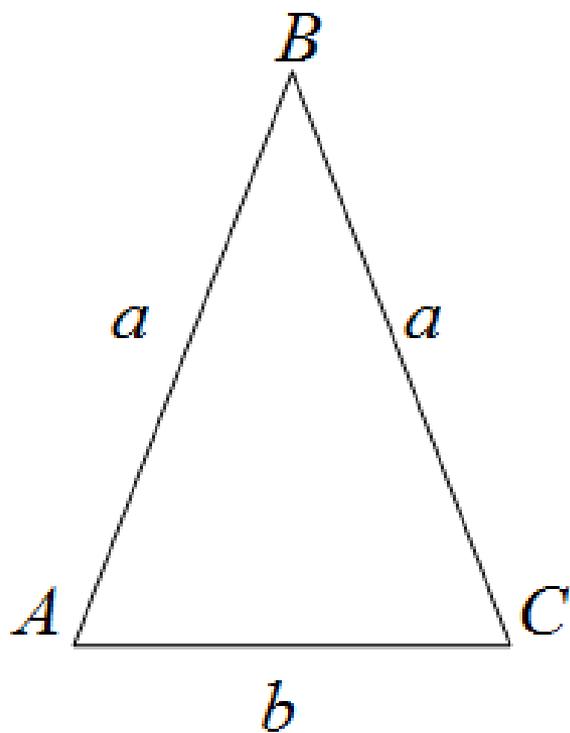




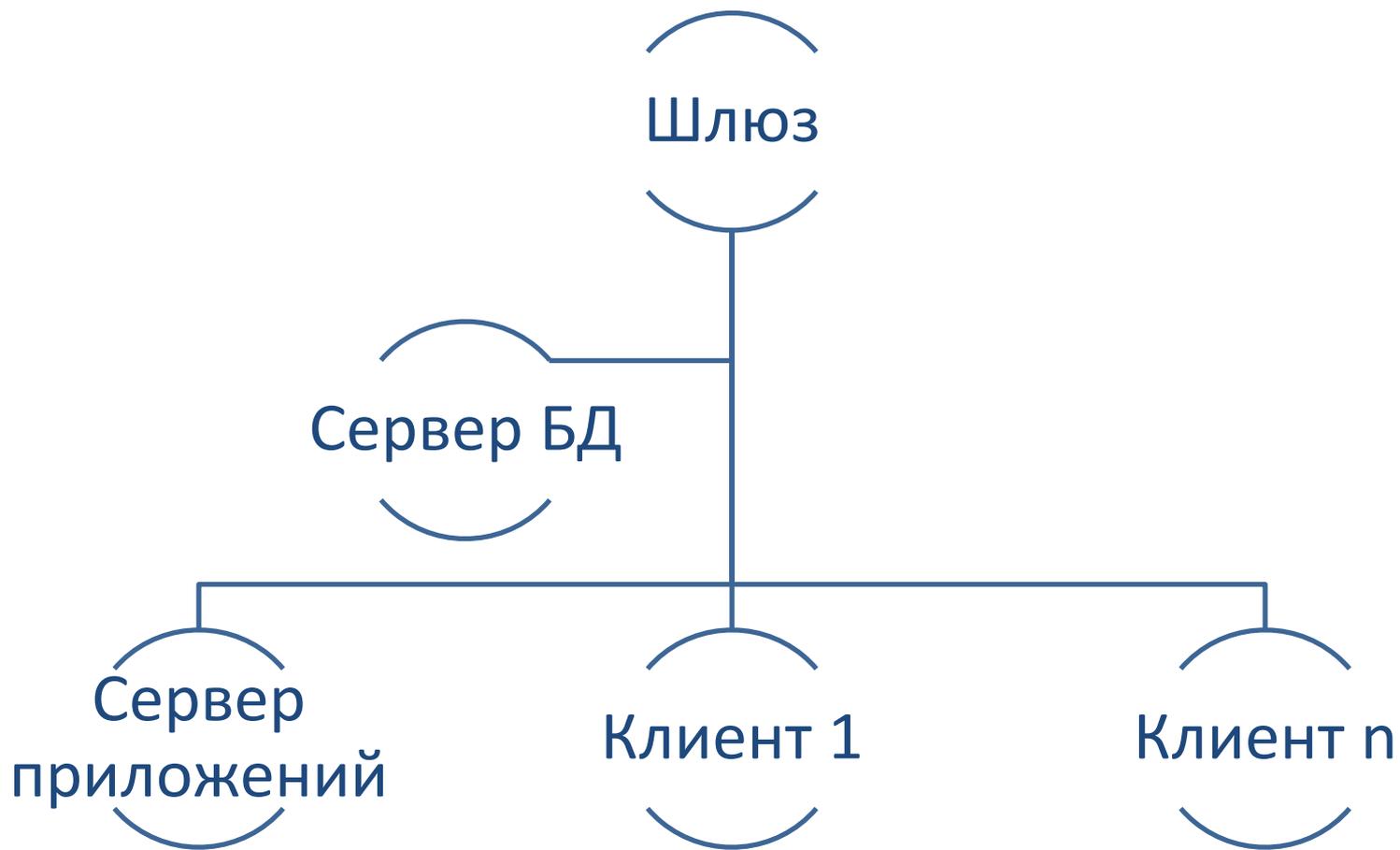
Защищённый периметр. Он есть или его нет?

