How to setup IPSec NAT traversal on DFL-860

Topology:



(1) We need to add a new service "TCP-UDP-ICMP-IPSEC".



(2) Choose "all_tcpudpicmp" and "ipsec-suite". "ipsec-suite" has IP protocol 50, 51 and UDP port 500 and 4500.

A Service Group is a collection of service objects, which can then be used by different policies in the system.						
General						
€) General						
Name: TCP-UDP-ICMP-IPSE						
€) Service Group						
Group members Availabe Availabe All_Service all_cerp all_cerp all_cerp all_cerp bootps chargen chargen chargen chargen						
Comments:						
OK Cancel						

(3) Because IPSec traffic is bidirectional. We need use new service "TCP-UDP-ICMP-IPSEC" for LAN to WAN rules and WAN to LAN rules. Because DFL-860 just do IPSec NAT traversal therefore we need to use SAT+ALLOW rule make IPSec traffic transmit to DFL-210.

DFL-260E IPSec remote endpoint is IP address 190.41.99.178.

DFL-860	An IP Rule F	wan1 older can be used to group IP Rules into logical grou	ps for better overview	and simplified management.				
Dijects	2 AM	dit this object						
E RAddress Book								
ALG with AV/WCF	#	Manag	A shine	Course Interferer	Course a strength	Prosting to the form	Production and sold	Canalas
Services	1	NAT_VPN	SAT	🔯 wan1	😌 all-nets	Ci core	😔 IPFWWan1	CP-UDP-ICMP-IPSEC
P Pools	2	NAT_VPN_Allow	Allow	🔯 wan1	😌 all-nets	Core	IPFWWan1	TCP-UDP-ICMP-IPSEC
	3	8 NAT-VPN-WAN2	SAT	🔀 wan2	😌 all-nets	Core	😌 IPFWWan2	TCP-UDP-ICMP-IPSEC
Contract Schedules	4	NAT-VPN-ALLOWZ	Allow	S3 wanz	all-nets	Eg core	1PFWWan2	TCP-UDP-ICMP-IPSEC
	5	§ Lan	NAT NAT	🔝 lan	😌 LanInternal_Agro	R Internet_Failover	😌 all-nets	TCP-UDP-ICMP-IPSEC
E 🙀 VPN Objects	6	g drop_smb-all	Drop	🔢 lan	😌 lannet	wan1	😸 all-nets	smb-all
HTTP Banner Files	7	allow_ping-outbound	NAT NAT	🔝 lan	😌 lannet	wan1	🗟 all-nets	ping-outbound
8 Rules	8	8 allow ftp-passthrough av	NAT	[3] lan	R lannet	Wan1	all-nets	ftp-passthrough-av
- \$ IP Rules	9	8 allow standard	NAT	153 Jan	lannet	Wan1	all-nets	all topudp
ian_to_wan1		• -			¥.		×.	
Access							0	Right-click on a row for additional option
Interfaces								
😽 Ethernet								

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.						
General Log Settings NAT SAT Multiplex SAT SLB SAT SLB Monitors						
2) General						
Name:	Name: NAT_VPN					
Action:	SAT	*				
Service:	Service: TCP-UDP-ICMP-IP V Sohedule: (None) V					
Sohedule:						
2 Address Filter						
Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.						
	Interface		Network			
Source:	wan1	*	all-nets 🗸			
Destination:	core	*	IPFWWan1 🗸			
2 Comments						

(4) IsaServer = IP address 10.1.1.2/24

8 NAT_VPN An IP rule specifies what action to perform on network traffic that matches the specified filter oriteria.	
General Log Settings NAT SAT Multiplex SAT SLB SAT SLB Monitors	
D General	
Translate the	
Source IP	
Destination IP	
to:	
New IP Address: IsaServer	
New Port: (1) This value may only be applied on TCP/UDP services with port set to either a single port number or a port range without gaps	
All-to-One Mapping: rewrite all destination IPs to a single IP	

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.							
General Log Settings NAT SAT Multiplex SAT SLB SAT SLB Monitors							
2) General							
Name:	Lan						
Action:	NAT	~					
Service:	TCP-UDP-ICMP-IP	*					
Schedule:	(None)	~	•				
		_					
划 Addre	彭 Address Filter						
Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.							
	Interface		Network				
Source:	lan	*	LanInternal_Agro				
Destination:	Internet_Failover	*	all-nets	✓			

(5) Go to advanced settings. Disable "IPSec before rule".

Ę	DFL-860	Settings for the lifes tunnel interfaces used for establishing Pieco VPI connections to and from this system.					
Ð	System	Oneset					
	Objects O	Seneral					
		IPsec Max Rules:	0	Amount of IPsec rules allowed (0 = automatic)			
		IPsec Max Tunnels:	0	Amount of IPsec tunnels allowed (0 × automatic)			
	Schedules	IKE Send Initial Contact:		Send 'initial contact' messages.			
	Authentication Objects Authentication Objects	IKE Send CRLs:		Send CRLs in the liKE exchange.			
		IPsec Before Rules:		Pass IKE & IPsec (ESP/AH) traffic sent to the security gateway directly to the IPsec engine without consulting the ruleset.			
	- Rules	IKE CRL Validity Time:	86400	Maximum number of seconds a CRL is considered valid (0+obey the 'next update' field in the CRL).			
	E- 8 IP Rules	IKE Max CA Path:	15	Maximum number of CA certificates in a certificate path.			
	lan_to_wan1	IPsec Certificate Cache Max Certs:	1024	Maximum number of entries in the certificate cache.			
		IPsec Gateway Name Cache Time:	14400	Amount of time to keep an IPsec tunnel open when the remote DNS name fails to resolve.			
		Dead Peer Detection	🕑 Dead Peer Detection				
		DPD Metric:	3	Metric 10s of seconds with no traffic or other evidence of life in tunnel before \$A is removed.			
		DPD Keep Time:	2	Number 10s of seconds a SA will remain in dead cache after a delete. DPD will not trigger if peer already is cached as dead.			
		DPD Expire Time:	15	Number of seconds that PRD.P.I.I.TuEDE measurement will be sent			
	- 1 PPTP/L2TP Clients			Homes of george data of the off-the function and a set of the set			



END