

Tunele IPSec

Schemat komunikacyjny

- Zaoenie jest do proste utrzymujemy stale kilka tuneli z partnerami dziki czemu przecazanie ruchu w razie problemów odbywa si pynnij.
- Hosty z SUBNETU 10.168.2.0 bd widziane u partnera w TUNELU o PEER IP 54.171.102.133 chyba e tunel ten nie dziaa (Sprawdzamy w ORION -> **Monitoring Tuneli - Raport** - odnoniki poniej kolumnie **MONITORING**)
- Pojawi si mog dodatkowe pytania
 - na jaki adress dana usuga si czy (sprawdzamy usug oraz SPIS ACL w opisie poszczególnych tuneli)
 - z jakiego adresu wasza usuga czy si do naszej (ta informacja równie znajduje si w opisie tuneli, jest to spis ACLEK. Do danego IP po stronie klienta jest przypisany obecnie 1 adres EIP nalecy do nas - wystarczy wejs w opis tunelu - kolumna **DESCRIPTION**)
 - w tym przypadku jeli dziaaj oba tunele tzn e ruch wychodzi tak jak na powyszym rysunku, moe si zdaj e w danym momencie który tunel bdzie lea a to oznacza e ruch z sieci w której macierzysty router nie moe przekaza ruchu do klienta skieruje go na router z sieci ssiedniej. Dlatego te w opisie macie dwie tabele dla obu tuneli zróónymi ACLkami (prawie zawsze). Warto wic albo sprawdzi gdzie odpalon macie usug i nastpnie zajrze do opisu tunelu albo poda oba adresy IP za którymi widoczny moe by nasz ruch. Przypadk poniej.

DIGITAL VIRGO .X.CONFERENCE Spaces • People Browse • Create

IKE SA Lifetime [seconds]	86400 28800	86400
Xauth	disabled	
Mode Config.	disabled	
IPSec - Phase 2	Digital Virgo SA	PLUS
Transform (IPSec protocol)	ESP	
Perfect Forward Secrecy - IPSec	Group2	Group2
Encryption algorithm - IPSec	AES256 AES128 3DES	AES256
Hashing algorithm - IPSec	SHA1	SHA1
IPSec SA Lifetime [seconds]	3600	3600
IPSec SA Lifetime [kilobytes]	4608000	4608000
Aggressive Mode Support	No	
Encryption Traffic (IP ACL)	Digital Virgo SA	PLUS
S2.19.20.145	212.2.118.15	
S2.19.20.145	212.2.118.11	
S2.19.20.145	212.2.103.222	
S2.19.20.145	212.2.118.14	
S2.19.20.145	192.168.7.38	
S2.19.20.145	212.2.118.6	
S2.19.20.145	212.2.118.7	
S2.19.20.145	212.2.118.6	
S2.19.20.145	212.2.96.83	
S2.19.20.145	212.2.96.82	
S2.19.20.145	212.2.96.67	
S2.19.20.145	212.2.96.80	
S2.19.20.145	192.168.5.162	
S2.19.20.145	192.168.5.163	
S2.19.20.145	212.2.96.65	
S2.19.20.145	212.2.103.215	
S2.19.20.145	212.2.122.19	
S2.19.20.145	212.2.122.20	
S2.19.20.145	212.2.119.157	
S2.19.20.145	212.2.119.158	
S2.19.20.145	212.2.119.154	
S2.19.20.145	212.2.119.155	
S2.19.20.145	212.2.122.90	
S2.19.20.145	212.2.122.91	
S2.19.20.145	212.2.123.16	
S2.19.20.145	212.2.123.17	
S2.19.20.145	212.2.96.223	
S2.19.20.145	212.2.96.134	
S2.19.20.145	212.2.96.135	
S2.19.20.145	212.2.123.14	
S2.19.20.145	212.2.123.15	
S2.19.26.251	212.2.126.203	
S2.18.127.155	212.2.123.242	
S2.18.127.155	212.2.123.240	
S2.18.127.155	212.2.123.241	

Like Be the first to like this

Write a comment...