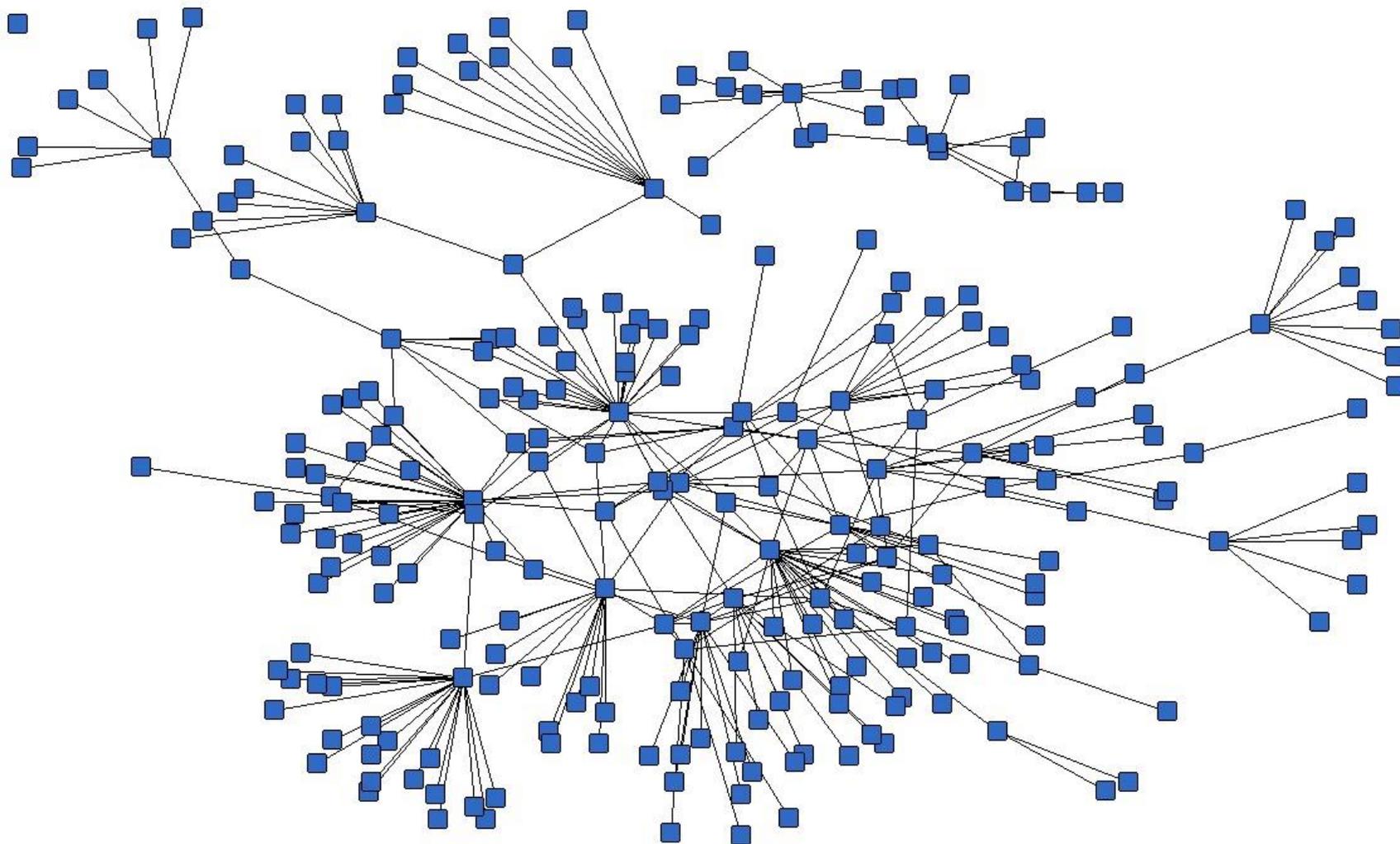
Юрий Мухортов
Директор Департамента специальных проектов
АО «ЭЛВИС-ПЛЮС»



