

Einrichtung von VPN für Mac Clients bei Nortel VPN Router



NORTEL VPN Router															
<ul style="list-style-type: none"> + System - Services <ul style="list-style-type: none"> - Available - AOT - Demand - IPsec - PPTP - FWUA - L2TP - L2F - RADIUS - Firewall / NAT - Syslog - SSL TLS + Routing + QoS + Profiles + Servers + Admin + Status + Help 	<p>192.168.180.2 » IPsec Settings View or modify the authentication settings used for</p> <p>Authentication</p> <table border="1"> <tr> <td>User Name and Password/Pre-Shared Key</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>RSA Digital Signature</td> <td><input checked="" type="checkbox"/></td> </tr> </table> <p>RADIUS Authentication</p> <table border="1"> <tr> <td>PassGo Technologies Defender</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>RSA SecurID</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>User Name and Password</td> <td><input checked="" type="checkbox"/></td> </tr> </table> <p>Encryption</p> <table border="1"> <tr> <td>ESP - 256-bit AES with SHA1 Integrity</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>ESP - 128-bit AES with SHA1 Integrity</td> <td><input checked="" type="checkbox"/></td> </tr> </table>	User Name and Password/Pre-Shared Key	<input checked="" type="checkbox"/>	RSA Digital Signature	<input checked="" type="checkbox"/>	PassGo Technologies Defender	<input checked="" type="checkbox"/>	RSA SecurID	<input checked="" type="checkbox"/>	User Name and Password	<input checked="" type="checkbox"/>	ESP - 256-bit AES with SHA1 Integrity	<input checked="" type="checkbox"/>	ESP - 128-bit AES with SHA1 Integrity	<input checked="" type="checkbox"/>
User Name and Password/Pre-Shared Key	<input checked="" type="checkbox"/>														
RSA Digital Signature	<input checked="" type="checkbox"/>														
PassGo Technologies Defender	<input checked="" type="checkbox"/>														
RSA SecurID	<input checked="" type="checkbox"/>														
User Name and Password	<input checked="" type="checkbox"/>														
ESP - 256-bit AES with SHA1 Integrity	<input checked="" type="checkbox"/>														
ESP - 128-bit AES with SHA1 Integrity	<input checked="" type="checkbox"/>														

Einrichtung des Nortel VPN Routers (Contivity)	3
<i>Konfigurieren der globalen IPSec Einstellungen</i>	3
<i>Authentication</i>	3
<i>RADIUS Authentication</i>	3
<i>Encryption</i>	3
<i>IKE Encryption and Diffie-Hellman Group</i>	4
<i>NAT Traversal</i>	4
<i>Einstellungen speichern</i>	4
<i>Einstellen der Benutzergruppen</i>	5
<i>Erstellen einer Nutzergruppe für Macuser</i>	5
<i>IPSec Einstellungen der Macuser Gruppe</i>	6
<i>User anlegen</i>	8
Einrichtung des VPN Tracker	9
<i>Erstellen einer neuen Verbindung</i>	9
<i>Grundeinstellungen</i>	9
<i>Netzwerkeinstellungen</i>	9
<i>Authentifizierung</i>	9
<i>Identifizierung</i>	10
<i>DNS</i>	10
<i>Erweiterte Einstellungen</i>	12
<i>Phase 1</i>	12
<i>Phase 2</i>	12
Verbindung aufbauen	13

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

Authentication

User Name and Password/Pre-Shared Key	<input checked="" type="checkbox"/>
RSA Digital Signature	<input checked="" type="checkbox"/>

1.1.2. RADIUS Authentication

RADIUS Authentication

PassGo Technologies Defender	<input checked="" type="checkbox"/>
RSA SecurID	<input checked="" type="checkbox"/>
User Name and Password	<input checked="" type="checkbox"/>

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.

Encryption

ESP - 256-bit AES with SHA1 Integrity	<input checked="" type="checkbox"/>
ESP - 128-bit AES with SHA1 Integrity	<input checked="" type="checkbox"/>

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)	<input type="checkbox"/>
Triple DES with Group 2 (1024-bit prime)	<input type="checkbox"/>
Triple DES with Group 7 (ECC 163-bit field)	<input type="checkbox"/>
128-bit AES with Group 5 (1536-bit prime)	<input checked="" type="checkbox"/>
128-bit AES with Group 8 (ECC 283-bit field)	<input checked="" type="checkbox"/>
128-bit AES with Group 2 (1024-bit prime)	<input checked="" type="checkbox"/>
256-bit AES with Group 5 (1536-bit prime)	<input checked="" type="checkbox"/>
256-bit AES with Group 8 (ECC 283-bit field)	<input checked="" type="checkbox"/>

