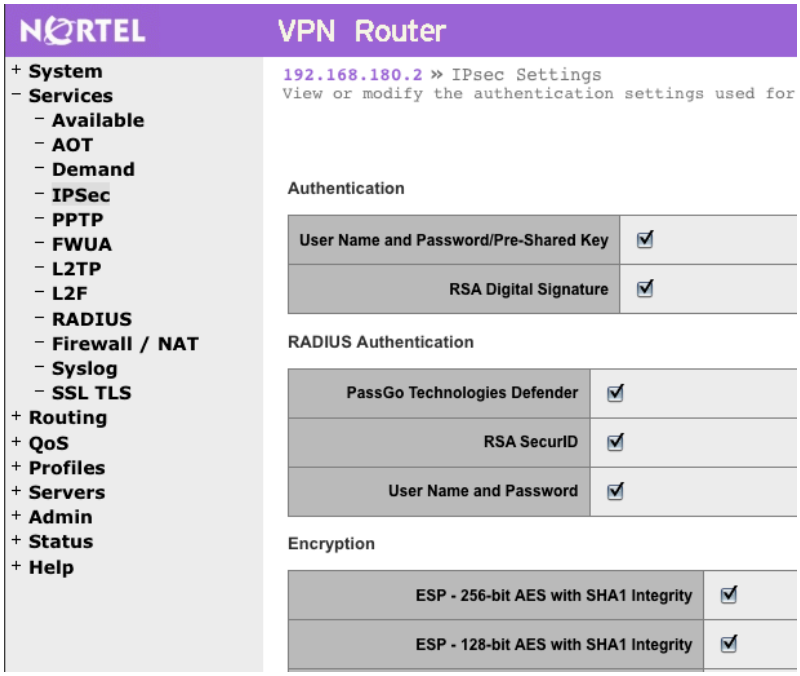
Einrichtung von VPN für Mac Clients bei Nortel VPN Router

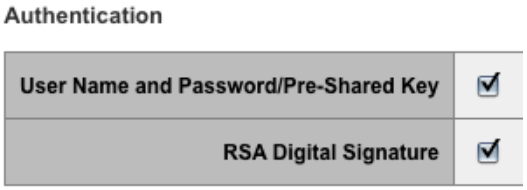


1. Einrichtung des Nortel VPN Routers (Contivity)

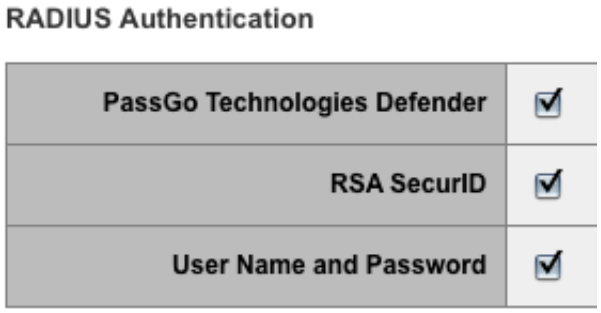
1.1.Konfigurieren der globalen IPSec Einstellungen

Für diese Beispielkonfiguration werden unter **Services > IPSec** folgende Einstellungen gemacht.

1.1.1. Authentication

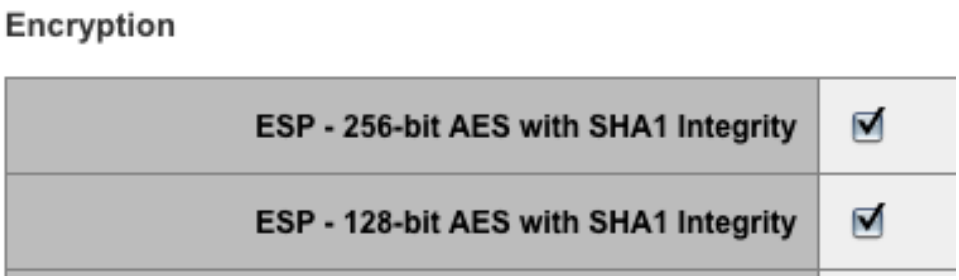


1.1.2. RADIUS Authentication



1.1.3.Encryption

Als Encryption wird in diesem Beispiel AES 128-bit für VPN Tracker 5 Personal und AES 256-bit für die Professional Variante genutzt. Alle anderen Methoden werden abgeschaltet.



1.1.4. IKE Encryption and Diffie-Hellman Group

Alle Gruppen mit AES aktivieren.