$$P_{\Delta ABC} = 2a + b$$

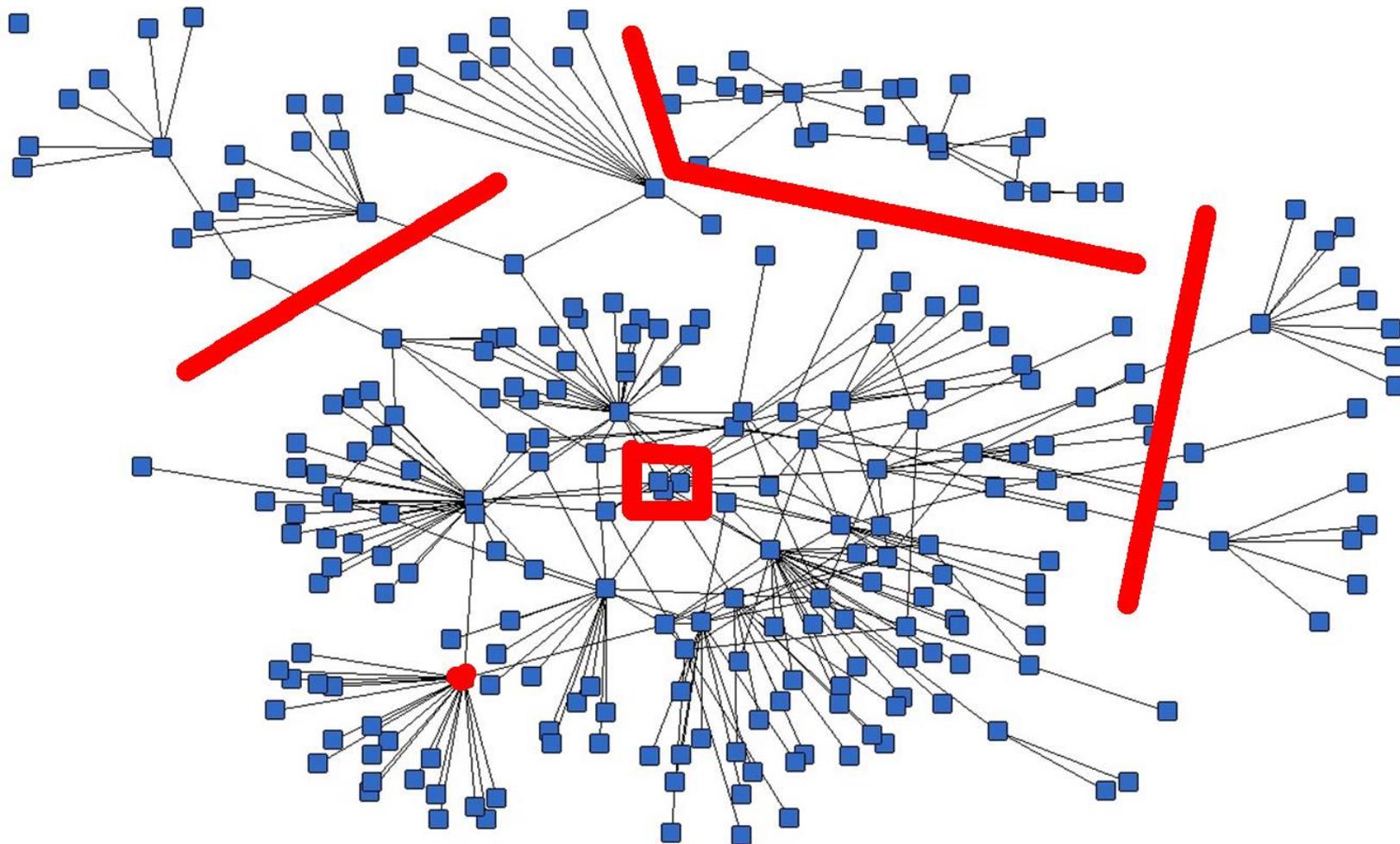
Рис.1

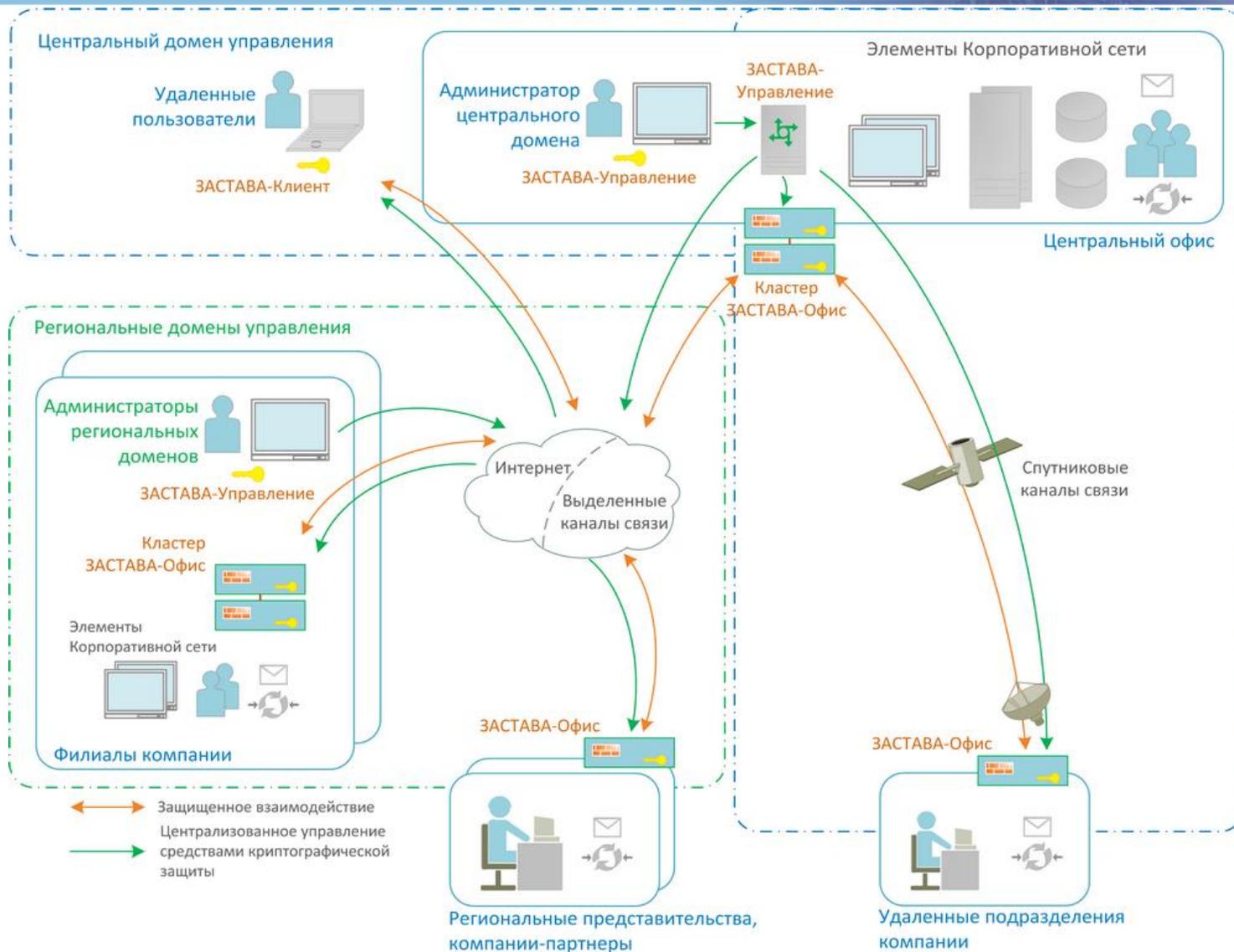






Промежуточные периметры





99 %

- Доступ для устаревших ИС
- В бухгалтерии ничего не работает!!!
- Аварийный канал связи
- Начальник сказал
