Túl a határvédelmen,

avagy a kifordított UTM

Tekler Krisztián

Vezető rendszermérnök

SOPHOS Certified Architect

newco TRADING ICT security services

SOPHOS Security made simple.

Határvédelemmel kapcsolatos elvárások változása

Kliensek védelme, szeparálása

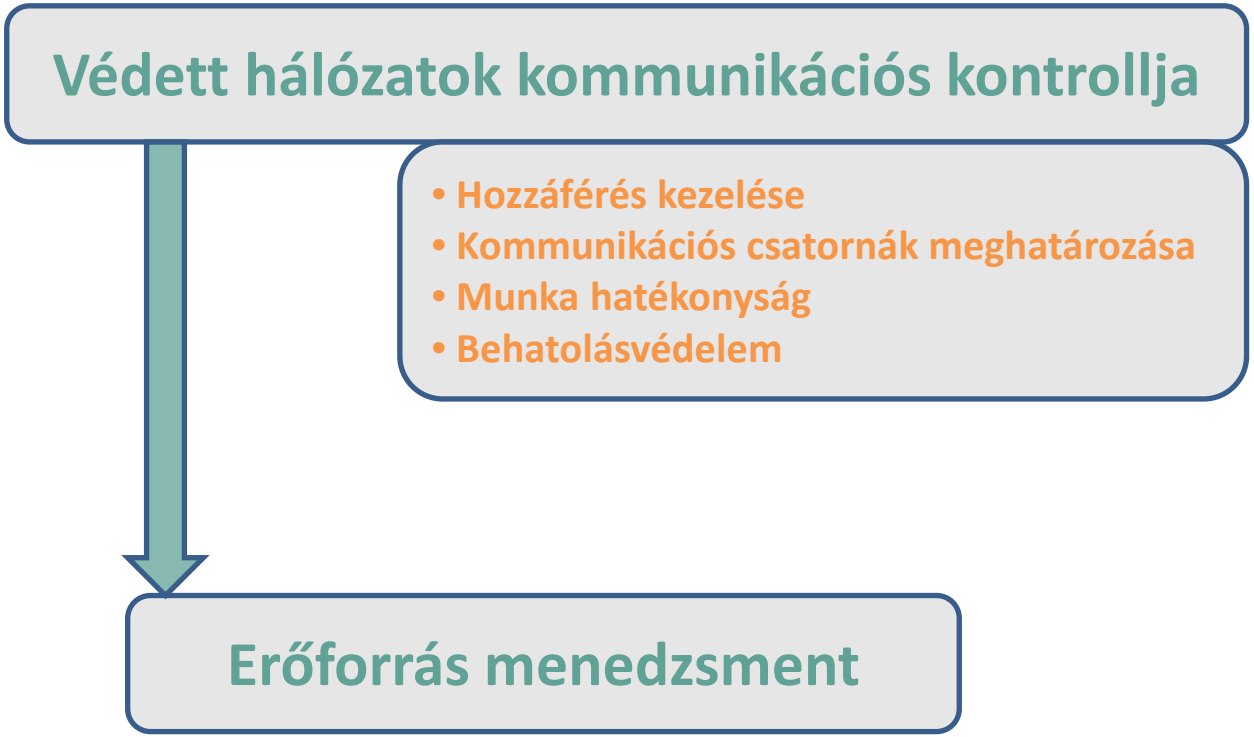
- Saját hálózatom
- Hálózatomon kívüli kérések kezelése

Védett hálózatok felosztása

- Logikai szétválasztás
- Fizikai szétválasztás (szerverszobák)
- Hozzáférés kontroll – hálózati

