## Laboratorium 3

# Zaawansowana konfiguracja i zarządzanie zaporami sieciowymi D-Link NetDefend cz.3.

## 1. "Konfiguracja VLAN



192.168.1.20/24

Przywrócić domyślne ustawienia zapory. Skonfigurować VLAN o VLANID: 2 na przełączniku DES 3828 tak, by należał do niego co najmniej jeden port nietagowany i jeden port tagowany.

Na komputerze należącym do VLANu ręcznie ustawić adres IP z podsieci 192.168.11.0/24 gdzie brama domyślna ma adres 192.168.11.254 oraz ręcznie podać adresy serwerów DNS: DNS1: 157.158.3.1 DNS2: 157.158.3.2.

W książce adresowej utworzyć obiekty dla podsieci i interfejsu IP dla podsieci VLAN



Genera	ral User Authentication	
) Gene	eral	
Name:	VLAN2_net	
ddress:	192.168.11.0/24	
Com	vmonte	
Comi	iments Is:	

Dodać interfejs VLAN na konkretnym interfejsie fizycznym, określić VLAN ID, interfejs IP oraz sieć dla tworzonego interfejsu. Utworzyć regułę NAT maskującą ruch z VLANu do Internetu.

Genera	Log Settings	NAT	SAT Multiplex SAT
🕥 Genei	ral		
Name:	VLAN2_NAT		
Action:	NAT	~	
Service:	all_tcpudpicmp	~	
Schedule:	(None)	~	
Addre	ess Filter		
Specify so	urce interface and sourc	e network	together with destination interface and destination network. All parameters have to match for the rule to match.
	Source		Destination
terface:	VLAN_2	~	wan 💙

Zapisać i aktywować konfiguracje.

## 2. Połączenie VPN PPTP



Na potrzeby ćwiczenia przywrócić ustawienia domyślne zapory. W książce adresowej utworzyć obiekt dla serwera PPTP oraz obiekt z zakresem adresów IP przydzielanych klientom PPTP.

→ Ppy Aq			
lame 👻	Address 👻	User Auth Groups 👻	Comments 👻
🚽 all-nets	0.0.0/0		All possible networks
] InterfaceAddresses			
PPTPaddrrange	10.1.1.2-10.1.1.126		
PPTPservaddr	10.1.1.1		

Utworzyć lokalną bazę danych do uwierzytelniania użytkowników PPTP. Do utworzonej bazy danych dodać użytkownika wprowadzając jego nazwę oraz hasło.

General User	s			
Add 🛨				
lame	Groups	IP Pool	Networks	Comments
💁 student	pptpserv			
				(1) Right-click on a row for additional options

Utworzyć tunel PPTP i określić jego konfigurację. Wskazać adres IP serwera PPTP, protokół, Interfejs zewnętrzny. Wskazać pulę adresów jaka będzie przydzielana użytkownikom.

General	Parameters	Add Route	
) General			
Name:	PPTPtunel		
nner IP Address:	PPTPservaddr	~	
funnel Protocol:	РРТР	~	
Outer Interface Filter:	wan	~	
Server IP:	wan_ip	~	

Określić reguły uwierzytelniania użytkowników PPTP. Wybrać agenta uwierzytelniania, źródło danych uwierzytelniających, interfejs na którym będzie następować uwierzytelnianie.

General	Settings Au	thenticatio	n Options Accounting Agent Options Restrictions	
) General				
Name:	pptpauth			
Authentication agent:	PPP	~		
Authentication Source:	Local	*		
nterface:	PPTPtunel	*		
Originator IP:	all-nets	~	For XAuth and PPP, this is the tunnel originator IP.	

Utworzyć regułę IP (Allow) zezwalającą na ruch przez utworzony tunel PPTP.

Genera	Log Settings	NAT	SAT	Multiplex S	SAT										
🕥 Gene	ral														
Name:	pptpallow														
Action :	Allow	~													
Service:	all_services	~													
Schedule:	(None)	~													
<b>Addre</b> Specify so	e <b>ss Filter</b> urce interface and source Source	2 network	, together with des Destination	tination inte	rface a	nd de:	stinati	on netw	iork. All	paramete	ers have	e to ma	ntch fo	r the rul	e to mat
	PPTPtunel	~	lan	1	~										
iterrace:		The second se													

Zapisać i aktywować konfiguracje, Sprawdzić poprawność konfiguracji poprzez ustanowienie połączenia korzystając z klienta PPTP wbudowanego w system Windows XP.