- Админ проковырял себе лазейку
- Технологические доступы
- Спешка





Не должно быть
бесконтрольного доступа.
Что не разрешено — запрещено!

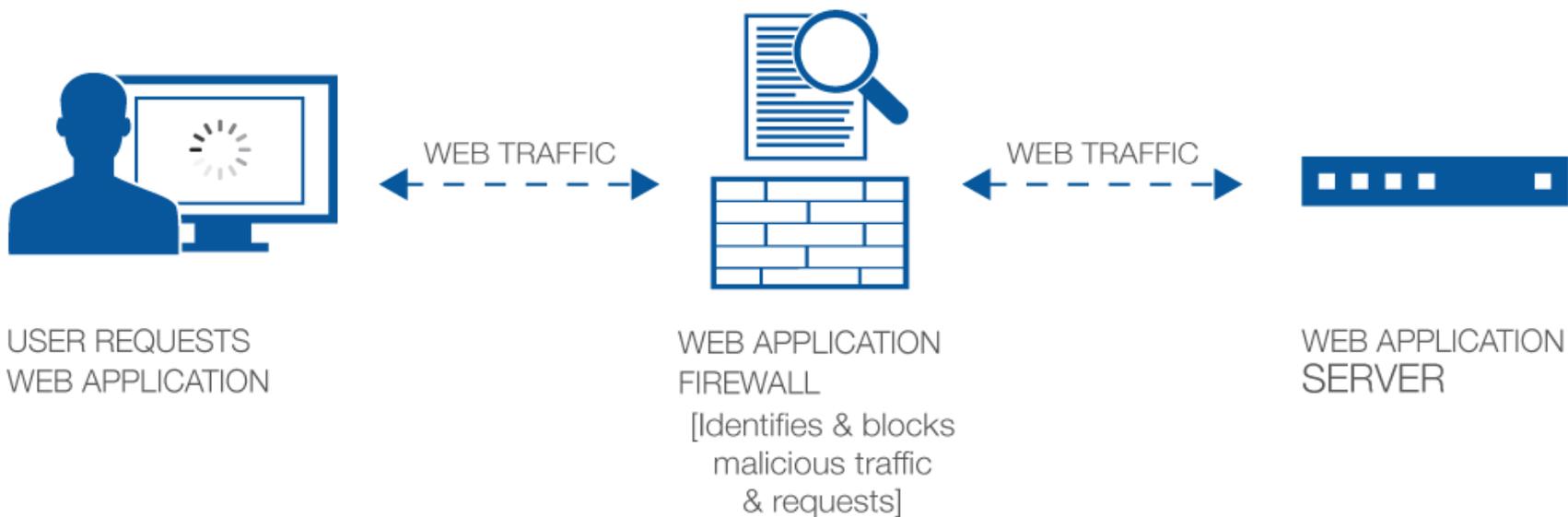
Традиционные межсетевые экраны обычно предлагают либо удобство, либо безопасность.