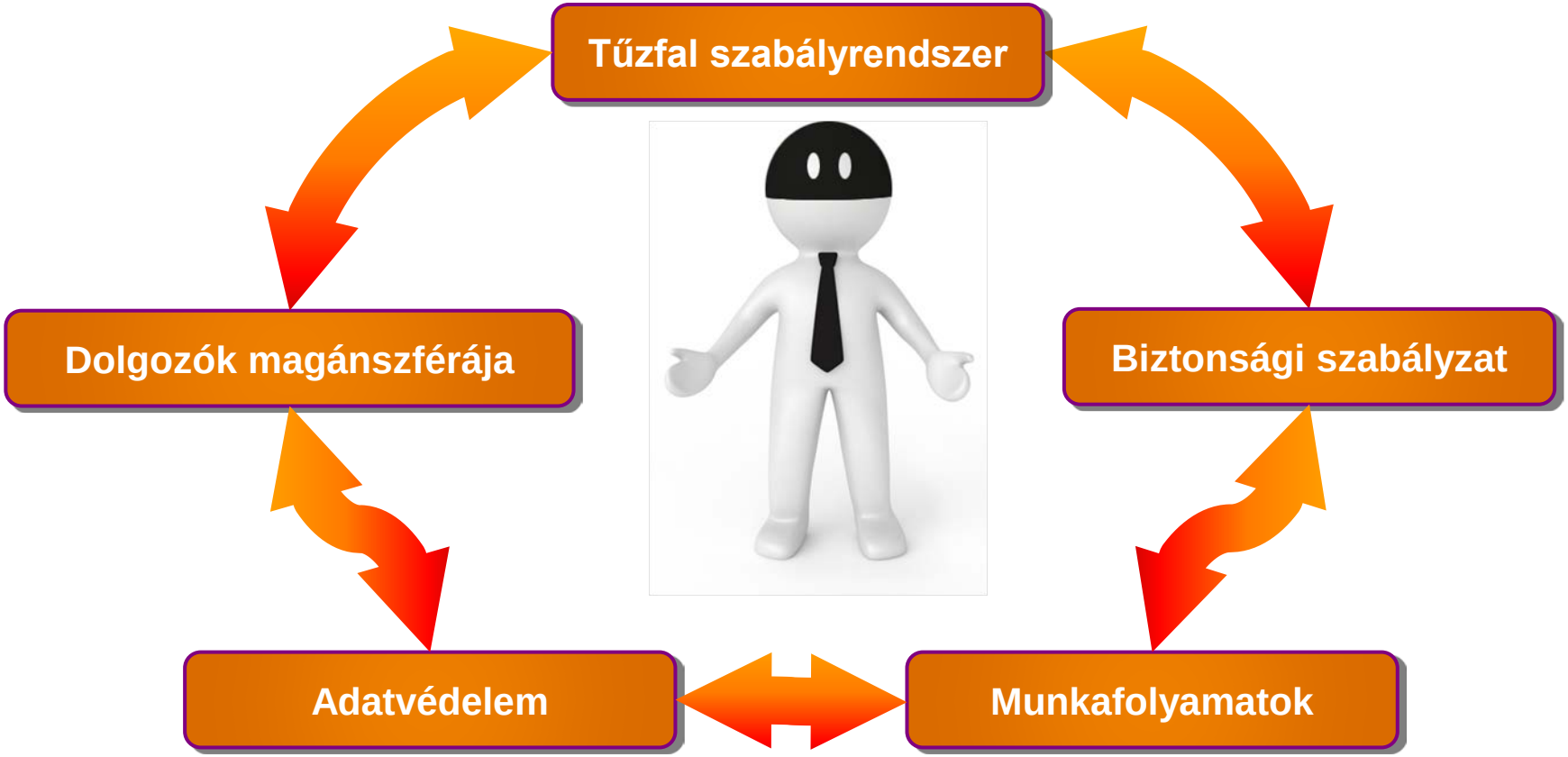
Védett hálózatok kommunikációs kontrollja