IKE Encryption and Diffie-Hellman Group

56-bit DES with Group 1 (768-bit prime)	☐
Triple DES with Group 2 (1024-bit prime)	☐
Triple DES with Group 7 (ECC 163-bit field)	☐
128-bit AES with Group 5 (1536-bit prime)	☑
128-bit AES with Group 8 (ECC 283-bit field)	☑
128-bit AES with Group 2 (1024-bit prime)	☑
256-bit AES with Group 5 (1536-bit prime)	☑
256-bit AES with Group 8 (ECC 283-bit field)	☑

1.1.5. NAT Traversal

NAT Traversal*

Enabled	☑ User Tunnel ☐ Branch Office Tunnel
Disable Client IKE Source Port Switching	☐
UDP Port	10001

*Changing NAT traversal settings will cause active tunnels to disconnect.

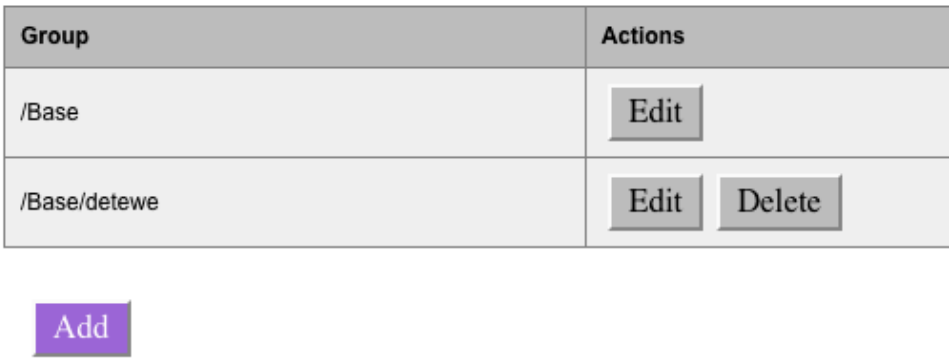
1.1.6. Einstellungen speichern

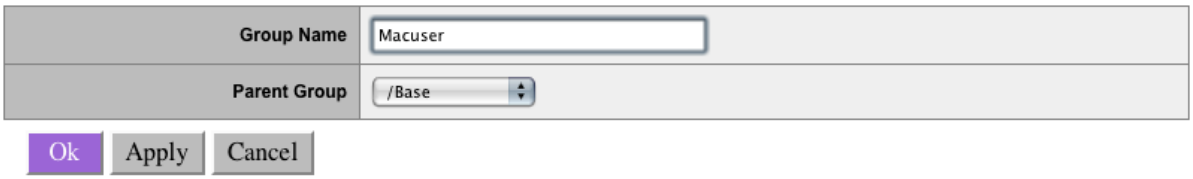
OK Cancel

1.2. Einstellen der Benutzergruppen

1.2.1. Erstellen einer Nutzergruppe für Macuser

Unter **Profiles > Groups** die Gruppen konfigurieren.





Nun die Gruppe noch bearbeiten

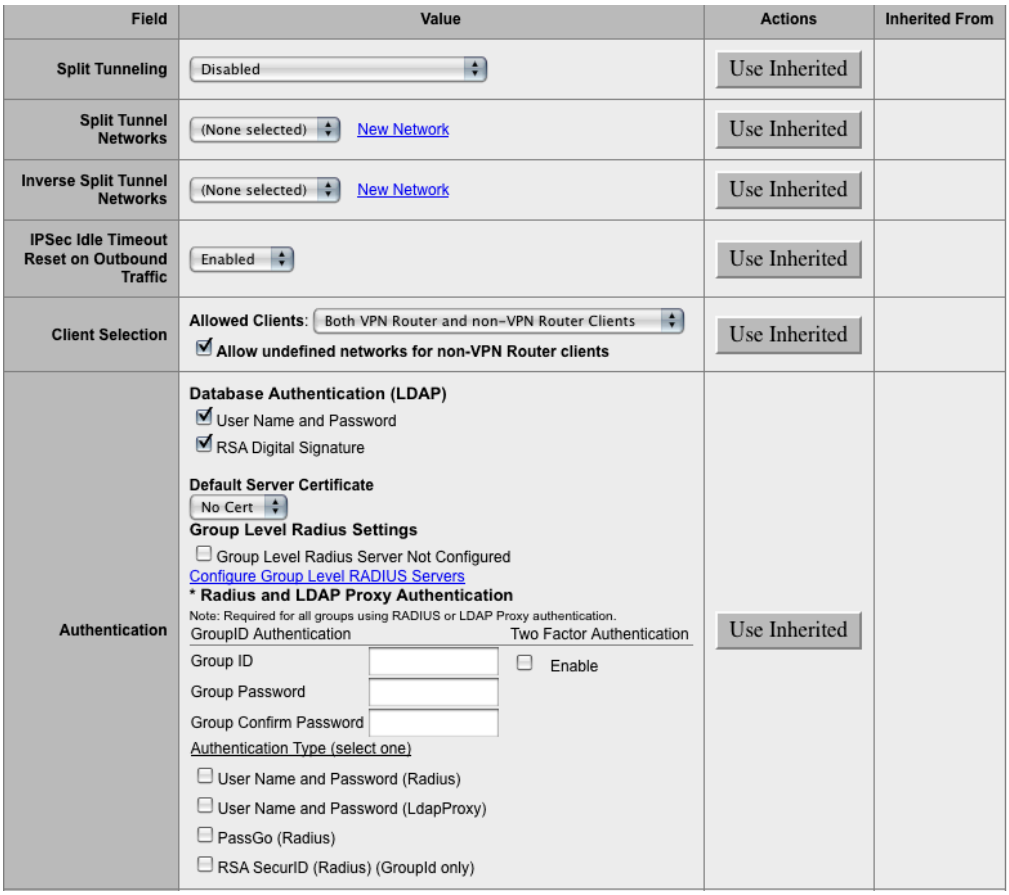
Nach Bedarf können Accesshours etc. eingestellt werden. In dieser Anleitung werden aber nur die grundlegenden Einstellungen behandelt.