NGFW решают эту проблему.



Palo Alto NG FW, Cisco ASA-X, HP TippingPoint NGFW, McAfee NGFW, CheckPoint, Fortinet FortiGate

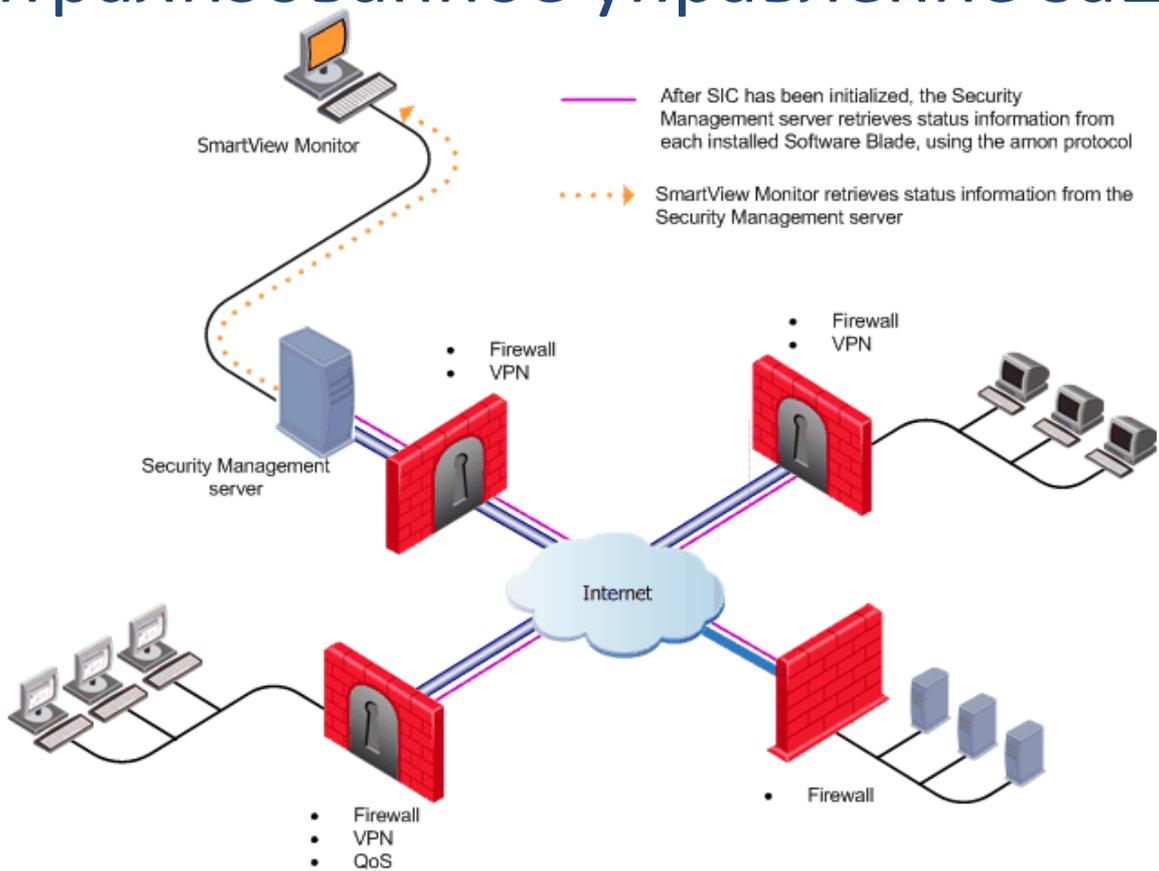
WEB APPLICATION FIREWALL



Positive Technologies Application Firewall, Imperva Web Application Firewall , F5



Централизованное управление защитой



Cisco Security Manager, Palo Alto Panorama, CheckPoint Security Management Server



Palo Alto NG FW, Cisco FirePower, IBM XGS, HP TippingPoint, McAfee Network Security Platform