#### 3. Połączenie VPN L2TP over IPSec



Na potrzeby ćwiczenia: przywrócić ustawienia domyślne. W książce adresowej utworzyć obiekt dla serwera L2TP oraz obiekt z zakresem adresów IP przydzielanych klientom L2TP.

Add 🛨			
lame 👻	Address 👻	User Auth Groups 👻	Comments 👻
all-nets	0.0.0/0		All possible networks
InterfaceAddresses			
🚽 L2TPaddr	10.1.1.1		

Utworzyć lokalną bazę danych do uwierzytelniania użytkowników L2TP. Do utworzonej bazy danych dodać użytkownika wprowadzając jego nazwę oraz hasło.

General Users		
Add 🛨		
	1000 / 1000 Parks	

W obiektach uwierzytelniania dodać nowy obiekt współdzielonego klucza IPSec.

L2TPprek	<b>ey</b> Key) autheritication is	baced on a shared secret that is known only by the parties involved
General	rey) admentication is	based on a shared secret that is known only by the parties involved.
🔊 General		
Name: L2TPpr	ekey	
·····	8	
Shared Secret	1) 	
Shared Secret:	•••••	Note! Existing passwords will always be shown with 8 characters to hide the actual length.

Utworzyć tunel IPSec. Wybrać odpowiednią: Sieć lokalną, Sieć zdalną, Zdalny węzeł, Typ enkapsulacji. Wybrać odpowiedni klucz IPSec dla tunelu. Ustawić odpowiednie opcje tras routingu.

General Aut	nentication X	Auth	Routing	E Settings	Keep-alive	Advanced	
🕥 General				Pre-s	hared Kev		
Name:	L2TPtunel			Pre-s	hared key:	L2TPprekey	×
Local Network:	wan_ip	~					- Notes
Remote Network:	all-nets	*		🛃 Rot	rting		
Remote Endpoint:	(None)	*		Alle	w DHCP over	IPsec from single-ho	ost clients
Encapsulation mode:	Transport	*		Dy Dy	namically add	route to the remote r	etwork when a tunnel is establish
IKE Config Mode Pool:	(None)	*					
) Algorithms				🔬 Auto	omatic Rou	te Creation	
Algorithms	Medium	~			cally add route	te Creation for remote network.	
Algorithms IKE Agorithms: IKE Lifetime:	Medium 28800	*	seconds	Automati Automati Automati Add	cally add route route for remo etric: 90	te Creation for remote network. ote network	
Algorithms IKE Agorithms: IKE Lifetime: IPsec Agorithms:	Medium 28800 Medium	~	seconds	Automati	cally add route route for remo etric: 90	te Creation for remote network. ote network	*
Algorithms IKE Agorithms: IKE Lifetime: IPsec Agorithms: IPsec Lifetime:	Medium 28800 Medium 3600	<ul> <li></li> <li></li> <li></li> <li></li> </ul>	seconds		omatic Rou cally add route route for reme atric: 90	te Creation for remote network. ote network	

Utworzyć tunel L2TP i określić jego konfigurację. Określić: adres IP serwera L2TP, protokół, Interfejs zewnętrzny. Wskazać pulę adresów jaka będzie przydzielana użytkownikom.

General PPF	Parameters	Add Route				
ງ General			🔬 IP Poo	ľ		
Name:	L2TPserv		IPPool:	L2TPrange	~	
Inner IP Address:	L2TPaddr	~		L	92289	
Tunnel Protocol:	L2TP	*				
Outer Interface Filter:	L2TPtunel	~				
Server IP:	wan_ip	~				

Określić reguły uwierzytelniania użytkowników L2TP. Określić: agenta uwierzytelniania, źródło danych uwierzytelniających, interfejs na którym będzie następować uwierzytelnianie.

General Log Settings Authentication			n Options Accounting Agent Options Restrictions
) General			
lame:	L2TP auth		
uthentication agent:	thentication agent: ppp		
uthentication Source:	Local	*	
nterface:	L2TPserv	~	

Utworzyć regułę IP (Allow) zezwalającą na ruch przez utworzony tunel L2TP. Wybrać odpowiednie: Usługę, Interfejs i Sieć.

