



Router GSM MIDGE

(Ma zastosowanie również do MG102i)

Analiza ruchu sieciowego / Wireshark

Wersja oprogramowania:

3.6.40.109

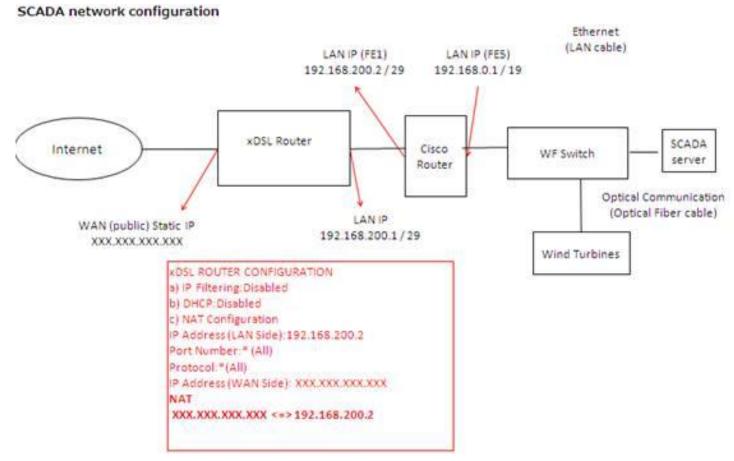
Data doku	mentu:	13 marca 2014	Aktualizacja: 3.02.2014r	Wersja 1.2
Przygoto	wał:	Jan Batycki	support@karczpolska.pl	61 827 30 90
Zweryfik	ował:	Krzysztof Karcz	support@karczpolska.pl	61 827 30 90

Analiza ruchu sieciowego M!DGE/Wireshark, sprawdzanie portu komunikacyjnego.

W routerach M!DGE/MG102i mamy do dyspozycji bardzo ciekawą funkcję służącą do analizy ruchu w sieci. Narzędzie tcpdump. Generuje ono pliki PCAP (przechwytywania sieci) które możemy później analizować programem Wireshark (<u>http://www.wireshark.org/</u>). Dokumentacja do programu dostępna <u>http://www.wireshark.org/docs/wsug_html_chunked/</u>



W poniższym przykładzie przedstawię opis rozwiązania problemu u naszego klienta. Router **M!DGE** dostarcza Internet, za routerem znajduje się drugi router CISCO obsługujący zabezpieczoną sieć VPN. Za routerem CISCO znajdują się urządzenia sieciowe. Problemem był brak informacji ze strony klienta na jakich portach pracuje VPN i CISCO. Rozwiązaniem było przekierowanie całego ruchu sieciowego z M!DGE na CISO, jednak pozbawiało nas to możliwości kontroli i konfiguracji routera M!DGE, np. uruchomienia dodatkowych usług diagnostycznych dla Klienta.



Rys.: Konfiguracja sieci u klienta

M!DGE



	HUME INTERFA	CES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT				
System Settings	- Network Debugging					
Time & Region System Information Restart		ererates a network capture (PCAP) of an interface which can be later analyzed with				
Authentication Authentication	Wireshark.					
User Accounts Remote Authentication	Interface:	WWAN1 -				
Software Update Manual Software Update Automatic Software Update	Exclude:	☐ http ☐ https ☐ teinet ☐ ssh				
Configuration Manual File Configuration Automatic File Configuration Factory Configuration	Start					
Troubleshooting Network Debugging System Debugging Tech Support						
Keys & Certificates						
Licensing						

HOME A INTEREACES A DOUTING A FIREWARK A VENA SERVICES A SYSTEM A LOCOUT

Rys.: Wybór interfejsu do skanowania

Analizę ruchu możemy przeprowadzać na interfejsach (interface) WWAN, LAN1 i LAN2. Aby zmniejszyć ilość danych możemy wykluczyć (exclude) nie interesujące nas protokoły np. http, https, telnet, ssh. W przypadku naszego klienta monitorowaliśmy ruch na interfejsie LAN1.

Po wybraniu interfejsu który chcemy obserwować klikamy na start.