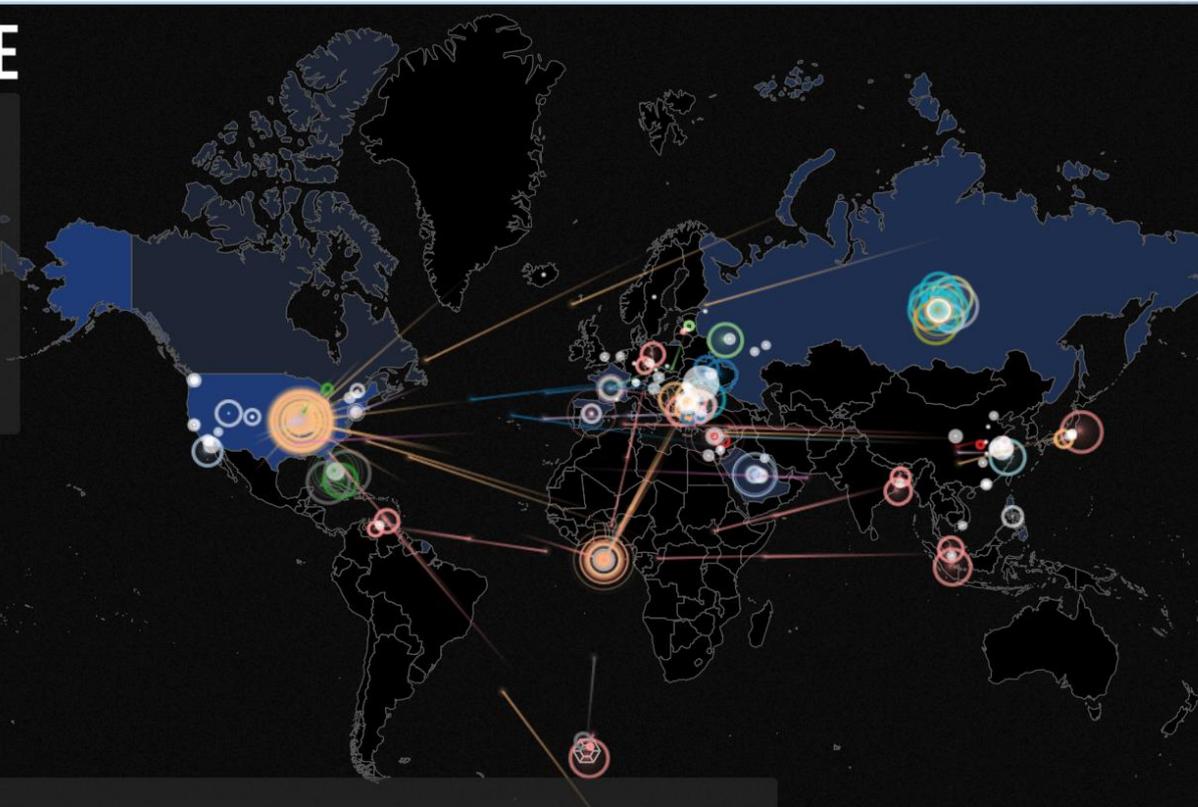


Чудес не бывает — 0-day уязвимость по-прежнему актуальны



ATTACK ORIGINS

#	COUNTRY
239	Moldova
65	China
43	United States
34	Russia
34	Bulgaria
23	Mil/Gov
6	Japan
5	Hong Kong
4	Saudi Arabia
4	Cyprus



ATTACK TARGETS

#	COUNTRY
329	United States
91	Mil/Gov
24	Russia
17	France
14	Philippines
8	Saudi Arabia
8	Spain
6	Cyprus
5	Bulgaria
4	Canada

LIVE ATTACKS

TIMESTAMP	ATTACKER ORGANIZATION	LOCATION	IP	TARGET LOCATION	TYPE SERVICE	PORT
2015-06-18 13:01:14.73	Easy Fondi SIA	unknown, Latvia	95.215.47.13	unknown, Mil/Gov	rfb	5900
2015-06-18 13:01:15.18	China Unicom Henan	Luohe, China	123.8.228.206	unknown, Mil/Gov	unknown	790
2015-06-18 13:01:15.35	N/A	unknown, Mil/Gov	162.244.35.24	unknown, Russia	unknown	21320
2015-06-18 13:01:15.84	TOKAI Corporation	Numazu, Japan	116.254.66.105	unknown, Mil/Gov	unknown	62538
2015-06-18 13:01:16.11	ISP Fregat Ltd.	unknown/Ukraine	46.98.219.40	Saint Louis, Unifred	unknown	21950
2015-06-18 13:01:16.53	SIA Lattelcom	Riga, Latvia	81.198.220.93	unknown, Mil/Gov	microsoft-ds	445
2015-06-18 13:01:16.72	Info Data Center Ltd.	unknown, Bulgaria	195.88.74.199	unknown, Mil/Gov	csd-mgmt-port	3071
2015-06-18 13:01:16.72	Info Data Center Ltd.	unknown, Bulgaria	195.88.74.200	unknown, Mil/Gov	csd-mgmt-port	3071

