ALL7007 v2.12 & ALL VPN Client v2.51



Einstellungen ALL7007:

Klicken sie auf Policy Objekt dann auf VPN und anschließend auf IPSec Autokey

ALLNET			
System	Policy Object > VPN > IPSec Autokey		
Interface			
Policy Object	Necessary Item		
d Address	Name	Test	
C Service	To Destination		
Schedule	Remote Gateway Fixed IP or Domain Name		
uos Alle Ver	Remote Gateway or Client Dynamic IF) 	
Autrentication	Authentication Method	Preshare 💌	
Unitern Biocking	Preshared Key	123456	
VIRLUAI Server	Encapsulation		1
	ISAKMP Algorithm		1
DDTD Contex	ENC Algorithm	3DES 💌	1
PPTP Client	AUTH Algorithm	SHA1 V	1
	Group	GROUP 2 V	-
Policy	IPSec Algorithm		-
Mail Security	Data Encryption + Authentication		
TIDP	FINC Algorithm	3DES T	-
Anomaly Flow IP	AUTH Algorithm	SHA1 V	-
Monitor	C Authentication Only		1
	Optional Item		
	Perfect Forward Secrecy	GROUP 2 💌	1
	ISAKMP Lifetime	3600 Seconds	1
	IPSec Lifetime	28800 Seconds	1
	Mode	C Main mode C Aggressive mode	1
	My ID	@home.de	
	Peer ID	@remote.de	
	GRE/IPSec		1

Stellen sie nun die Werte ein, wie auf dem Screenshot zu sehen ist. Gehen sie dann auf den Menüpunkt Tunnel und legen sie dort die von ihnen bevorzugten Werte fest.

System Policy Object > VPN > Tunnel Modify Tunnel_Mueller Tunnel Name Tunnel_Test Name Tunnel_Test From Source Subnet / Mask 192.168.100.0 / [255.255.25.0] To Destination Content Blocking VPN PPTP Server PPTP Server PPTP Client Policy Mail Security IDP Mail Security IDP Automaty Flow IP	ALLNET					
Interface Policy Object Address Service Service Service Chedule Oo8 Authentication Content Blocking VPN VPN Service PPTP Server PPTP Client Tonnel Authentication to the service Network Neighborhood	System	Policy Object > VPN > Tunnel				
Policy Object Name Tunnel_Test From Source © LAN C DMZ From Source Subnet / Mask 192108:100.0 1/255.255.255.0 To Destination © Content Blocking © Virtual Server Virtual Server VPN • PPTP Server • PPTP Server • PPTP Client © Tonel Folicy Mail Security IDP Automaty Flow IP Mail Security	🖬 Interface	Modify Tu	mail Mueller Tunnel			
Address Gate Gate Gate Gate Gate Gate Gate Gat	Policy Object	Nere		Tuppol Tost		
Service CAN S DM2 CAN S DM2 CAN S DM2 From Source Subnet / Mask 192.168.100.0 / [255.255.0] To Destination C To Destination C To Destination Subnet / Mask / Content Blocking VPN C Remote Client VPN Keep alive IP: C Content Proceed C Show remote Network Neighborhood PDTP Server PPTP Client C Mail Security IDP Anomaly Flow IP Mail Security IDP Anomaly Flow IP	ddress 🖸	From Sour	C.9			
Schedule Indition QoS Authentication Content Blocking VPN VPN VPN VPN Keep aliva IP: Verture	🖸 Service	Even Sour	as Suknet (Maak	100.169.100.0	1055 355 355 0	_
Q QOS In Destination ▲ Authentication ▲ Content Blocking ▲ VPN ▲ VPN ▲ IPSec Autokey ▲ PPTP Server ▲ PPTP Client ▲ Tonnel ♥ Policy Mail Security ♥ IDP ▲ Automaty Flow IP	C Schedule	To Destina	Le Subilet / Mask	132,100,100.0	1/1200.200.200.0	
Authentication Authentication Content Blocking Withal Server VPN CIPSec Autokey PPTP Client Tunnet Policy Mail Security	QoS	To Destina				-
Content Blocking VPN VPN VPN PSec Autokey PTP Server PTP Client Tunnel Policy Mail Security Mail Security Mail Security Mail Security Mail Security Mail Security	Authentication	C To D	estination Subnet / Mask		1	
VYINUAI Server VPN VPN VPPTP Server PPTP Client Tunnel Policy Mail Security	Content Blocking	(• Rem	ote Client			
VPN Keep alive IP: PTP Server PTP Client Tunnel Policy Mail Security IDP Anomaly Flow IP Monthmere	💶 Virtual Server	IPSec / PP1	/P Setting	Test		
	G VPN	Keep alive	IP :			
	→ IPSec Autokey	Show	remote Network Neighborhood			
	→ PPTP Server					
Tunnel Folicy Mail Security Anomaly Flow IP Monitor	→ PPTP Client					OK Can
	Le Tunnel					
Mail Security FIDP FOR IP Monitor Monitor	Policy					
IDP Anomaly Flow IP Monitor	Mail Security					
TAnomaly Flow IP	IDP .					
Monitor	🖸 Anomaly Flow IP					
Monitor	📴 Monitor					

Klicken sie nun auf Policy dann auf Outgoing fügen sie hier einen neuen Eintrag hinzu wie auf dem Screenshot zu sehen ist.