		_	_
///!	D	G	



	HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT
System Settings	Network Debugging
Time & Region System Information Restart	ping traceroute tcpdump darkstat
Authentication	tcpdump: listening on wwwanO, link-type LINUX_SLL (Linux cooked), capture size 1500 by
Authentication User Accounts	Captured 29 packets
Remote Authentication	
Software Update	
Manual Software Update	
Automatic Software Update	
Configuration	
Manual File Configuration	
Automatic File Configuration	Stop
Factory Configuration	
Troubleshooting	
Network Debugging	
System Debugging Tech Support	
Keys & Certificates	
Licensing	

Rys.: Capture

Powinniśmy zobaczyć poniższe informacje:

tcpdump: listening on wwan0, link-type LINUX_SLL (Linux cooked), capture size 1500 bytes

Captured 221 packets

MIDGE



	HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT
System Settings Time & Region System Information Restart	Network Debugging ping traceroute tcpdump darkstat
Authentication Authentication User Accounts Remote Authentication	tcpdump: Listening on wwanO, link-type LINUX_SLL (Linux cooked), capture size 1500 by 499 packets received by filter O packets dropped by kernel
Software Update Manual Software Update Automatic Software Update	Captured 499 packets
Configuration Manual File Configuration Automatic File Configuration Factory Configuration	Run again Download
Troubleshooting Network Debugging System Debugging Tech Support	
Keys & Certificates	
Licensing	

Rys.: Download

Jeśli liczba przechwyconych pakietów nam odpowiada klikamy na stop, możemy teraz kliknąć na **download** i pobrać plik przechwytywania, ma o nazwę "tcpdump.pcap"

N!DGE	
System Settings Time & Region System Information Restart	Home Interfaces Routing Firewall VPN Services SYSTEM Logout Network Debugging ping traceroute topdump darkstat
Authentication Authentication User Accounts Remote Authentication	tcpdump: listening on wwwanO, link-type LIMUX_SLL (Linux cooked), capture size 1500 by 301 packets received by filter 0 packets dropped by kernel
Software Update Manual Software Update Automatic Software Update	Captured 300 packets Otwieranie topdump.pcap XI Rozpoczęto pobieranie piłku: XI
Configuration Manual File Configuration Automatic File	Typ pilus: Wreshark capture file (76,4 KB) Adres: http://
Configuration Factory Configuration	Run again Download Po zakończeniu pobierania: • Ottwórz za pognocą Wireshark (domyślny) C Zapisz plik • Zapisz plik • Zapisz plik
Troubleshooting Network Debugging System Debugging Tech Support	Capiez pik.
Keys & Certificates	OK Anuluj
Licensing	

Rys.: Zapisywanie pliku do wireshark

Taki plik możemy otworzyć programem Wireshark i przystąpić do analizy. Dostępne informacje które podaje nam program to: numer, czas, źródło pakietu, cel pakietu, protokół, długość i opis:

1 0.00000041.61.144.231 25.50.116.222 TCP 1276 [TCP segment of a reassembled PDU]

Po kliknięciu na wybraną pozycję dodatkowo możemy sprawdzić np. port komunikacyjny na jakim odbywa się transmisja. Port zarówno źródłowy jak i docelowy np.:

User Datagram Protocol, Src Port: ipsec-nat-t (4500), Dst Port: ipsec-nat-t (4500) User Datagram Protocol, Src Port: isakmp (500), Dst Port: 53471 (53471)