ATTACK TYPES

#	SERVICE	PORT
239	ssh	22
52	microsoft-ds	445
28	csd-mgmt-port	3071
20	http	80
11	telnet	23
11	mysql	3306
11	http-alt	8080
10	domain	53

digitalattackmap.com

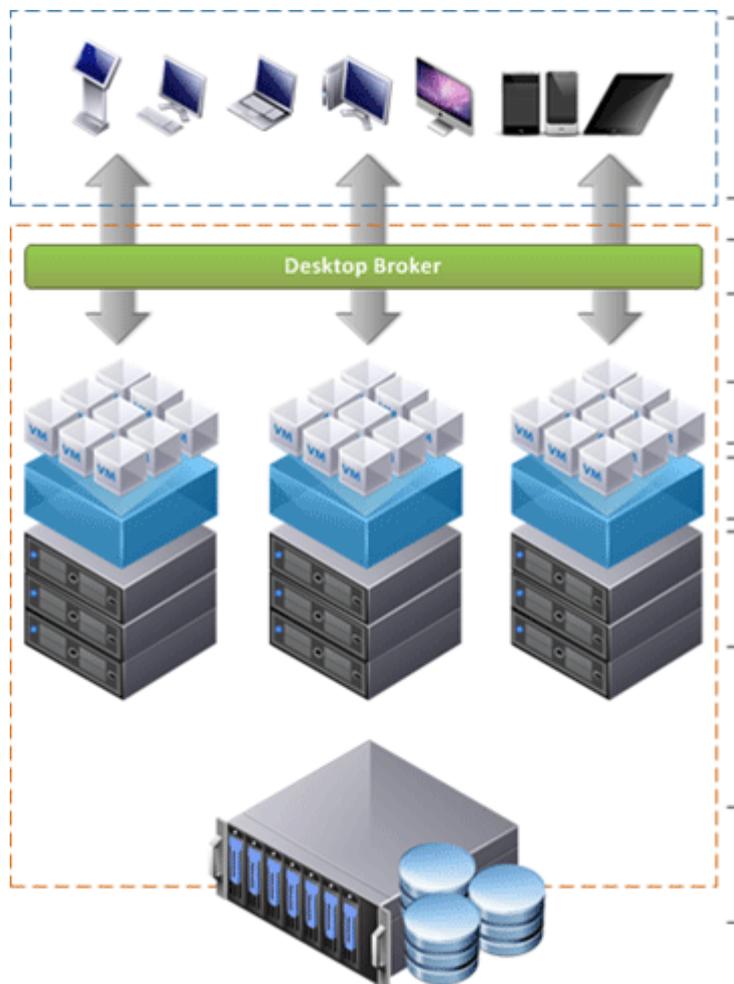
map.ipviking.com

Arbor Networks,

Qrator Labs,

Kaspersky DDoS Prevention





Клиенты (ПК, ноутбуки, тонкие клиенты, мобильные устройства)

