ALL7007 VPN-Tunnel Musterkonfiguration zwischen zwei ALL7007 über dynamische IP-Adressen mit PPPoE

Wichtig: Beide Geräte müssen auf der LAN-Seite unterschiedliche IP-Kreise verwenden! Jeder der Schritte muss auf BEIDEN Geräten durchgeführt werden!

Konfiguration der Test-Router:

LAN1: Router IP: 192.168.1.1 LAN2: Router IP: 192.168.2.1

Alle für ALLNET sicherheitsrelevanten Daten wurden in dieser Anleitung unkenntlich gemacht!

Schritt 1: Einrichtung WAN-Port

Öffnen sie das Menü "Interface \rightarrow WAN" und tragen sie dort ihre Internetzugangsdaten ein und speichern diese über einen Klick auf "OK" ab.

🚰 NetGuardian - Microsoft In	ternet Explorer		
Datei Bearbeiten Ansicht	Eavoriten Extras ?		2
🙆 Zurück 🔹 🍙 🖌 🔀	🔄 🔥 🔎 Suchen 🥠 Favoriten 🚱 📿 -	2 📮 🐺	
			Ula de ante aux - Ula la 💥
Adresse C http://192.168.2.1/			
ALES.			
System	Interface > WAN		
Sinterface	WAN Interface		
L→ LAN	PPPoE (ADSL User)		
-+ WAN	O Dynamic IP Address (Cable Mod	em User)	
L⇒ DMZ	O Static IP Address		
🚨 Policy Object			
💶 Policy	Current Status	Connected	Connect
🚨 Mail Security	IP Address	84.151.252.205	Disconnect
	User Name	(Max. 60 character	s)
Anomaly Flow IP	Password	(Max. 60 character	s)
Monitor	IP Address provided by ISP	Oynamic	
		C Fixed	
		IP Address	
		Netmask	
		Default Gateway	
	Max. Downstream Bandwidth	30000 Kbps (Ra	ange: 1 - 30720)
	Max. Upstream Bandwidth	30000 Kbps (Re	ange: 1 - 30720)
	Service-On-Demand		
	Auto Disconnect if idle 0 m	inutes(Range: 1 - 99999, 0: means always conne	cted)
		-	_
	Enable System Management	I≝ Ping	M HTTP
			OK Cancel
Eartin			
C rerug		J	

Schritt 2: Einrichtung DynDNS

Sie benötigen hierfür einen dynamischen Domainnamen. Diesen erhalten sie beispielsweise auf www.dyndns.org. Wenn sie bereits einen Account haben können sie diesen in der ALL7007 eintragen.

Gehen sie hierfür in das Menü "System \rightarrow Configuration \rightarrow Dynamic DNS". Hier können sie ihren DynDNS-Server auswählen und ihre Zugangsdaten eintragen.

🚈 NetGuardian - Microsoft 1	t Internet Explorer
Datei Bearbeiten Ansicht	t Eavoriten Extras 2
🔇 Zurück 🔹 🕥 🖌 💌	📔 😚 🔎 Suchen 🤺 Favoriten 🤣 😥 🔜 👼
Adresse 🙆 http://192.168.2.	2.1/ 👻 🔁 Wechseln zu Link
ALLNET	
🖻 System	System > Configure > Dynamic DNS
🖬 Administration	
🚍 Configure	Modify Dynamic DNS
–⇒ Setting	Service Provider : DynDNS (www.dyndns.com) [U.S.A.] Sign up
→ Date/Time	WAN IP: 84.151.252.205 V Automatically WAN
→ Multiple Subnet	User Name : User Name :
→ Route Table	Password :
-⇒ DHCP	Domain Name: dyndins.org
Dynamic DNS	
Host lable	OK Cancel
Legaut	
Reliev Object	
Policy	
Mail Security	
💶 IDP	
💶 Anomaly Flow IP	
🚨 Monitor	
😂 Fertig	🥥 Internet

Wenn ihre Daten korrekt abgeglichen werden konnten, sehen sie folgenden Bildschirm:

🚈 NetGuardian - Microsoft Int	ernet Explorer					_ 8 ×
<u>D</u> atei <u>B</u> earbeiten <u>A</u> nsicht <u>E</u>	avoriten E <u>x</u> tras <u>?</u>					
🔆 Zurück 🔹 🕥 🖌 🔀 🕻	🕄 🏠 🔎 Suchen 👷	Favoriten 🧭 🔗 🍡 📘	2 😻			
Adresse 🙆 http://192.168.2.1/						Wechseln zu Links »
ALLNET						
🖻 System	System > Configure > Dyna	mic DNS				
Administration						
Configure	i	Domain Name	WAN IP	Configu	re	
→ Setting		Bernard growth State	84.151.252.205	Modify F	Remove	
_⇒ Date/Time						
→ Multiple Subnet			New Entry			
→ Route Table						
-⇒DHCP						
Dynamic DNS						
→ Host Table						
L⇒ Language						
Logout						
lnterface						
Policy Object						
Moil Cocurity						
Anomaly Flow IP						
🖾 Monitor						
😂 Fertig					Internet	

Schritt 3: Einrichtung IPSec-Policy

Für die Konfiguration der IP-Sec-Policy begeben sie sich bitte in das Menü "Policy Object \rightarrow VPN \rightarrow IPSec Autokey". Tragen sie hier ihre Daten gemäß der Musterkonfiguration ein. Wichtig sind hierbei folgende Punkte:

- Im Feld "To Destination → Remote Gateway" können sie den DynDNS-Domainnamen der gegenüberliegenden Seite eintragen.

- Der Preshared-Key muss aus mindestens acht Zeichen bestehen und muss auf beiden Geräten identisch konfiguriert werden.
- Alle Verschlüsselungsoptionen müssen identisch eingestellt werden.
- Die Werte in den Feldern "My ID" und "Peer ID" müssen auf den Geräten jeweils gespiegelt konfiguriert werden. Das @-Zeichen ist hierbei wichtig!
- In den Feldern "GRE Local IP" und "GRE Remote IP" werden die LAN-Adressen der Geräte eingetragen. "GRE Local IP" beschreibt die lokale, "GRE Remote IP" beschreibt die entfernte LAN-Adresse.





NetGuardian - Microsoft Interpretention	ternet Explorer					_ 8 ×
Datei Bearbeiten Ansicht I	Favoriten Extras ?					
Zurück + (3) - (2)	z 🔬 💭 Suche	en 🐈 Favoriten 🧭	🔊 - 📐 🥽 🐺			
Adresse Abttp:///192.168.2.1/		~ ~ []			Vierbe	eln zu Links »
ALLNET						
🖾 System	Policy Object > VP1	N > IPSec Autokey				
🚨 Interface						-
🖻 Policy Object	1	Name	Gateway IP	IPSec Algorithm	Configure	_
🖬 Address	<u>i</u>	ALLTEST	THE COURSE SECTION	DES / MD5	In Use	
🗳 Service						
🖬 Schedule			New	Entry		
🗳 QoS						
💶 Authentication						
🔛 Content Blocking						
🔛 Virtual Server						
S VPN						
IPSec Autokey						
PPTP Server						
- → PPTP Client						
Policy						
Mail Security						
Anomaly Flow IP						
Monitor						
🕘 Fertig					📄 📄 Internet	

Schritt 4: Konfiguration des Tunnels

Nach der Konfiguration der IP-Sec-Policy müssen sie dem Gerät mitteilen, dass sie einen VPN-Tunnel nutzen möchten. Hierfür gehen sie im Menü auf den Punkt "Policy Object \rightarrow VPN \rightarrow Tunnel". Hier haben sie die Möglichkeit den Tunnel wie folgt zu öffnen:

- Geben sie im Bereich "From Source Subnet / Mask" ihr lokales Subnetz und die lokale Subnetzmaske an.
- Im Bereich "To Destination" wählen sie "To Destination Subnet / Mask" und geben hier das entfernte lokale Subnetz und die entsprechende Subnetzmaske ein.
- Im Feld "IPSec/PPTP-Setting" wählen sie die vorher konfigurierte IPSec Policy aus.
- Im Feld "Keep alive IP" tragen sie eine lokale IP-Adresse aus dem gegenüberliegenden Netz ein.