<u>E</u> dit ⊻iew 9		Wireshark 1.10.5 (SVN Rev 54 itatistics Telephony <u>T</u> ools Int			_ 8
	<u> </u>			D. 🔟 🙀 🗹 🥵 % 💢	
r:			Expression Clear Apply	Save	
Time	Source	Destination	Protocol	Length Info	
1 0.0000			ISAKMP	458 Aggressive	
2 1.2064			ISAKMP	138 Informational 138 Informational	
3 1.2091 4 2.9564			ISAKMP ISAKMP	47 NAT Keepalive	
5 6.1666			UDP	58 Source port: 53470 Destination port: 62515	
	76 192.168.200.		ICMP	70 Destination unreachable (Port unreachable)	
7 6.1966			ISAKMP	910 Aggressive	
8 6.2220			ISAKMP	458 Aggressive	
9 6.3664			ISAKMP	138 Informational	
	92 192.168.200.		ISAKMP	138 Informational	
	244 192.168.200. 449 192.168.200.		ISAKMP ISAKMP	458 Aggressive 138 Informational	
	147 192.168.200.		ISAKMP	138 Informational	
	439 192.168.200.		ISAKMP	47 NAT Keepalive	
	418 192.168.200.		ESP	142 ESP (SPI=0x8e103320)	
	011 192.168.200.		ESP	126 ESP (SPI=0x2d4b8b27)	
17 15.796	424 192.168.200.	1 192.168.200.2	ESP	118 ESP (SPI=0x8e103320)	
	086 192.168.200.		ESP	174 ESP (SPI=0x2d4b8b27)	
	409 192.168.200.		ISAKMP	458 Aggressive	
	463 192.168.200.		ESP	126 ESP (SPI=0x8e103320)	
	064 192.168.200. 065 192.168.200.		ESP ESP	142 ESP (SPI=0x2d4b8b27) 126 ESP (SPI=0x2d4b8b27)	
	687 192.168.200.		ESP	118 ESP (SPI=0X20408027)	
	423 192.168.200.		ESP	134 ESP (SPI=0x8e103320)	
	924 192.168.200.		ESP	134 ESP (SPI=0x2d4b8b27)	
26 20.000	476 192.168.200.		ISAKMP	458 Aggressive	
27 20.076	707 192.168.200.	1 192.168.200.2	ESP	126 ESP (SPI=0x8e103320)	
	20 h. +	(1104 bits) 130 bits			
			s captured (1104 bits)	77.76 (20.82.60.03.77.7)	
		F•/0•00 (00•07•30•ff•			
thernet II	, Src: RacomSRO_f	f:c9:00 (00:02:a9:ff: src: 192.168.200.1 (
thernet II nternet Pr	, Src: RacomSRO_f otocol Version 4,	src: 192.168.200.1 (192.168.200.1), Dst: 19	92.168.200.2 (192.168.200.2)	
thernet II hternet Pr ser Datagr	, Src: RacomSRO_f otocol Version 4,	Src: 192.168.200.1 (Port: ipsec-nat-t <mark>(45</mark>		92.168.200.2 (192.168.200.2)	
hernet II Iternet Pr Pr Datagr P Encapsu	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F	Src: 192.168.200.1 (Port: ipsec-nat-t <mark>(45</mark>	192.168.200.1), Dst: 19 0 <mark>0)</mark> , Dst Port: ipsec-na	92.168.200.2 (192.168.200.2)	
thernet II nternet Pr ser Datagr DP Encapsu	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F	Src: 192.168.200.1 (Port: ipsec-nat-t <mark>(45</mark> ackets	192.168.200.1), Dst: 19 0 <mark>0)</mark> , Dst Port: ipsec-na	92.168.200.2 (192.168.200.2)	
hernet II Iternet Pr Pr Datagr P Encapsu	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F	Src: 192.168.200.1 (Port: ipsec-nat-t <mark>(45</mark> ackets	192.168.200.1), Dst: 19 0 <mark>0)</mark> , Dst Port: ipsec-na	92.168.200.2 (192.168.200.2)	
hernet II Iternet Pr Pr Datagr P Encapsu	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F	Src: 192.168.200.1 (Port: ipsec-nat-t <mark>(45</mark> ackets	192.168.200.1), Dst: 19 0 <mark>0)</mark> , Dst Port: ipsec-na	92.168.200.2 (192.168.200.2)	
hernet II ternet Pr er Datagr P Encapsu	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F	Src: 192.168.200.1 (Port: ipsec-nat-t <mark>(45</mark> ackets	192.168.200.1), Dst: 19 0 <mark>0)</mark> , Dst Port: ipsec-na	92.168.200.2 (192.168.200.2)	
hernet II ternet Pr er Datagr P Encapsu	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F	Src: 192.168.200.1 (Port: ipsec-nat-t <mark>(45</mark> ackets	192.168.200.1), Dst: 19 0 <mark>0)</mark> , Dst Port: ipsec-na	92.168.200.2 (192.168.200.2)	
hernet II ternet Pr er Datagr P Encapsu	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F	Src: 192.168.200.1 (Port: ipsec-nat-t <mark>(45</mark> ackets	192.168.200.1), Dst: 19 0 <mark>0)</mark> , Dst Port: ipsec-na	92.168.200.2 (192.168.200.2)	
hernet II ternet Pr er Datagr P Encapsu	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F	Src: 192.168.200.1 (Port: ipsec-nat-t <mark>(45</mark> ackets	192.168.200.1), Dst: 19 0 <mark>0)</mark> , Dst Port: ipsec-na	92.168.200.2 (192.168.200.2)	