Powered by Atlassian Confluence 5.7, Team Collaboration Software - Report a bug - Atlassian News

SPIS tuneli (powinien zgadzac si z list w systemie monitoringu)

LP	RTR-AWS-A 54.171.102.133	RTR-AWS-B 54.171.234.183	DESCRIPTION	MONITORING	crypto map id	IKE version	KONTAKT	NOTES
1	160.218.24.2	160.218.24.2	O2SK	Orion - O2SK	700	v1		

2	195.8.220.199	195.8.220.199	Teleaudio	Orion - Teleaudio	800	v1		
3	212.2.102.235	212.2.102.235	PLUS	Orion - PLUS	900	v1		
4	91.212.223.1	91.212.223.1*	Orlen	Orion - Orlen	1000	v1		
5	212.160.172.46	212.160.172.46	Orange	Orion - Orange	1500	v1		
6	31.186.83.35	31.186.83.35	Newaxis (O2O)	Orion - Newaxis - One2One	1650	v1		
7	193.109.244.139	193.109.244.139	PZU	Orion - PZU	1900	v2		
8	89.108.203.12	89.108.203.12	Play #2	Orion - Play 2	2100	v1		
9	188.40.109.77	188.40.109.77	Mobartis	Orion - Mobartis	2300	v1		
10	217.149.242.17	217.149.242.17	NVT	Orion - NVT	2400	v1		
11	195.69.124.88	195.69.124.88	Asseco (P4, DRQ)	Orion - Asseco	2500	v1		
12	85.120.83.67	85.120.83.67	Telekom Romania	Orion - Telekom Romania	2600	v1		
13	83.220.126.243	83.220.126.243	T-MOBILE [PL]	Orion - T-Mobile PL	2700	v1		
14	85.233.207.251	85.233.207.251	SAP	Orion - SAP	2800	v1		
15	163.156.213.29	163.156.213.29*	AXA	Orion - AXA	2900	v1	Jaroslav.Jaskola@axa.pl (PL) john.hyszczuk@axa.com (UK)	
15.5	163.156.213.6		AXA (new)	Orion - AXA	2950	v2	Jaroslav.Jaskola@axa.pl (PL) john.hyszczuk@axa.com (UK)	
16	194.154.227.146	194.154.227.146	T-MOBILE [SK]	Orion - T-Mobile SK	3000	v1		
17	193.111.37.166	193.111.37.166	VIRGIN MOBILE 1	Orion - Virgin Mobile 1	3400	v1		
18	83.238.11.122	83.238.11.122	VIRGIN MOBILE 2	Orion - VirginMobile 2	3450	v1		
19	85.158.168.112	85.158.168.112	DV Spain	Orion - DV Spain	3900	v1		
20	93.158.77.116	93.158.77.116	CLX1	Orion - CLX 1	4000	v1		
21	213.248.76.228	213.248.76.228	CLX2	Orion - CLX 2	4100	v1		
22	89.108.194.198	89.108.194.198	Play #1	Orion - Play 1	4200	v1		
23	193.105.74.4	193.105.74.4	Infobip	Orion - Infobip	4300	v1		

- Partnerzy którzy nie mają zestawionych dwóch ipsec (brak HA, wymagane zgłoszenie w przypadku nie działania)

Monitoring rozszerzony

- W Orionie dodany jest check/zapytanie które wyciąga z monitoringu P1 czy tunele są zestawione (na obu RTR'ach):
 - <http://orion.avantis.pl/Orion/APM/ApplicationDetails.aspx?NetObject=AA:347>

```
SELECT COALESCE((SELECT TOP 1( ROW_NUMBER() OVER(ORDER BY P1_PEER ASC))
FROM [SolarWindsOrion].[dbo].[NETCTL_IPSEC_HISTORY]
where TUN_STATUS = 'NOTACTIVE' and CHECK_TIME > DATEADD(mi,-5,GETDATE())
group by CHECK_TIME, TUN_STATUS, P1_PEER, LOCATION_ID
order by P1_PEER DESC) ,0) AS statistic , (SELECT STUFF((SELECT P1_PEER
+', '
FROM [SolarWindsOrion].[dbo].[NETCTL_IPSEC_HISTORY]
where TUN_STATUS = 'NOTACTIVE' and CHECK_TIME > DATEADD(mi,-5,GETDATE())
group by CHECK_TIME,TUN_STATUS,P1_PEER, LOCATION_ID
FOR XML PATH('') ,1,1, '')) as information
```

Wybudzanie

- Monitor - check tcp na Netscalerze A oraz B, powoduje podniesienie fazy drugiej i jej utrzymywanie przez generowanie sztucznego ruchu.