Határvédelemmel kapcsolatos elvárások változása

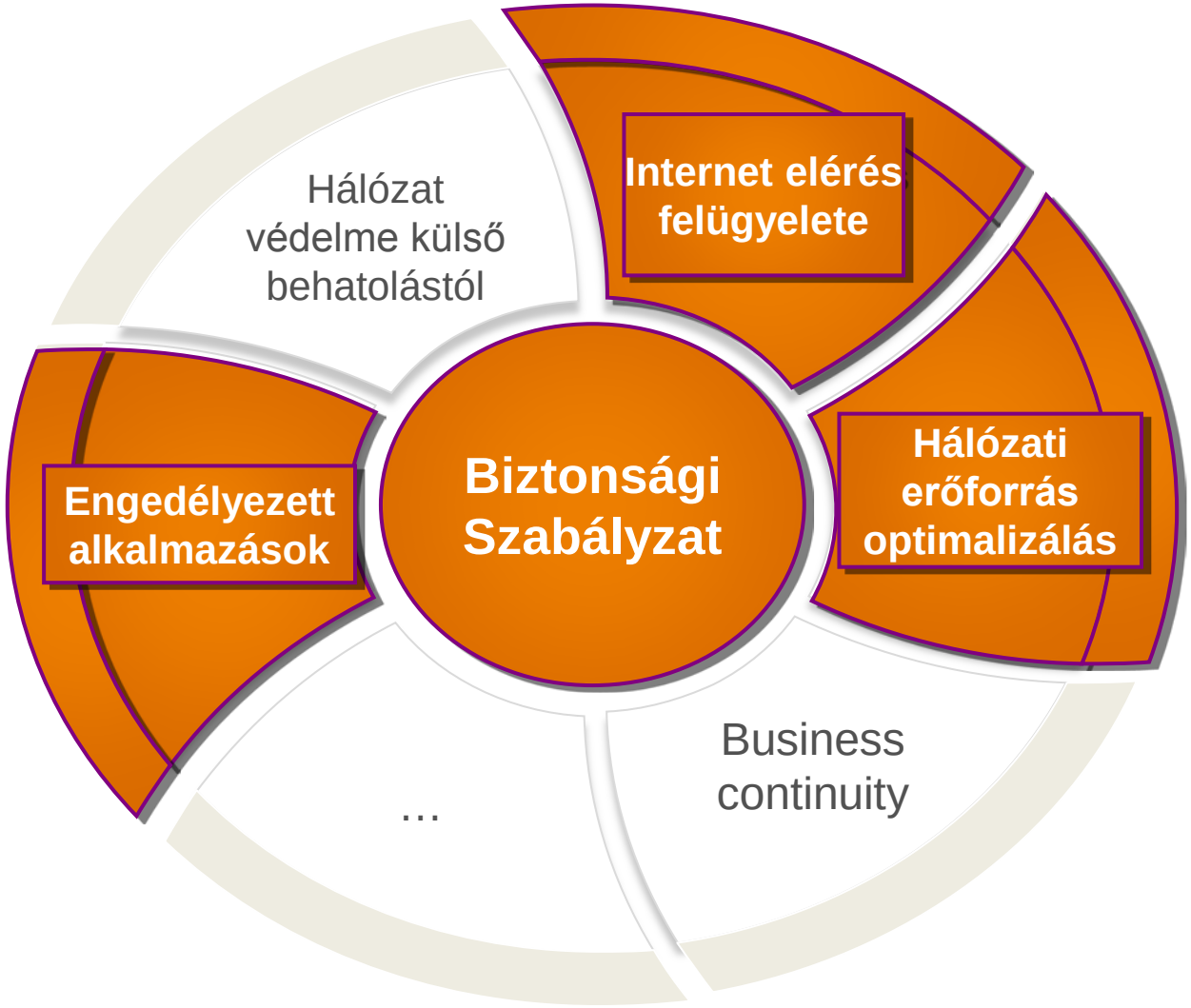


Biztonsági szabályzat

Tyúk vagy a tojás ?



SOPHOS UTM válaszok



Ismerjük meg a hálózatunkat

- **Webes Alkalmazások**

Web Protection

Web Usage Re... | Search Engine ... | Departments | Scheduled Rep... | **Application Con...** | Deanonymization

Top Applications | Today | number of rows | « » | Update

Results: 1-20 of 37

Top	Application	Application Category	Packets	%	Dest. Hosts	%	Src. Hosts	%
1	HTTP	Web Services	5 190	65.48	211	48.84	13	20.97
2	Sophos EP Update	Networking	1 333	16.82	38	8.80	2	3.23
3	Facebook	Social Networking	275	3.47	21	4.86	2	3.23
4	Kaspersky	File Transfer	200	2.52	13	3.01	1	1.61
5	Doubleclick	Web Services	140	1.77	7	1.62	1	1.61
6	Google Video	Streaming Media	136	1.72	7	1.62	1	1.61
7	YouTube	Streaming Media	114	1.44	13	3.01	1	1.61
8	Google	Web Services	107	1.35	22	5.09	3	4.84
9	Google Analytics	Web Services	102	1.29	10	2.31	3	4.84
10	Bet365	Games	56	0.71	2	0.46	1	1.61
11	BITS	File Transfer	42	0.53	2	0.46	2	3.23