1.2.2. IPSec Einstellungen der Macuser Gruppe

Ganz unten den Button **All Fields** *Configure* anklicken. Da sonst jedes Feld einzeln aktiviert werden muss.

Hier müssen keine Einstellungen mehr gemacht werden da alles von der /Base Gruppe vererbt wird.
Wenn die /Base Gruppe nicht entsprechend konfiguriert ist, muss die Macuser Gruppe folgendermaßen aussehen.

Field	Value	Actions	Inherited From
Split Tunneling	Disabled	Use Inherited	
Split Tunnel Networks	(None selected) New Network	Use Inherited	
Inverse Split Tunnel Networks	(None selected) New Network	Use Inherited	
IPSec Idle Timeout Reset on Outbound Traffic	Enabled	Use Inherited	
Client Selection	Allowed Clients: Both VPN Router and non-VPN Router Clients Allow undefined networks for non-VPN Router clients	Use Inherited	
Authentication	Database Authentication (LDAP) User Name and Password RSA Digital Signature Default Server Certificate No Cert Group Level Radius Settings Group Level Radius Server Not Configured Configure Group Level RADIUS Servers * Radius and LDAP Proxy Authentication Note: Required for all groups using RADIUS or LDAP Proxy authentication. GroupID Authentication / Two Factor Authentication Group ID / Enable Group Password Group Confirm Password Authentication Type (select one) User Name and Password (Radius) User Name and Password (LdapProxy) PassGo (Radius) RSA SecurID (Radius) (GroupId only)	Use Inherited	



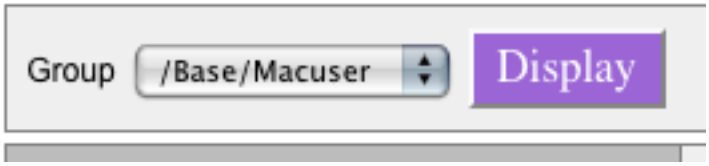
Field	Value	Actions	Inherited From
Split Tunneling	Disabled	Use Inherited	
Split Tunnel Networks	(None selected) New Network	Use Inherited	
Inverse Split Tunnel Networks	(None selected) New Network	Use Inherited	
IPSec Idle Timeout Reset on Outbound Traffic	Enabled	Use Inherited	
Client Selection	Allowed Clients: Both VPN Router and non-VPN Router Clients Allow undefined networks for non-VPN Router clients	Use Inherited	
Authentication	Database Authentication (LDAP) User Name and Password RSA Digital Signature Default Server Certificate No Cert Group Level Radius Settings Group Level Radius Server Not Configured Configure Group Level RADIUS Servers * Radius and LDAP Proxy Authentication Note: Required for all groups using RADIUS or LDAP Proxy authentication. GroupID Authentication / Two Factor Authentication Group ID / Enable Group Password Group Confirm Password Authentication Type (select one) User Name and Password (Radius) User Name and Password (LdapProxy) PassGo (Radius) RSA SecurID (Radius) (GroupId only)	Use Inherited	

Weitere Einstellungen werden für Macuser nicht vorgenommen, da DNS Server etc. im VPN Tracker eingestellt werden.

1.2.3. User anlegen

Unter **Profiles > Users** werden die User konfiguriert.