hernet II ternet Pr er Datagr P Encapsu	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F	Src: 192.168.200.1 (Port: ipsec-nat-t <mark>(45</mark> ackets	192.168.200.1), Dst: 19 0 <mark>0)</mark> , Dst Port: ipsec-na	92.168.200.2 (192.168.200.2)	
hernet II ternet Pr er Datagr P Encapsu	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F	Src: 192.168.200.1 (Port: ipsec-nat-t <mark>(45</mark> ackets	192.168.200.1), Dst: 19 0 <mark>0)</mark> , Dst Port: ipsec-na	92.168.200.2 (192.168.200.2)	
hernet II Iternet Pr Pr Datagr P Encapsu	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F	Src: 192.168.200.1 (Port: ipsec-nat-t <mark>(45</mark> ackets	192.168.200.1), Dst: 19 0 <mark>0)</mark> , Dst Port: ipsec-na	92.168.200.2 (192.168.200.2)	
chernet II Iternet Pr Ser Datagr OP Encapsu	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F	Src: 192.168.200.1 (Port: ipsec-nat-t <mark>(45</mark> ackets	192.168.200.1), Dst: 19 0 <mark>0)</mark> , Dst Port: ipsec-na	92.168.200.2 (192.168.200.2)	
thernet II nternet Pr ser Datagr DP Encapsu	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F	Src: 192.168.200.1 (Port: ipsec-nat-t <mark>(45</mark> ackets	192.168.200.1), Dst: 19 0 <mark>0)</mark> , Dst Port: ipsec-na	92.168.200.2 (192.168.200.2)	
thernet II nternet Pr ser Datagr DP Encapsu	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F	Src: 192.168.200.1 (Port: ipsec-nat-t <mark>(45</mark> ackets	192.168.200.1), Dst: 19 0 <mark>0)</mark> , Dst Port: ipsec-na	92.168.200.2 (192.168.200.2)	
thernet II nternet Pr ser Datagr DP Encapsu	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F	Src: 192.168.200.1 (Port: ipsec-nat-t <mark>(45</mark> ackets	192.168.200.1), Dst: 19 0 <mark>0)</mark> , Dst Port: ipsec-na	92.168.200.2 (192.168.200.2)	
thernet II nternet Pgr Ser Datagr DP Encapsu nternet Se	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F curity Associatio	src: 192.168.200.1 (Port: ipsec-nat-t (45 ackets n and Key Management	192.168.200.1), Dst: 1 0 <mark>0)</mark> , Dst Port: ipsec-na Protocol	22.168.200.2 (192.168.200.2) at-t (4500)	
thernet II nternet Pr ser Datapsu DP Encapsu nternet Se	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F curity Associatic	Src: 192.168.200.1 (Port: ipsec-nat-t (45 ackets in and Key Management and Key Management ff c9 00 08 00 45 f6 36 c0 a8 c8 01 c0	00 [°] .r+E. a8 . ~4. 6	22.168.200.2 (192.168.200.2) at-t (4500)	
thernet II nternet Pr Ser Datagr DP Encapsu nternet Se 0 c0 8c 6 0 00 7c 7. 0 c8 02 1	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F curity Associatio 0 93 72 2b 00 02 e e5 00 00 34 11 94 11 94 00 68	Src: 192.168.200.1 (Port: ipsec-nat-t (45 ackets n and Key Management a9 ff c9 00 08 00 45 f6 36 c0 a8 c8 01 c0 a6 49 00 00 00 00 43	00`.r+E. 8E. 8	32.168.200.2 (192.168.200.2) at-τ (4500)	
:hernet II iternet Pr ser Datapsu pP Encapsu iternet Se 0 00 7c 7: 0 00 72 30 3	, Srć: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F curity Associatic curity Associatic 0 93 72 2b 00 02 e e5 00 00 34 11 1 94 11 94 00 68 9 13 a5 80 90 c4	src: 192.168.200.1 (Port: ipsec-nat-t (45 ackers n and Key Management a9 ff c9 00 08 00 45 f6 36 c0 a8 c8 01 c0 a6 49 00 00 00 00 43 48 d8 25 52 3d 41 08 00 5c 2f 1a 6b d9 e5	00`.r+E. 80`.r+E. 90`.r+E. 90`.r+E. 90`.r+E. 90`E. 90E. 90E. 90E. 90E. 90E. 90	22.168.200.2 (192.168.200.2) at-t (4500)	
0 c0 8c 6 0 c0 8c 6 0 c0 7 0 c0 8c 6 0 c0 7 0 c0	, Src: RacomSRO_f otocol Version 4, am Protocol, Src lation of IPsec F curity Associatic e 5 00 00 34 11 1 94 11 94 00 68 9 13 a5 84 90 c4 6 3b 64 31 00 00	src: 192.168.200.1 (Port: ipsec-nat-t (45 ackets n and Key Management 49 ff c9 00 08 00 45 f6 36 c0 a8 c8 01 c0 a6 49 00 00 00 00 43 48 d8 25 23 d4 10 00 5c 2f 1a 6b d9 e5 c 77.0 2 00 c6 12	00`.r+E. 80`.r+E. 90`.r+E. 90`.r+E. 90`.r+E. 90`E. 90E. 90E. 90E. 90E. 90E. 90	22.168.200.2 (192.168.200.2) at-t (4500)	