💣 Fertig

🔹 🚺 👔 Internet

Schritt 5: Konfiguration der Outgoing/Incoming Policys

Damit ihr VPN funktioniert müssen sie sowohl eine Outgoing wie auch eine Incoming Policy für das VPN definieren. Zusätzlich muss jeweils eine Outgoing und eine Incoming Policy für den Internettraffic vergeben werden. Diese müssen wie folgt konfiguriert werden (Traffic Log und Statistic können, müssen aber nicht aktiviert werden:

Wichtig: Im Feld "Tunnel" wählen sie den von ihnen vorher konfigurierten VPN-Tunnel aus.

Outgoing-Policy VPN:

餐 NetGuardian - Microsoft In	ternet Explorer			_ 8 ×
Datei Bearbeiten Ansicht	<u>Eavoriten Extras ?</u>			
🚱 Zurück 🔹 🕥 - 💌	💈 🏠 🔎 Suchen	🛧 Favoriten 🙆	• 😓 🖂 😻	
Adresse 🙆 http://192.168.2.1/				💌 🌛 Wechseln zu 🛛 Links 🌺
ALLNET				
💴 System	Policy > Outgoing			
🚨 Interface				
💴 Policy Object	Co	mment : ALLTEST_OUT	(Max. 32 characters)	
Policy	M	odity Policy		
-+ Outgoing	So	ource Address		
→ Incoming	De	estination Address		
LAN TO DMZ	30	st vice		
→ DMZ To WAN	30	theotication Licer		
L DMZ TO LAN		innen lucation oser		
💴 Mail Security	10 A/			
	Tr	affic Log		
Anomaly Flow IP	st	atistics		
- Wornton	D	p		
	Co	ontent Blocking		
	M	AX. Concurrent Sessions		
	Q	s	None 💌	
			(ок) с	ancel
🧉 Fertig			📄 📄 👘 🔮 Inte	arnet

Outgoing-Policy:

Date Barbeten Brankt Barokt Bar	🚈 NetGuardian - Microsoft	Internet Explorer				_ 8 ×
Image: Source of the source of th	Datei Bearbeiten Ansicht	Eavoriten Extras	2			
Adves http://192.188.2.1/	😋 Zurück 🛛 🕤 👻 🔀	👔 🚮 🔎 Such	nen 🤺 Favoriten 🥝 🔗	🤄 😓 🥅 🐺		
System Interface Policy Object Policy Object Incoming Want To DMZ Incoming Want To DMZ DM2TO VWAN OMZ TO LAN Turinef action Incoming Want To DMZ DM2 To VWAN DM2 To VWAN DM2 To VWAN OBAT To WAN Ob	Adresse Adresse Adresse	.1/			-	Wechseln zu Links »
Policy > Outgoing Policy Object Policy Object Policy Object Policy Noment: Modify Policy Scree Address Policy Noment: Modify Policy Scree Address Policy Noment: Modify Policy Scree Address Policy Noment: Scree Address Policy Noment: Scree Address	ALLNET					
Interface Policy Outgoing - Outgoing - Wan To DMZ - LAN TO DMZ - DMZ To LAN Mail Security - Mail Security - Monitor I DP - Enable Drable Concurrent Secsions DP Concurrent Secsions Op Op Concurrent Secsions Op Concurrent Secsions Op Concurrent Secsions Op Concurrent Secsions Concurrent Secsions Concurrent Secsions <th>💶 System</th> <th>Policy > Outgoing</th> <th></th> <th></th> <th></th> <th></th>	💶 System	Policy > Outgoing				
F Policy Object Policy Incoming + Incoming + WAN To DMZ - DMZ To LAN Mail Security IDP Traffic Log F Enable Statistics DP Traffic Log IDP Content Blocking	🖾 Interface					
Policy Modify Policy Surce Address Inside_Any ▼ > WAN To DMZ Destination Address > DMZ To WAN Service > DMZ To WAN Service > DMZ To WAN Mone ▼ > Mail Security None ▼ ™ Anomaly Flow IP Turnel ™ Monitor PERMIT ▼ © DP Trable Tortert Blocking Enable Contert Blocking Enable Contert Blocking Enable MAX. Concurrent Sessions D Gos None ▼	💴 Policy Object		Comment :	(Max. 32 characters)		
→ incoming Source Address Outside_Any ▼ → incoming Destination Address Outside_Any ▼ → WAN To DMZ Schedule None ▼ → DMZ To VAN Adhentication User None ▼ → DMZ To VAN Adhentication User None ▼ → DMZ To VAN Adhentication User None ▼ Adhentication User None ▼ Action PERMIT ▼ Tarfitic Log ▼ Enable Octert Blocking □ Enable Cortert Blocking □ Enable MAX. Concurrent Sessions □ QoS None ▼	Policy		Modify Policy			
Pestination Address Udside_Any Pestination Address Visual Add	-+ Outgoing		Source Address			
LAN TO DMZ OMZ TO LAN OMZ TO LAN OMZ TO LAN Mail Security Action PERMIT Action PERMIT Action PERMIT Turnel None Action PERMIT Traffic Log V Enable DP Traffic Log V Enable DP Tenable MAX. Concurrent Sessions O Ox Cancel	→ Incoming		Destination Address			
> DMZ To VAN Authentication User None ▼ > DMZ To LAN None ▼ Authentication User * Mail Security Turnel None ▼ * Action PERMIT ▼ * Anomaly Flow IP Traffic Log ✓ Enable Statistics ✓ Enable OPP □ Enable Cortext Blocking □ QoS None ▼ OK Cancel	► WAN TO DWZ		Service	ANY		
Authentication User None Tunnel None Tunnel None Tunnel None Tartíc Log Fenade Statistics Fenade DP Enade Content Blocking Enade MAX. Concurrent Sessions O OK Cancel	→ DMZ To WAN		Schedule	None		
Mail Security Mail Security Action PERMIT Action PERMIT Action PERMIT Action PERMIT Traffic Log IP Traffic Security Reable DP Installe Contert Blocking Installe MAX. Concurrent Sessions D Gos None I	L DMZ TO LAN		Authentication User	None 💌		
IDP Action PERMT Image: Content Blocking Traffic Log Image: Content Blocking Image: Content Blocking OC Content Blocking Image: Content Blocking Ox S None ▼	🚨 Mail Security		Tunnel	None		
Image: Anomaly Flow IP Traffic Log Image: Anomaly Flow IP Statistics Image: Anomaly Flow IP Enable IDP Image: Enable Image: Anomaly Flow IP Content Blocking Image: Enable Image: Anomaly Flow IP AX. Concurrent Sessions Image: Enable Image: Anomaly Flow IP OK Cancel Image: Enable	🚨 IDP		Action	PERMIT		
Monitor Statistics Enable DP Enable Cortent Blocking	🚨 Anomaly Flow IP		Traffic Log	Enable		
IDP Include Contert Blocking Include MAX. Concurrent Sessions Include QoS None Include	🚨 Monitor		Statistics	Finable		
Contert Blocking Contert Blocking Cos None Cos			IDP	Enable		
			Content Blocking			
			MAX. Concurrent Sessions			
			QoS	None 💌		
					OK Cancel	
	The second se				all Takanak	

Michael Fiolka, 1. September 2006 www.allnet.de Wenn sie beide Policies konfiguriert haben erhalten sie folgende Übersichtsseite. Wichtig ist, dass die VPN-Policy als erster Eintrag in der Liste steht!

🚰 NetGuardian - Microsoft Int	ernet Explorer								×
<u>D</u> atei <u>B</u> earbeiten <u>A</u> nsicht <u>B</u>	<u>Eavoriten Extras ?</u>								
🌀 Zurück 🝷 🕥 🖌 🗾	🔰 🏠 🔎 Suche	en chavoriten	છ	- 🎍 🛛	2	*			
Adresse 🙆 http://192.168.2.1/									💌 🔁 Wechseln zu 🛛 Links 🎽
ALLNET									
🗳 System	Policy > Outgoing					_			
🚨 Interface	0.000	Destination	Ormiter	0 officers			and a se		Canfinung Maus
Policy Object	Source	Orteide Apu	AND	WEN			puon In a	<u> </u>	Modify Remove Pause
Policy	Inside_Any	Outside Any				-	11		Modify Remove Pause To 2
→ Incoming	inolde_riny	catolao_Any							
→ WAN To DMZ						4	New Ent	try	
-→ LAN To DMZ									
–♦ DMZ To WAN									
L DMZ TO LAN									
Anomaly Flow IP									
🚨 Monitor									
🐴 Fertia		_							Internet

Incoming Policy VPN:

🚰 NetGuardian - Microsoft Int	ternet Explorer		_ 8 ×
Datei Bearbeiten Ansicht F	Eavoriten E <u>x</u> tras <u>?</u>		
🔆 Zurück 🔹 🕥 - 💌	💈 🐔 🔎 Suchen 🤺 Favoriten 🧔 🔗	3- 😓 🚍 🐺	
Adresse Altp://192.168.2.1/			Wechseln zu Links »
ALLNET			
🗳 System	Policy > Incoming		
🖬 Interface			
💶 Policy Object	Comment : ALLTEST_IN	(Max. 32 characters)	
🗏 Policy	Modify Policy		
→ Outgoing	Source Address	Outside_Any 💌	
Incoming	Destination Address	Inside_Any 🔽	
→ WAN To DMZ	Service	ANY	
LAN TO UMZ DMZ To WAN	Schedule	None	
	Tunnel	ALLTEST2	
Mail Security	Action	PERMIT	
DP	Traffic Log	Enable	
🚨 Anomaly Flow IP	Statistics	Finable	
🚨 Monitor	IDP	Enable	
	MAX. Concurrent Sessions	0 (Fample L-See A. O) measure (Jundos)	
	QoS	None 💌	
	NAT	Enable	
		OK Cancel	
ercig		j j j j 🖉 Internet	

Incoming Policy:

🚰 NetGuardian - Microsoft Int	ernet Explorer					_ 8 ×			
Datei Bearbeiten Ansicht E	avoriten E <u>x</u> tras <u>?</u>								
🔇 Zurück 🛛 🕥 - 💌 👔	🕄 🏠 🔎 Suchen	Favoriten 🚱 🔗	- 😓 🔜 😻						
Adresse 🕘 http://192.168.2.1/	Adresse 🎒 http://192.168.2.1/ 🔍 🄁 Wechseln zu Links »								
ALLNET									
System	Policy > Incoming					MY20000			
🖬 Interface									
💴 Policy Object		Comment :	(Max. 32 characters)						
🗏 Policy		Modify Policy							
-+→ Outgoing		Source Address	Outside_Any 💌						
-+ Incoming		Destination Address	Inside_Any						
-⇒ WAN To DMZ		Service	ANY						
LAN TO DMZ		Schedule	None 💌						
→ DMZ To WAN		Tunnel	None						
Weil Couvritu		Action	PERMIT						
		Traffic Log	Enable						
Anomaly Flow IP		Statistics	Enable						
🖾 Monitor		IDP	Enable						
		MAX. Concurrent Sessions	0	0					
		QoS	None 💌						
		NAT	Enable						
	· · · ·		h.						
					OK Cancel				
2 2									
🛃 Fertig					i Internet				

Wenn sie beide Policies konfiguriert haben erhalten sie folgende Übersichtsseite. Wichtig ist, dass die VPN-Policy als erster Eintrag in der Liste steht!

🚰 NetGuardian - Microsoft Inte	ernet Explorer												_ 8 ×
Datei Bearbeiten Ansicht E	avoriten E <u>x</u> tras <u>?</u>												-
🔇 Zurück 👻 🕥 🖌 🚺	💈 🏠 🔎 Suchen	🔆 Favoriten	🔊 • 볼	2	*								
Adresse 🙆 http://192.168.2.1/												Wechseln zu	Links »
ALLNET													
🗳 System	Policy > Incoming												
😅 Interface	Course	Dection	Conviso	Bation		Out	lau			One		Maura	
Policy Object	Outoide Apu	Destination	ANY	MEN	6			Nat	Modifu	Remove	Pausa		-
Policy	Outside Any	Inside_Any(Routing)	ANY		6			Nat	Modify	Remove	Pause	To 2 V	-
	outoino_ mij	niolao_i nij(riolanig)						0				101-	
-+ WAN TO DMZ					0	New Entr	y)						
-→ LAN To DMZ													
→ DMZ To WAN													
L DMZ To LAN													
Mail Security													
Anomaly Flow IP													
🚨 Monitor													
E Fertig											🧿 Internet		

Schritt 6: Prüfen ob Tunnel aufgebaut wurde

Um zu sehen ob ihr Tunnel aufgebaut wurde können sie im Menü "Monitor \rightarrow Statistics \rightarrow Policy" folgenden Screen aufrufen:



Sofern hier bei Action ein grünes VPN-Icon zu sehen ist wurde der Tunnel erfolgreich aufgebaut.