Bei **Group** muss nun die ***/Base/Macuser*** Gruppe ausgewählt werden und einmal auf *Display* geklickt. Nun kann ein neuer User angelegt werden.



Hier wird der Vor- & Nachname eingegeben werden, bei IPSec eine UserID & Passwort.

Für den VPN Tracker ist zusätzlich eine feste IP Adresse nötig.

General

	First	Last
Name	mac	test
Group	/Base/Macuser	

	Static IP Address	Static Subnet Mask
Remote User	192.168.180.99	255.255.255.224

Note: The static IP subnet mask is used for IPsec connections only

User Accounts

	User ID	Password	Confirm Password	Expires (Days)	Status
IPsec	mactest	•••••••	•••••••		
PPTP					
L2TP					
L2F					
Firewall User Authentication					

Must Change Password at Next Logon	☐ (Nortel IPSEC Client Only)

Eine Automatische Konfiguration ist aktuell nicht möglich.

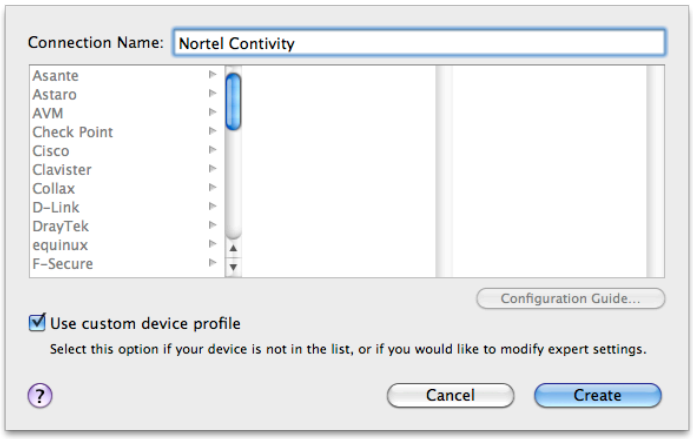
Hiermit ist die Konfiguration des Nortel VPN Router‘s beendet.

2. Einrichtung des VPN Tracker

2.1. Erstellen einer neuen Verbindung

Über den Menüpunkt **Ablage > Neue Verbindung** muss eine Verbindung erstellt werden.

Der Name kann frei gewählt werden und der Haken bei „Benutzerdefinierte Verbindung anlegen“ muss gesetzt sein.



2.2. Grundeinstellungen

2.2.1. Netzwerkeinstellungen

Je nach Bedarf kann die **Netzwerkeinstellung *Host zu allen Netzwerken*** oder ***Host zu Netzwerk*** gewählt werden.
Bei ***Host zu Netzwerk*** müssen die zu erreichenden Netzwerke im VPN Tracker angegeben werden.

In diesem Beispiel wird die Variante ***Host zu allen Netzwerken genutzt***.

Bei VPN Gateway ist die externe IP Adresse der Contivity an zu geben.

Die Lokale Adresse ist die Adresse die in der Userkonfiguration des VPN Router‘s angegeben wurde.

2.2.2. Authentifizierung

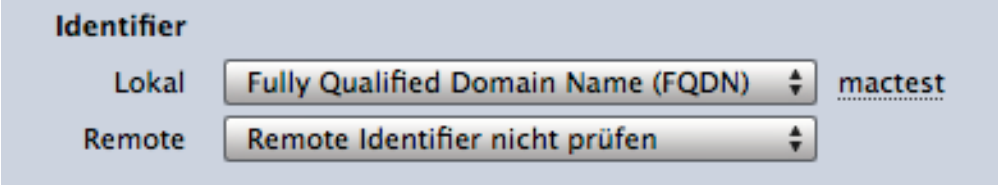
Für die **Authentifizierung** ist ***Pre-Shared Key*** zu nutzen. Wird das Passwort über den *Bearbeiten* Button nicht fest eingegeben, wird

beim ersten Verbinden nachgefragt und bei Bedarf an dieser Stelle gespeichert.

2.2.3. Identifier

Der **Lokale Identifier** ist ***Fully Qualified Domain Name (FQDN)*** und der Wert die eingestellte UserID.

Der **Remote Identifier** ist auf ***Remote Identifier nicht prüfen*** zu setzen.