1.1.5. NAT Traversal

NAT Traversal*

Enabled	<input checked="" type="checkbox"/> User Tunnel <input type="checkbox"/> Branch Office Tunnel
Disable Client IKE Source Port Switching	<input type="checkbox"/>
UDP Port	<input type="text" value="10001"/>

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

1.1.6. Einstellungen speichern



1.2. Einstellen der Benutzergruppen

1.2.1. Erstellen einer Nutzergruppe für Macuser

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

Group	Actions
/Base	<input type="button" value="Edit"/>
/Base/detewe	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Group Name	<input type="text" value="Macuser"/>
Parent Group	<input type="text" value="/Base"/> <input type="button" value="v"/>

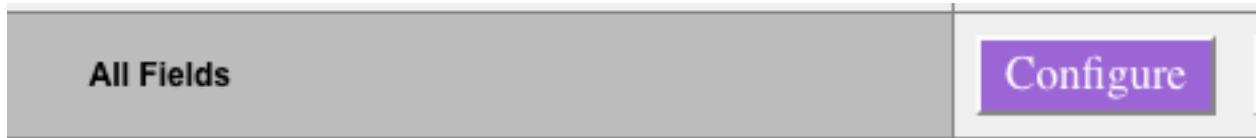
Nun die Gruppe noch bearbeiten

/Base/Macuser	<input type="button" value="Edit"/>
---------------	-------------------------------------

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 <input checked="" type="checkbox"/> Allow undefined networks for non-VPN Router clients	Use Inherited	
Authentication	Database Authentication (LDAP) <input checked="" type="checkbox"/> User Name and Password <input checked="" type="checkbox"/> RSA Digital Signature Default Server Certificate No Cert Group Level Radius Settings <input type="checkbox"/> Group Level Radius Server Not Configured Configure Group Level RADIUS Servers * Radius and LDAP Proxy Authentication <small>Note: Required for all groups using RADIUS or LDAP Proxy authentication.</small> GroupID Authentication <input type="checkbox"/> Two Factor Authentication Group ID <input type="text"/> Group Password <input type="text"/> Group Confirm Password <input type="text"/> Authentication Type (select one) <input type="checkbox"/> User Name and Password (Radius) <input type="checkbox"/> User Name and Password (LdapProxy) <input type="checkbox"/> PassGo (Radius) <input type="checkbox"/> 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 <input checked="" type="checkbox"/> Allow undefined networks for non-VPN Router clients	Use Inherited	
Authentication	Database Authentication (LDAP) <input checked="" type="checkbox"/> User Name and Password <input checked="" type="checkbox"/> RSA Digital Signature Default Server Certificate No Cert Group Level Radius Settings <input type="checkbox"/> Group Level Radius Server Not Configured Configure Group Level RADIUS Servers * Radius and LDAP Proxy Authentication <small>Note: Required for all groups using RADIUS or LDAP Proxy authentication.</small> GroupID Authentication Two Factor Authentication Group ID <input type="text"/> <input type="checkbox"/> Enable Group Password <input type="text"/> Group Confirm Password <input type="text"/> <u>Authentication Type (select one)</u> <input type="checkbox"/> User Name and Password (Radius) <input type="checkbox"/> User Name and Password (LdapProxy) <input type="checkbox"/> PassGo (Radius) <input type="checkbox"/> 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.

The screenshot shows a web interface for user configuration. It features a 'Group' label, a dropdown menu currently showing '/Base/Macuser', and a purple 'Display' button to the right.

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	<input type="text" value="mac"/>	<input type="text" value="test"/>
Group	<input type="text" value="/Base/Macuser"/>	
	Static IP Address	Static Subnet Mask
Remote User	<input type="text" value="192.168.180.99"/>	<input type="text" value="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	<input type="text" value="mactest"/>	<input type="password" value="....."/>	<input type="password" value="....."/>		
PPTP	<input type="text"/>	<input type="password"/>	<input type="password"/>		
L2TP	<input type="text"/>	<input type="password"/>	<input type="password"/>		
L2F	<input type="text"/>	<input type="password"/>	<input type="password"/>		
Firewall User Authentication	<input type="text"/>	<input type="password"/>	<input type="password"/>		
Must Change Password at Next Logon	<input type="checkbox"/> (Nortel IPSEC Client Only)				

Eine Automatische Konfiguration ist aktuell nicht möglich.