Ismerjük meg a hálózatunkat

- **Webes Alkalmazások**

Web Protection

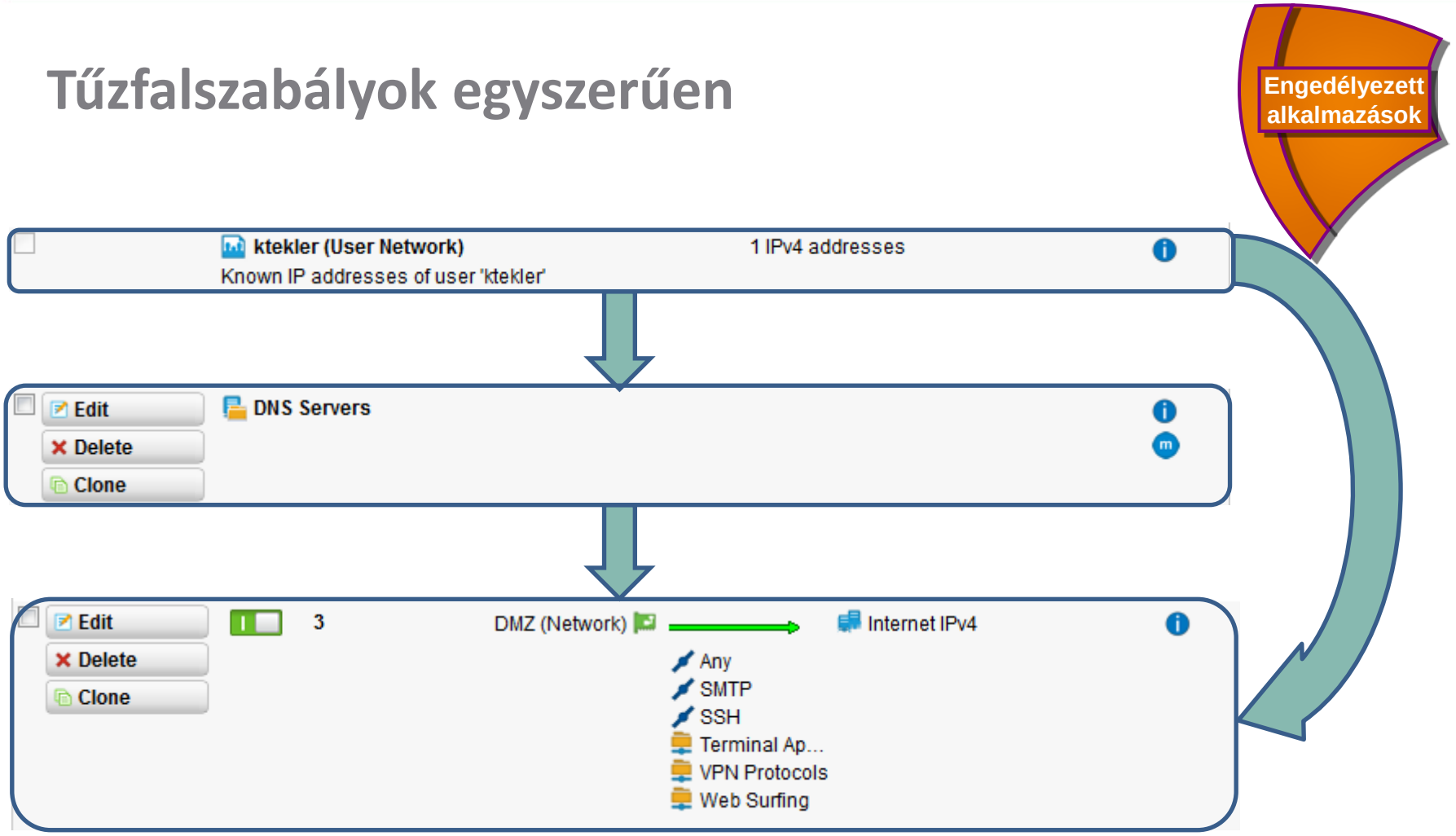
Web Usage Re... | Search Engine ... | Departments | Scheduled Rep... | Application Con... | Deanonymization