ALLNET		
	Baliau > Outacing	
🛅 System	Policy > Odigoing	
Therface Interface	Comment : Test	
Policy Object	Modify Policy	
	Source Address	Inside Any
	Destination Address	
WAN TO DMZ	Service	
L+ LAN TO DMZ	Cohedule	
DMZ TO WAN		
L DMZ TO LAN	Authentication User	
📴 Mail Security	Tunnel	lunnel_lest
🖸 IDP	Action	PERMIT
📴 Anomaly Flow IP	Traffic Log	Enable
📴 Monitor	Statistics	Enable
	IDP	Enable
	Content Blocking	
	MAX. Concurrent Sessions	
	QoS	None 💌
		OK Cancel

Wenn sie nun auf Outgoing klicken müssen sie die Action VPN an Stelle 1 setzen

ALLNET												
T Ductore	Policy > Outgoing				_	_		_	_	_		
oystem Vistoriana												
🖬 Interiace 🖬 Deligu Object		Source	Destination	Service	Action	1	ţ,	Optio	n		Configure	Move
Policy Object		Inside_Any	Outside_Any	ANY	VPN		Ø,				Modify Remove Pause	To 1 💌
L. Outgoing		ClientPCs	Outside_Any	Client-PCs	V		ø	Ľ	1		Modify Remove Pause	To 2 💌
_→ Incoming		PC03	Outside_Any	ClientPC_mit_VPN	1		\$	И	1		Modify Remove Pause	To 3 💌
- → WAN To DMZ		Server	Outside_Any	Server	1		ø	Ľ	1		Modify Remove Pause	To 4 💌
-→ LAN TO DMZ			1									
DMZ TO VVAN							New	Entry				
Mail Security												
IDP												
Anomaly Flow IP												
🖸 Monitor												

Klicken sie nun auf Policy dann auf Incoming fügen sie hier einen neuen Eintrag hinzu wie auf dem Screenshot zu sehen ist.

System Policy > Incoming	ALLNET			
Folicy Object Folicy Object Outgoing O	System Interface Policy Object Policy Object Policy Incoming Uncoming Unco	Policy ≥ Incoming Comment : Test Mddify Policy Source Address Destination Address Service Schedule Tunnel Action Traffic Log Statistics DP MAX. Concurrent Sessions QoS NAT	Outside_Any Inside_Any ANY ANY None Tunnel_Test PERMIT Enable Enable Enable Enable Enable Enable O None Enable O None	

Wenn sie nun auf Incoming klicken müssen sie die Action VPN an Stelle 1 setzen

ALLNET								
Svstem	Policy > Incom	ning						
Interface								
Policy Object		Source	Destination	Service	Action	Option	Configure	Move
Policy		Outside_Any	Inside_Any(Routing)	ANY	WPN		Modify Remove Pause	To 1 🔻
Outgoing								
Incoming						New Entry		
WAN TO DMZ								
♦ LAN To DMZ								
♦ DMZ To WAN								
DMZ TO LAN								
Mail Security								
IDP								
Anomaly Flow IP								
Monitor								

Einstellungen am VPN Client:

📀 Th Dateie	e GreenBow n <u>K</u> onfiguration	VPN Client		<u>_ ×</u>
AL	UNET VPN	Client	Networks based o Succ	on Information, ess, Friendship and more
R	Konsole	Authentisierur	ng	
٢	Parameter	Name (Phase 1)	CnxVpn1	
5	Verbindungen	Interface	×	-
= 🛃 К	Configuration	Zieladresse	217.57.8.123	
÷	CnxVpn1	Preshared Key	*****	
		Bestätigen		
		C Zertifikat	Zertifikat Verwaltung	
		IKE		Mehr
		Verschlüsselung	3DES -	
		Authentisierung	SHA -	
		Schlussel	DH1024 -	
•				Regeln anwenden
O VPN	betriebsbereit			

Klicken sie dann auf Mehr

Dateien Konfigura	w VPN Client tion <u>T</u> ools <u>?</u>	
	Fortgeschrittene Konf	on Information, ess, Friendship and more
💫 Konsole	Aggressive Mode	
Parameter	NAT Port	
S Verbindungen	Lokale ID	
🖻 🧔 Konfiguratior	Wert remote.de	
ia-₩ CnxVpn1	Type DNS	
	Entfernte ID	
	Wert home.de	
	Type DNS	Mehr
	Ok Abbruch	
- 		 Regeln anwenden
O VPN betriebsbereit	- <u>)</u>	

Fügen sie dann die Phase 2 hinzu.

ateien <u>K</u> onfiguratio	n <u>T</u> ools <u>?</u>		
	Client	Networks ba	sed on Information, Success, Friendship and n
A Konsole	IPSec Konfigu	ration	
🚱 Parameter	Name (Phase 2)	CnxVpn1	
🥰 Verbindungen	Lokale Adresse	192 . 168 .	1.55
- Konfiguration	Netzwerk Adresse	192 . 168 . 1	00.0
E-CnxVpn1	Netzwerk Mask	255 . 255 . 2	55 . 0
	ESP		
	Verschlüsselung	3DES 💌	Aktiv während
	Authentisierung	SHA 💌	Systemature
	Mode	Tunnel 💌	
	PFS Gruppe	DH1024 -	Tunnel Öffnen
			Regeln anwenden

Jetzt nur noch auf Tunnel öffnen klicken evtl. den VPN Client neu starten.