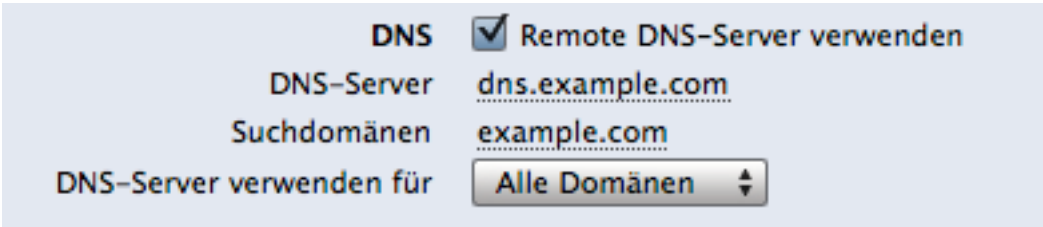


2.2.4. DNS

Remote DNS-Server verwenden kann bei Bedarf aktiviert werden.

Da dies Sinnvoll ist, müssen hier die entsprechenden **DSN-Server** und **Suchdomänen** eingegeben werden.

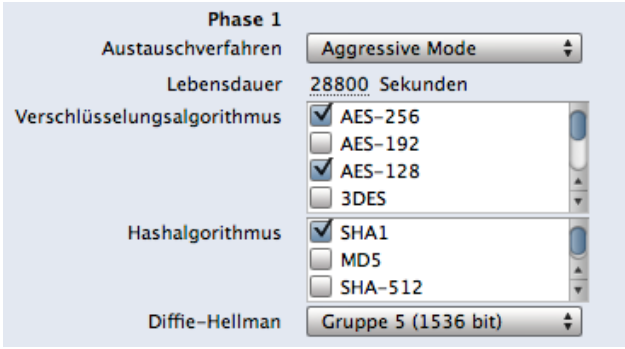
Wenn eine ***Host zu allen Netzwerken*** Verbindung benutzt wird sollte die Einstellung für **DNS-Server verwenden für** auf ***Alle Domänen (Global DNS)*** gestellt werden. Bei einer ***Host zu Netzwerk*** Verbindung kann auch die Einstellung ***Bestimmte Domänen (Split DNS)*** genutzt werden.



Wenn alle Einstellungen gemacht sind, muss es so aussehen.

2.3. Erweiterte Einstellungen

2.3.1. Phase 1



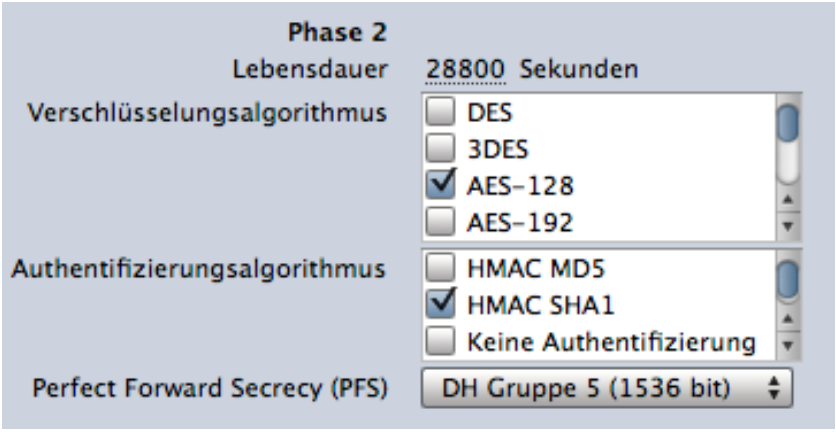
Als **Austauschverfahren** ist der ***Aggressive Mode*** einzustellen.
Beim **Verschlüsselungsalgorithmus** ist alles bis auf ***AES-128*** & ***AES-256*** zu deaktivieren.
AES-128 wird von der Personal und AES-256 von der Professional Version des VPN Tracker genutzt.

Hashalgorithmus ist ***SHA1***.

Als **Diffie-Hellman** Gruppe wird in diesem Beispiel ***Gruppe 5 (1536 bit)*** genutzt.

2.3.2. Phase 2

Beim **Verschlüsselungsalgorithmus** ist alles bis auf ***AES-128*** & ***AES-256*** zu deaktivieren. AES-128 wird von der Personal und AES-256 von der Professional Version des VPN Tracker genutzt.



Authentifizieungsalgorithmus ist ***HMAC SHA1***.

Perfect Forward Secrecy (PFS) verwenden aktivieren und die ***DH Gruppe 5 (1536 bit)*** einstellen (In diesem Beispiel).

Einen eigenen Phase 2 Tunnel für jedes Remote Netzwerk aufbauen deaktivieren.

Weitere Standardeinstellungen müssen nicht bearbeitet werden.

3. Verbindung aufbauen

Nun kann der VPN Tunnel aktiviert und getestet werden. Weitere Informationen zur Verwendung von VPN Tracker finden Sie im Handbuch unter “Hilfe > Handbuch”.