New custom Report — Available Reports: Categories

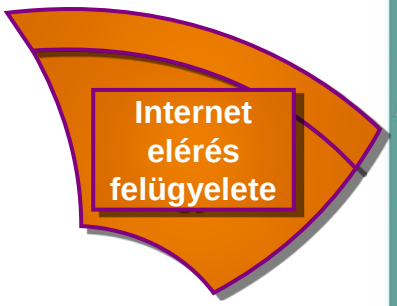
All | Today | All Departments

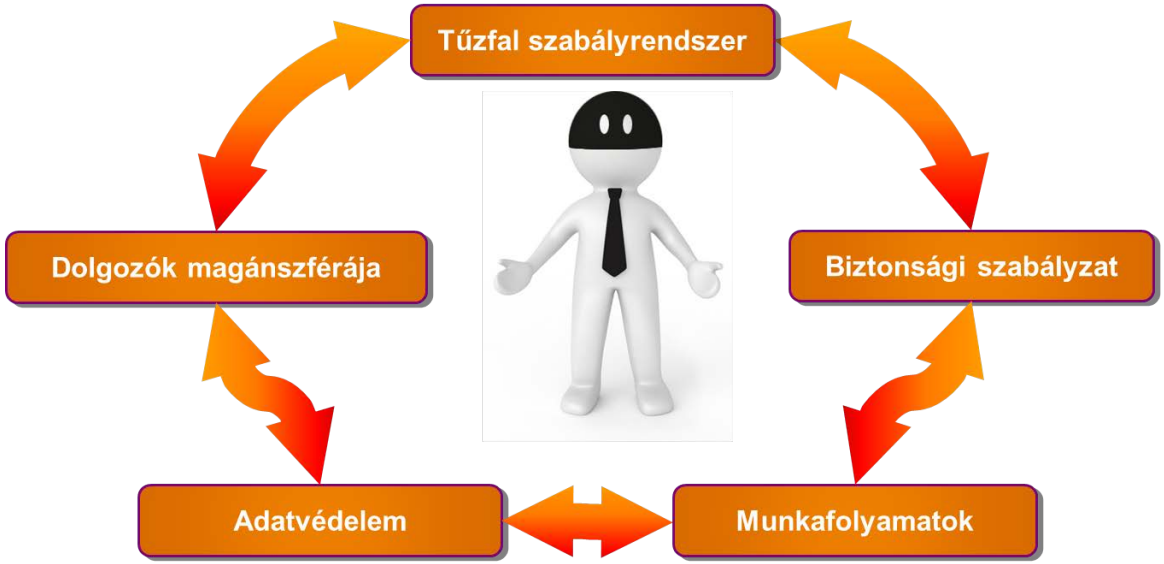
#	Category	Traffic	%	Pages	Requests
1	Content Server	105 MB	32.14	0	278
2	Software/Hardware	96 MB	29.42	12	2154
3	Media Sharing	47 MB	14.39	29	646
4	Categorization Failed	27 MB	8.12	52	1060
5	Web Ads	9 MB	2.73	118	592
6	Internet Services	9 MB	2.62	46	863
7	Entertainment	9 MB	2.61	10	108
8	Public Information	5 MB	1.55	9	49
9	Fashion/Beauty	4 MB	1.08	18	442
10	Online Shopping	3 MB	1.04	35	363
11	Social Networking	2 MB	0.73	157	442
12	Blogs/Wiki	1 MB	0.44	6	72
13	Finance/Banking	1 MB	0.41	2	69
14	Travel	1 MB	0.38	0	9
15	Shareware/Freeware	1 MB	0.38	0	58