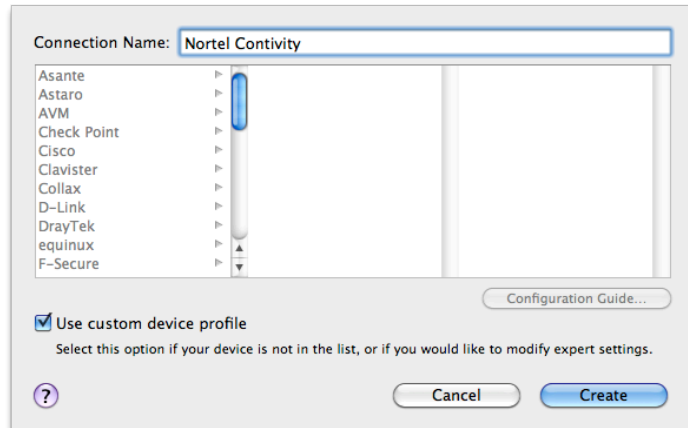
Hiermit ist die Konfiguration des Nortel VPN Router's beendet.

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 anzugeben.

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

Einrichtung von VPN für Mac Clients bei Nortel VPN Router

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.

Identifier	
Lokal	Fully Qualified Domain Name (FQDN) mactest
Remote	Remote Identifier nicht prüfen

2.2.4. DNS

Remote DNS-Server verwenden kann bei Bedarf aktiviert werden.

Da dies Sinnvoll ist, müssen hier die entsprechenden **DNS-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.

DNS	<input checked="" type="checkbox"/> Remote DNS-Server verwenden
DNS-Server	dns.example.com
Suchdomänen	example.com
DNS-Server verwenden für	Alle Domänen

Wenn alle Einstellungen gemacht sind, muss es so aussehen.

Grundeinstellungen		Erweitert	Aktionen	Export	Protokoll
 Nortel Contivity					
Verbindung basiert auf		<input type="radio"/> Custom Device <input checked="" type="radio"/> Konfigurationsanleitung			
VPN Gateway		gateway.example.com			
Netzwerkconfiguration		Manuelle Konfiguration			
Topologie		Host zu allen Netzwerken			
Lokale Adresse		192.168.180.99			
Remote Netzwerke		Kompletter Datenverkehr läuft über das VPN			
Authentifizierung		Pre-Shared Key <input type="button" value="Stored in connection"/>			
Erweiterte Authentifizierung (XAUTH)		Aus			
Identifizierung					
Lokal		Fully Qualified Domain Name (FQDN) mactest			
Remote		Remote Identifizierung nicht prüfen			
DNS		<input checked="" type="checkbox"/> Remote DNS-Server verwenden			
DNS-Server		dns.example.com			
Suchdomänen		example.com			
DNS-Server verwenden für		Alle Domänen			

2.3. Erweiterte Einstellungen

2.3.1. Phase 1

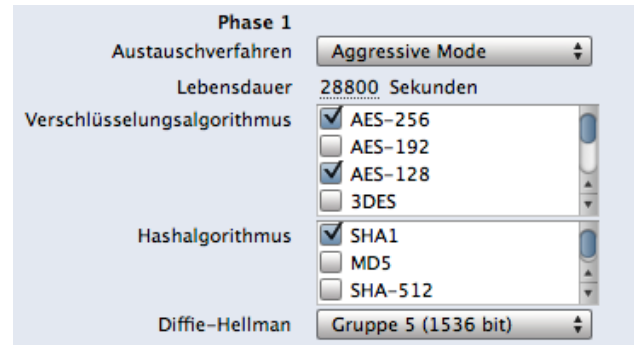
Als **Austauschverfahren** ist der **Aggressive Mode** einzustellen.

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.

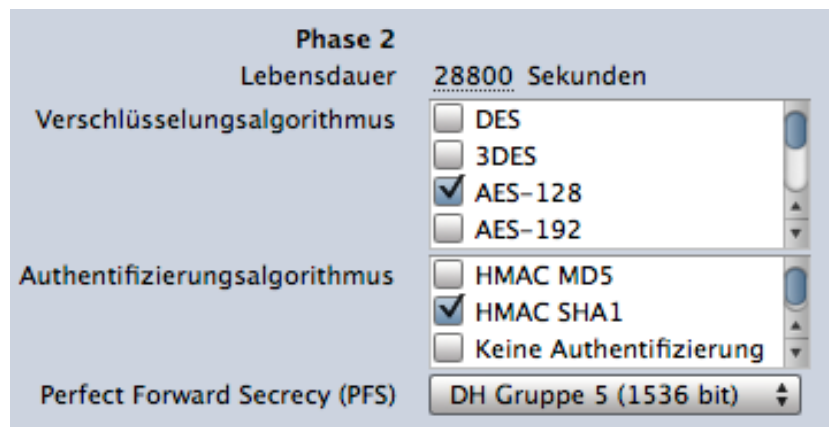


Hashalgorithmus ist **SHA1**.

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.



Authentifizierungsalgorithmus 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".