Брокер клиентских подключений

Виртуальные машины

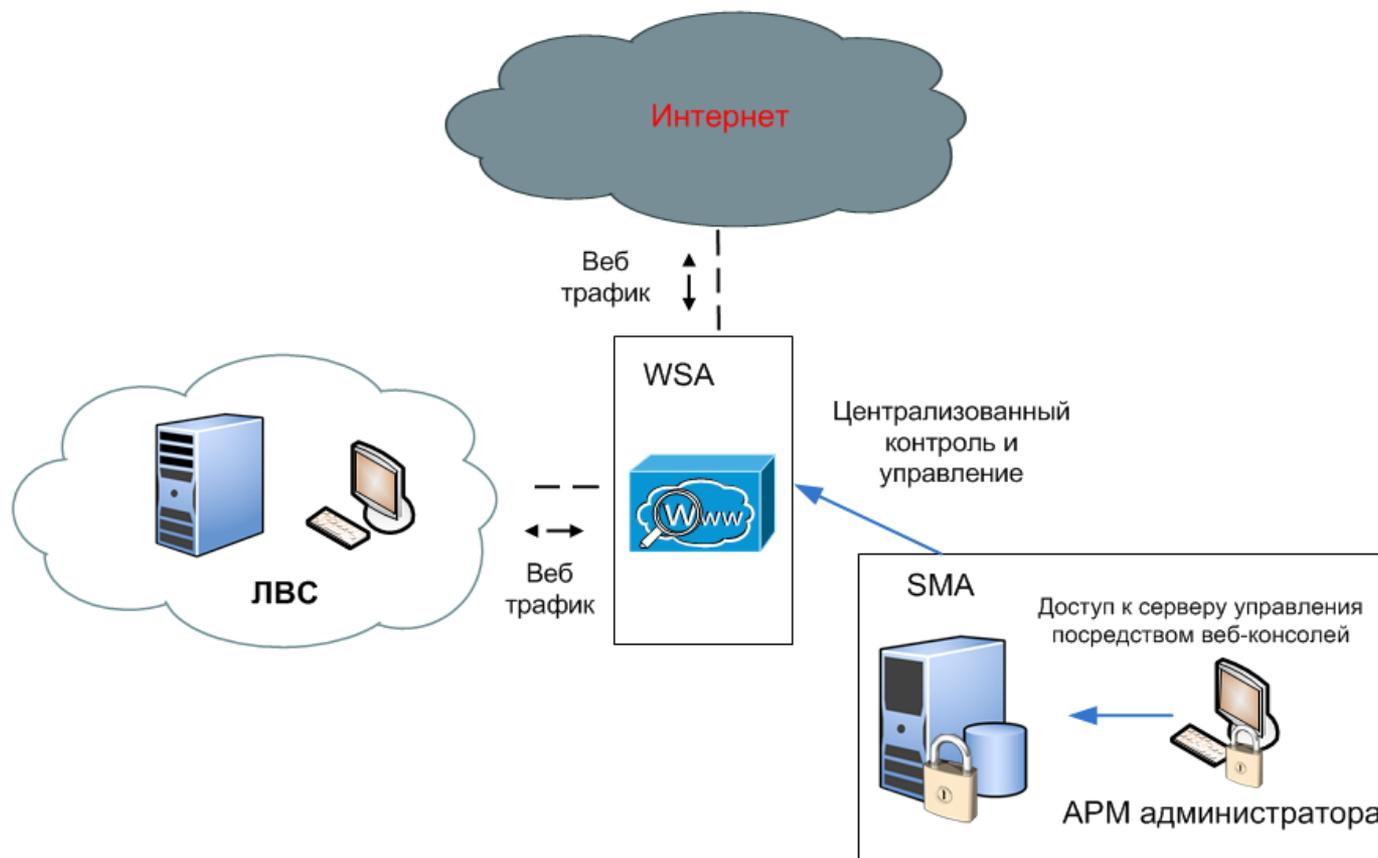
Гипервизор

Физические сервера

Система хранения данных

VMware VDI,

Citrix XenDesktop



McAfee Web Gateway + McAfee Email Gateway, Cisco Web Security Appliance + Cisco Email Security Appliance, Blue Coat Secure Web Gateway, устройства из NG FW



Контроль устройств



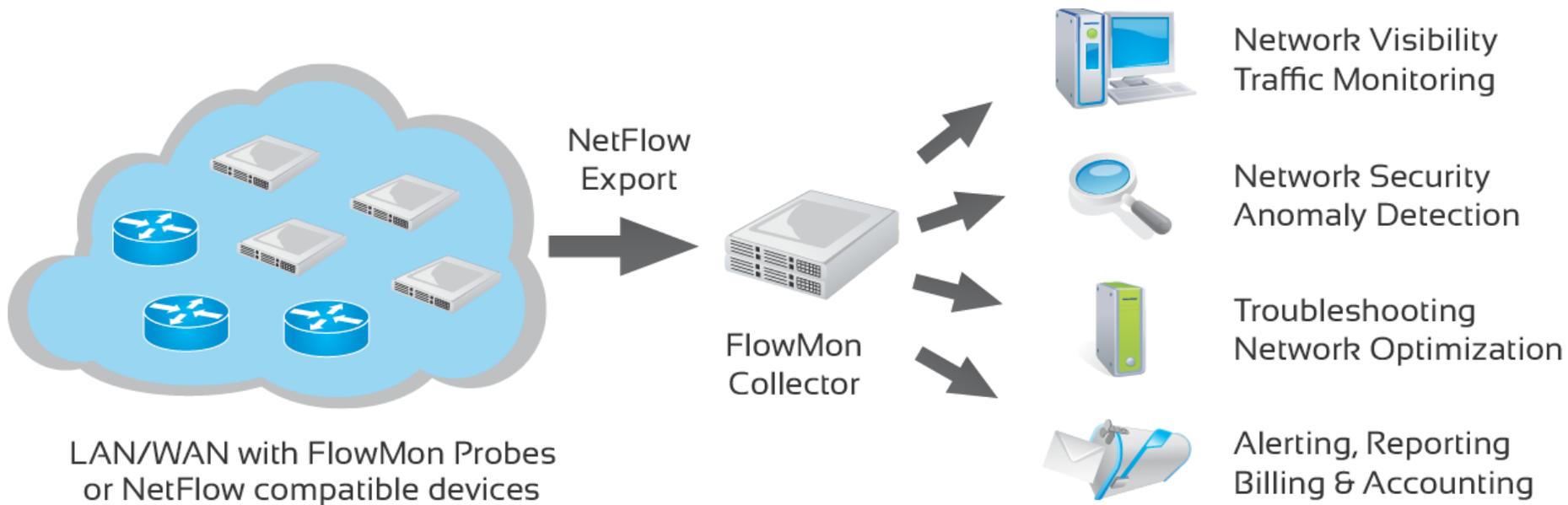
Cisco ISE, ForeScout CounterACT



Sandboxing — не игрушка!



**Palo Alto WildFire, McAfee ATD, Trend Micro Deep Discovery, FireEye,
Cisco Advanced Malware Protection**



NetFlow, Lancope StealthWatch



Абсолютной защиты не существует.

Но надо стремиться её создать.



Ваши вопросы?