Rys.: Wireshark analiza

			[Wireshark 1.10.5 (SVN Rev 54 Statistics Telephony Tools In			_ 8
			2 addades Telephony Tools In		L Q. Q. 🔟 🕷 🗹 🥵 % 🛱	
: [e					
•]	1	1-	(-			
_	Time 1 0.000000	50urce 192.168.200.	Destination 2 192.168.200.1	Protocol ISAKMP	Length Info 458 Aggressive	
	2 1.206448	192.168.200.		ISAKMP	138 Informational	
	3 1.209195	192.168.200.		ISAKMP	138 Informational	
		192.168.200.	1 192.168.200.2	ISAKMP	47 NAT Keepalive	
		192.168.200.		UDP	58 Source port: 53470 Destination port: 62515	
	6 6.167476			ICMP	70 Destination unreachable (Port unreachable)	
	7 6.196619	192.168.200.		ISAKMP	910 Aggressive	
	8 6.222058	192.168.200.		ISAKMP	458 Aggressive	
		192.168.200. 192.168.200.		ISAKMP ISAKMP	138 Informational 138 Informational	
		192.168.200.		ISAKMP	458 Aggressive	
		9 192.168.200.		ISAKMP	138 Informational	
		192.168.200.		ISAKMP	138 Informational	
		9 192.168.200.		ISAKMP	47 NAT Keepalive	
1	5 14.926418	3 192.168.200.	1 192.168.200.2	ESP	142 ESP (SPI=0x8e103320)	
		. 192.168.200.		ESP	126 ESP (SPI=0x2d4b8b27)	
		192.168.200.		ESP	118 ESP (SPI=0x8e103320)	
		5 192.168.200.		ESP	174 ESP (SPI=0x2d4b8b27)	
		192.168.200. 192.168.200.		ISAKMP ESP	458 Aggressive	
		192.168.200.		ESP	126 ESP (SPI=0x8e103320) 142 ESP (SPI=0x2d4b8b27)	
		192.168.200.		ESP	126 ESP (SPI=0x2d4b8b27)	
		192.168.200.		ESP	118 ESP (SPI=0x8e103320)	
		192.168.200.		ESP	134 ESP (SPI=0x8e103320)	
2	5 19.237924	192.168.200.	2 192.168.200.1	ESP	134 ESP (SPI=0x2d4b8b27)	
2	6 20.000476	5 192.168.200.	.2 192.168.200.1	ISAKMP	458 Aggressive	
	2 20 076707	192.168.200.	1 192.168.200.2	ESP	126 ESP (SPI=0x8e103320)	
2	20.076707					
2	.7 20.076707					
_		ytes on wire	(7280 bits), 910 bytes	captured (7280	pits)	
ar he	me 7: 910 bj ernet II, S	rc: RacomSRO_	ff:c9:00 (00:02:a9:ff:	c9:00), Dst: Cis	zo_93:72:2b (c0:8c:60:93:72:2b)	
ar h	me 7: 910 b ernet II, S ernet Proto	col version 4	ff:c9:00 (00:02:a9:ff: , Src: 192.168.200.1 (c9:00), Dst: Cis 192.168.200.1), I	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar the	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , src: 192.168.200.1 (Port: 53471 (53471),	c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar hi	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , Src: 192.168.200.1 (c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar hi ti	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , src: 192.168.200.1 (Port: 53471 (53471),	c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar hi ti	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , src: 192.168.200.1 (Port: 53471 (53471),	c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar hi ti	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , src: 192.168.200.1 (Port: 53471 (53471),	c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar hi ti	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , src: 192.168.200.1 (Port: 53471 (53471),	c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar hi	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , src: 192.168.200.1 (Port: 53471 (53471),	c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar hi ti	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , src: 192.168.200.1 (Port: 53471 (53471),	c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar hi ti	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , src: 192.168.200.1 (Port: 53471 (53471),	c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar hi	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , src: 192.168.200.1 (Port: 53471 (53471),	c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar hi	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , src: 192.168.200.1 (Port: 53471 (53471),	c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar hi	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , src: 192.168.200.1 (Port: 53471 (53471),	c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar hi	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , src: 192.168.200.1 (Port: 53471 (53471),	c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar hi ti	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , src: 192.168.200.1 (Port: 53471 (53471),	c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar hi ti	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , src: 192.168.200.1 (Port: 53471 (53471),	c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar hi	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , src: 192.168.200.1 (Port: 53471 (53471),	c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar hi	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , src: 192.168.200.1 (Port: 53471 (53471),	c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
ar hi	me 7: 910 b ernet II, S ernet Proto r Datagram I	rc: RacomSRO_ col Version 4 Protocol, Src	ff:c9:00 (00:02:a9:ff: , src: 192.168.200.1 (Port: 53471 (53471),	c9:00), Dst: Cis 192.168.200.1), I Dst Port: isakmp	co_93:72:2b (c0:8c:60:93:72:2b) Dst: 192.168.200.2 (192.168.200.2)	
int i	me 7: 910 b ernet II, S ernet Proto r Datagram ernet Secur	rc: RacomSRO col Version 4 Protocol, Src ity Associati	ff:c9:00 (00:02:a9.ff; , src: 192.168.200.1 (Port: 53471 (53471), on and Key Management	<pre>c9:00), bst: c1s; 192.168.200.1), 1 bst Port: isakmp Protocol</pre>	co_93:72:2b (c0:8c:60:93:72:2b) yst: 192.168.200.2 (192.168.200.2) (500)	
nt (c0 8c 60 9 03 80 12 1	irc: RacomSRO iccl Version 4 Protocol, Src ity Associati 3 72 2b 00 02 a 00 00 74 11	ff:c9:00 (00:02:a0;ff; , src: 192.168.200.1 (Port: 53471 (53471), on and Key Management a9 ff c9 00 08 00 45 1f fe c0 a8 c8 01 cc	<pre>c9:00), bst: c1s; 192.168.200.1), 1 bst Port: isakmp Protocol 00'.r+ a8t.</pre>	zo_93:72:2b (c0:8c:60:93:72:2b) pst: 192.168.200.2 (192.168.200.2) (500)	
nt e	c0 8c 60 9 03 80 12 1	rc: RacomSRO col Version 4 Protocol, Src ity Associati	a9 ff c9 00 08 00 45 a9 ff c9 00 08 00 45 a9 ff c9 00 71 ff fe c0 a8 c8 01 c0	<pre>c9:00), bst: c1s; 192.168.200.1), 1 bst Port: isakmp Protocol 00r+ a8t. c61</pre>	co_93:72:2b (c0:8c:60:93:72:2b) yst: 192.168.200.2 (192.168.200.2) (500)	
ar the rent	c0 8c 60 9 0 38 12 1 0 38 12 1 0 38 12 1 0 38 12 1 1 58 02 10 1 58 64 00 0 0 00 00 00		a9 ff c9 00 08 00 45 a9 ff c9 00 08 00 45 a1 fe c0 a8 c8 01 cc b1 c0 b1 c0 11 c0 40 00 cc	<pre>c9:00), bst: c1s; 192.168.200.1), 1 bst Port: fsakmp Protocol 00r+ a8t. c61 [00 xd [00 xd</pre>	zo_93:72:2b (c0:8c:60:93:72:2b) pst: 192.168.200.2 (192.168.200.2) (500)	

Rys.: Wireshark analiza cd.

Dzięki powyższej analizie ustaliśmy że porty które należy przekierować to: 500 i 4500 poniżej przykład przekierowania ruchu z WAN na odpowiednie IP w LAN.

M!DGE



irewall Administration	NAPT Rules Inbound						
Groups	This menu can be used to configure network address/port translation rules for inbound packets.						
Rules	Description	Interface	Target	Redirect to			
NAPT	CISCO VPN1	WAN	UDP ports 500-500	192.168.200.2			
Administration Inbound Rules	CISCO VPN2	WAN	TCP ports 500-500	192.168.200.2			
Outbound Rules	CISCO VPN3	WAN	UDP ports 4500-4500	192.168.200.2			
	CISCO VPN4	WAN	TCP ports 4500-4500	192.168.200.2			
					Ŧ		

Clear

Rys.: Przykładowe przekierowanie portów