Tűzfalszabályok egyszerűen



Internet elérés felügyelete

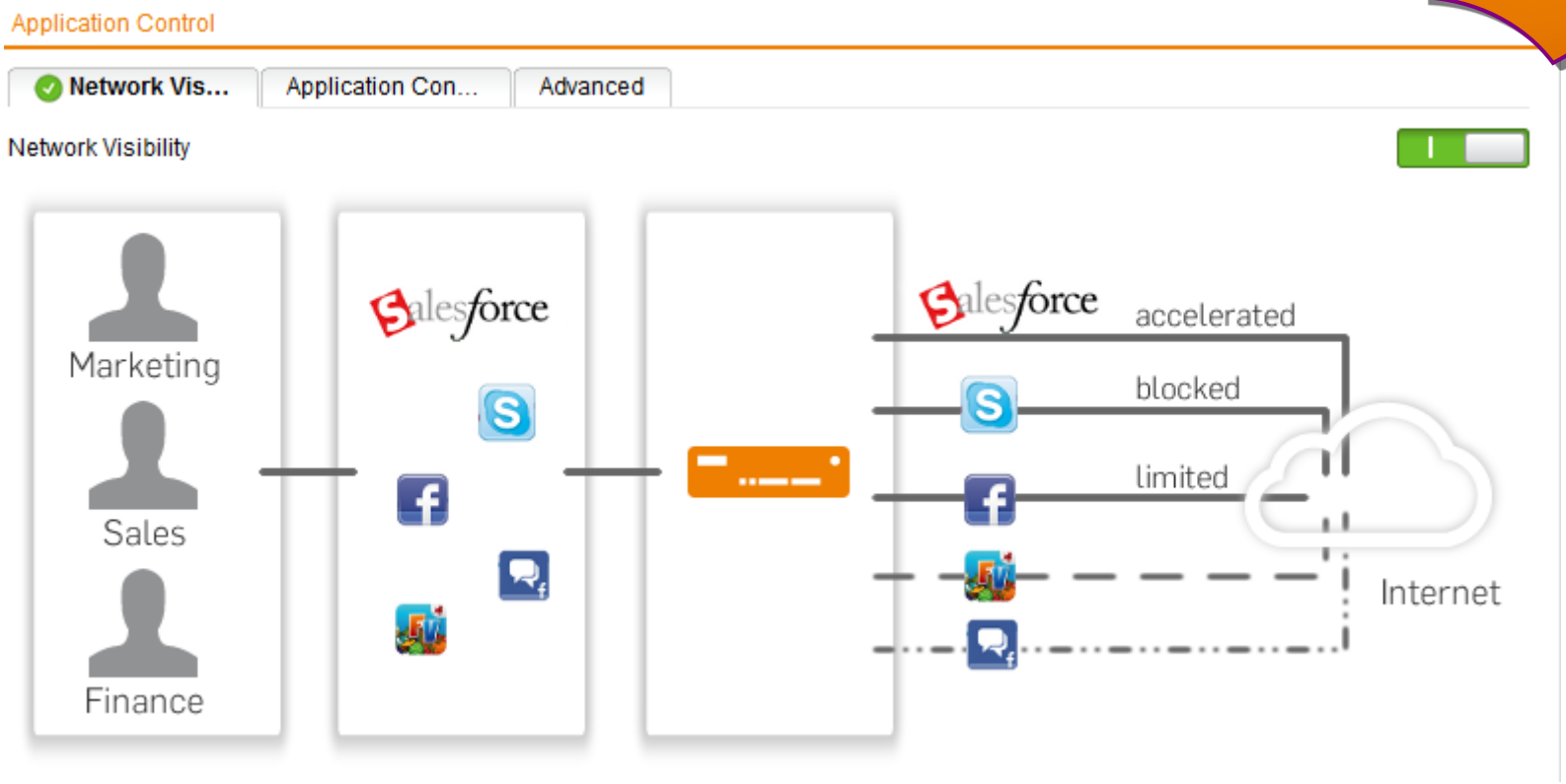




- Szükséges szeparálni ? (felhasználó, munkaállomás)
- Időkorlátozás ?
- Azonosítás ?