8 L21 An IP	Pallow rule specifies what a	ction to perfo	orm on network traf	fic that matches t	e specified 1	filter criteria.		_	
Genera	Log Settings	NAT	SAL	IUITIPIEX SAT					
🛐 Gener	al								
Name:	L2TPallow								
Action:	Allow	~							
Service:	all_services	~							
Schedule:	(None)	~							
Addre	ess Filter								
specity sou	urce interface and sol	urce network	, together with desti	nation interface ar	ia destination	n network. All	parameters hav	ve to match fo	or the rule to match.
5 B	Source	100	Destination						
nterface:	L2TPserv	*	lan	*					
vetwork:	L2TPrange	*	lannet	~					

Zapisać i aktywować konfiguracje. Sprawdzić poprawność konfiguracji poprzez ustanowienie połączenia VPN za pomocą klienta wbudowanego w system Windows.

### 4. Połączenie VPN LAN-to-LAN IPSec (split)



Na potrzeby ćwiczenia przywrócić ustawienia domyślne. W książce adresowej utworzyć obiekty dla zdalnej sieci LAN i zdalnego węzła.

P Use a	Address n IP4 Address item to define a name f	a specific IP4 host, network or range	a.		
General	User Authentication				
🔬 Gener	al				
Name:	REMOTE_HOST				
Address:	10.10.2.116				
Vise ar	Address n IP4 Address item to define a name fo	a specific IP4 host, network or range	1.		
General	User Authentication				
🔬 Gener	al				
Name:	REMOTE_NET				
Address:	192.168.1.0/24				

W obiektach uwierzytelniania dodaj nowy obiekt współdzielonego klucza IPSec.

Rec_p	re-shared_KE	ised on a shared secret that is known only by the parties involved.	
General			
🔬 General			
Name: IPSe	c_pre-shared_KE		
Shared Sector	ret		
Passphrase			_
Shared Secret	•••••	Note! Existing passwords will always be shown with 8 characters to hide the actual length.	
Confirm Secre	t:		

Utworzyć tunel IPSec. Wybrać odpowiednią: Sieć lokalną, Sieć zdalną, Zdalny węzeł, Typ enkapsulacji. Wybrać odpowiedni klucz IPSec dla tunelu.

👌 IPsec Tun	nel	naa andraint und wi	ll announ an a lociont	listadaan in the sur			
General Auth	nentication XAu	th Routing	IKE Settings	Keep-alive	Advanced		
) General							
Name:	IPSec_tunnel						
Local Network:	lannet	~					
Remote Network:	REMOTE_NET	~					
Remote Endpoint:	REMOTE_HOST	*					
Encapsulation mode:	Tunnel	~					
IKE Config Mode Pool:	(None)	*					
🔰 Algorithms							
IKE Algorithms:	(None)	*					
IKE Lifetime:	28800	seconds					
IPsec Algorithms:	(None)	*					
IPsec Lifetime:	3600	seconds					
IPsec Lifetime:	0	kilobytes					

Połączyć obydwa interfejsy w jedną grupę. Połączenie interfejsów w grupę pozwala na minimalizację liczby reguł obsługujących ruch w obydwu kierunkach.

USE an interface group to combine se	everal interfaces for a simplified security policy.
General	
ᢧ General	
Name: IPSEC-lan	
Security/Transport Equivalent	
Interfaces	
Available	Selected
core	IDSec turnel
1222	Trace united and the second se
dmz wan	
dmz wan	>>>
dmz wan	irsec_umei lan →>> <<
dmz wan	>>> <<

Utworzyć regułę IP (Allow) dla tunelu zezwalającą na ruch przez tunel IPSec. Wybrać odpowiednie: Usługę, Interfejs, Sieć.

S IP I An IP	<b>{UIC</b> rule specifies what ac	ation to perfo	rm on network traffic	t matches the specified filter oriteria.			
Genera	I Log Settings	NAT	SAT Mult	ex SAT			
🛃 Gener	ral						
Name:	IPSec-allow						
Action:	Allow	~					
Service:	all_services	~					
Schedule:	(None)	~					
🔊 Addre	ess Filter						
Specify so	urce interface and sou	urce network	, together with destinat	interface and destination network. All paramet	ers have to match for the rule to n	natch.	
	Source		Destination				
Interface:	IPSEC-lan	~	IPSEC-lan	*			
Network:	all-nets	*	all-nets	~			

Zapisać i aktywować konfiguracje.