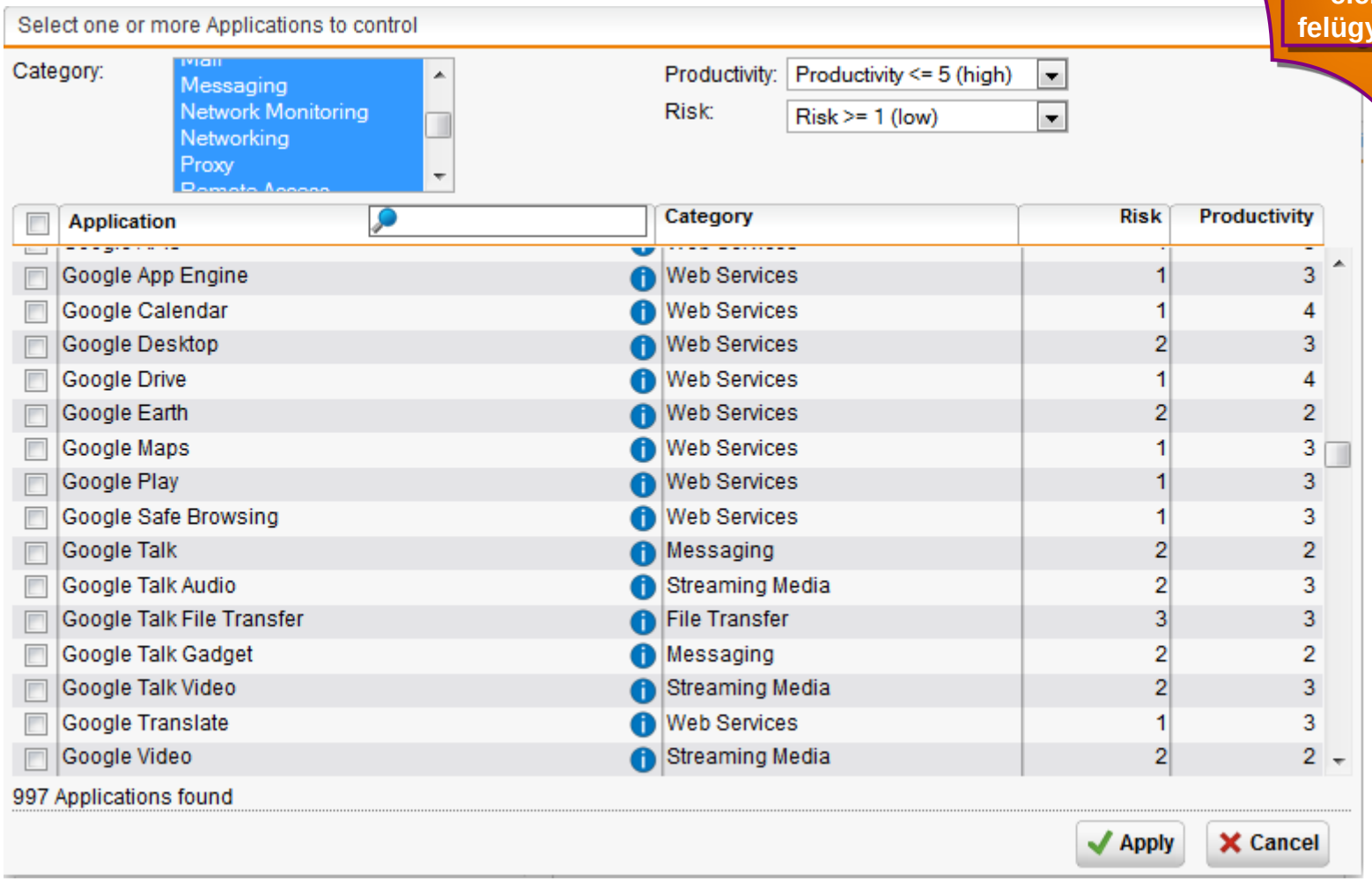
Application Control

Internet elérés felügyelete



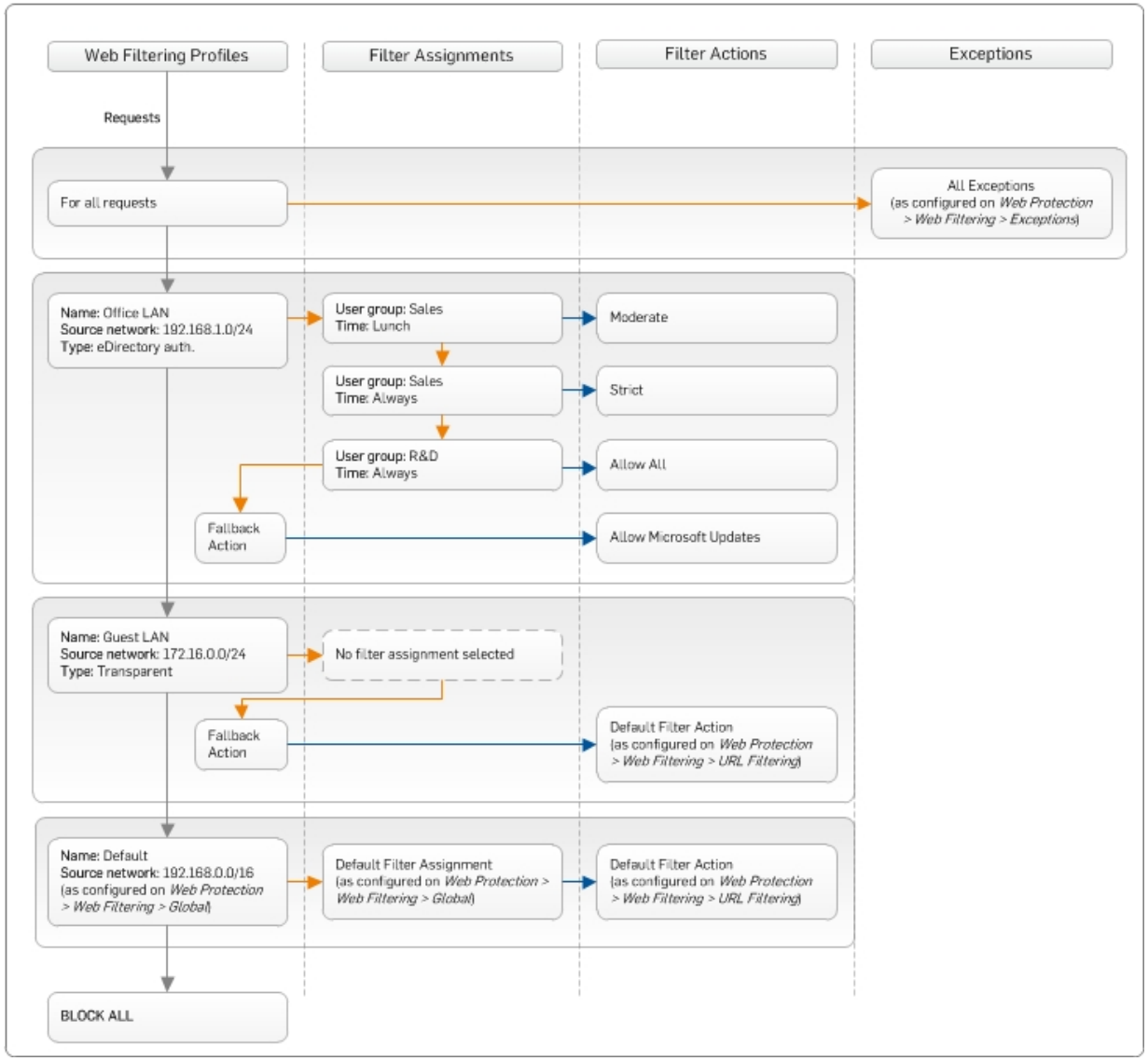
Application Control

Internet elérés felügyelete

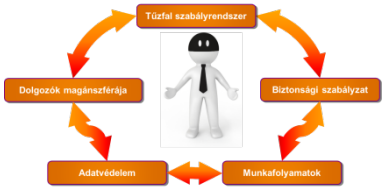


Proxy profiles

Internet elérés felügyelete



Anonimizálás



Internet elérés felügyelete

Reporting Settings

Settings | Exceptions | Anonymizing

Anonymizing status

Anonymizing Settings

First password:
Repeat:
Second password:
Repeat:

When enabling anonymized reporting, two passwords have to be provided. Both passwords are required for disabling anonymization or deanonymization of single users (four eyes principle).

Apply

Hálózati forgalom optimalizálás

Hálózati erőforrás optimalizálás

- MultiPath szabályok

Action	Status	Position	Name	Persist...	Source	Service	Destina...
Edit / Delete / Clone		1	Example HTTP [by Source/Destination]	[persistence by combination of SRC and DST IP address]			
			Any → Web Surfing → Any → Uplink Interfaces				
Edit / Delete / Clone		2	Example SMTP [by Destination]	[persistence by DST IP address]			
			Any → SMTP → Any → Uplink Interfaces				
Edit / Delete / Clone		3	Example DNS [by Connection]	[balance DNS request individually]			
			Any → DNS → Any → Uplink Interfaces				

Köszönöm a figyelmet!

ktekler@newcotrading.hu