Защищённый периметр.
Он есть или его нет?

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

ЭЛВИС-ПЛЮС

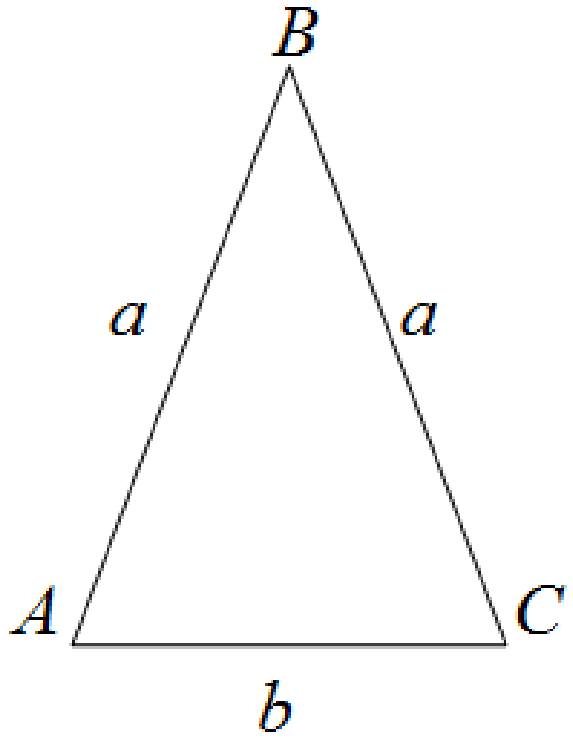
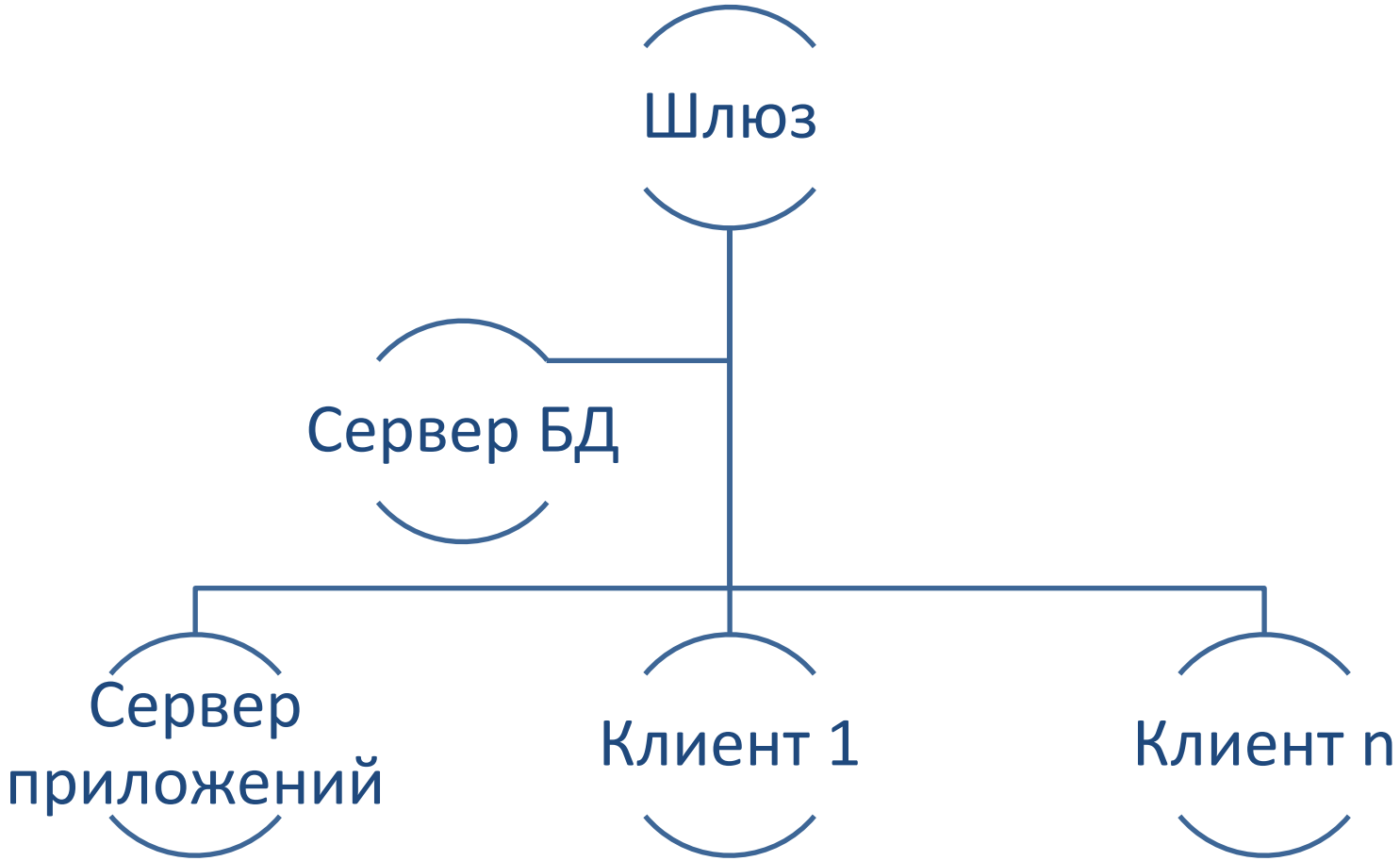
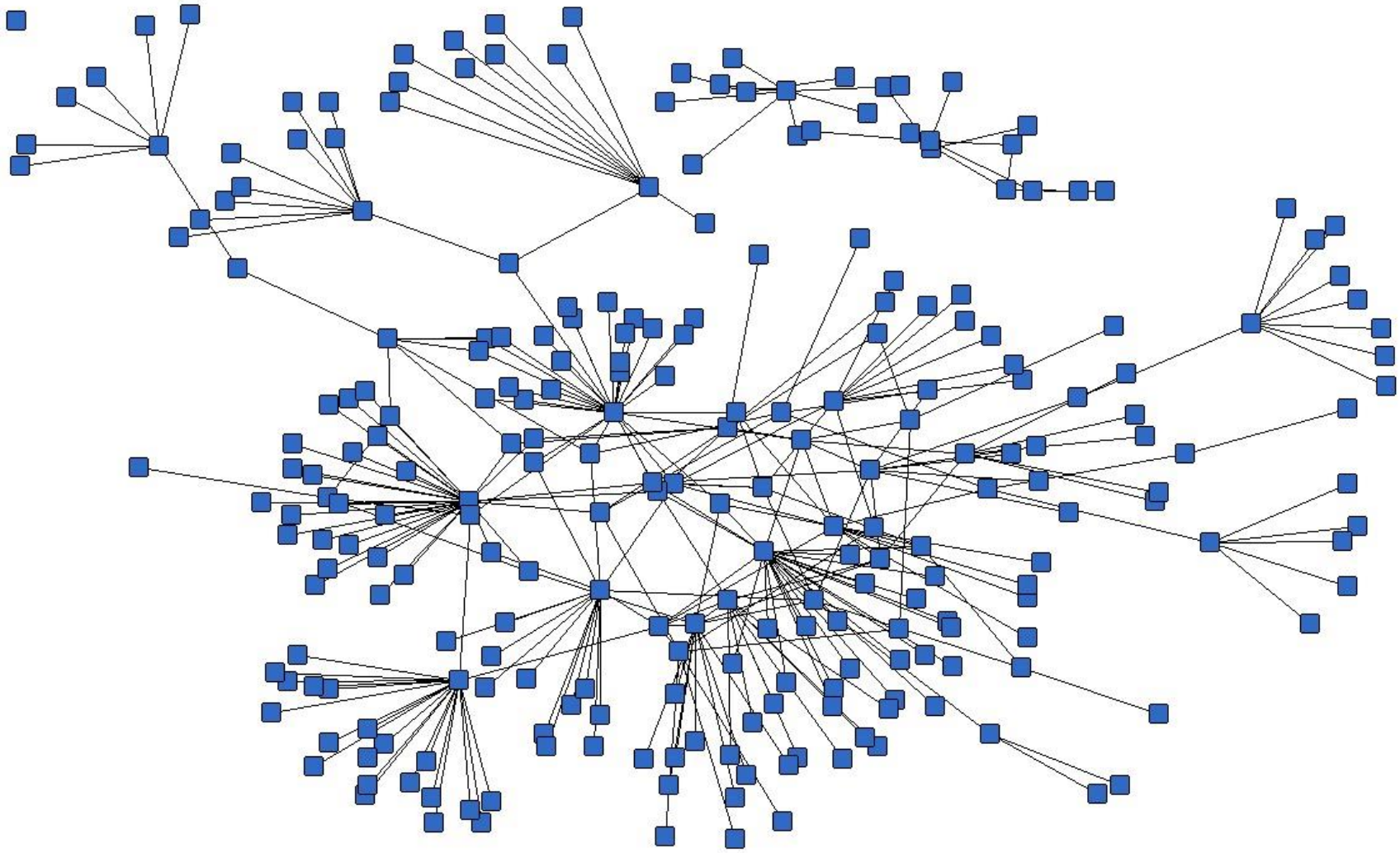


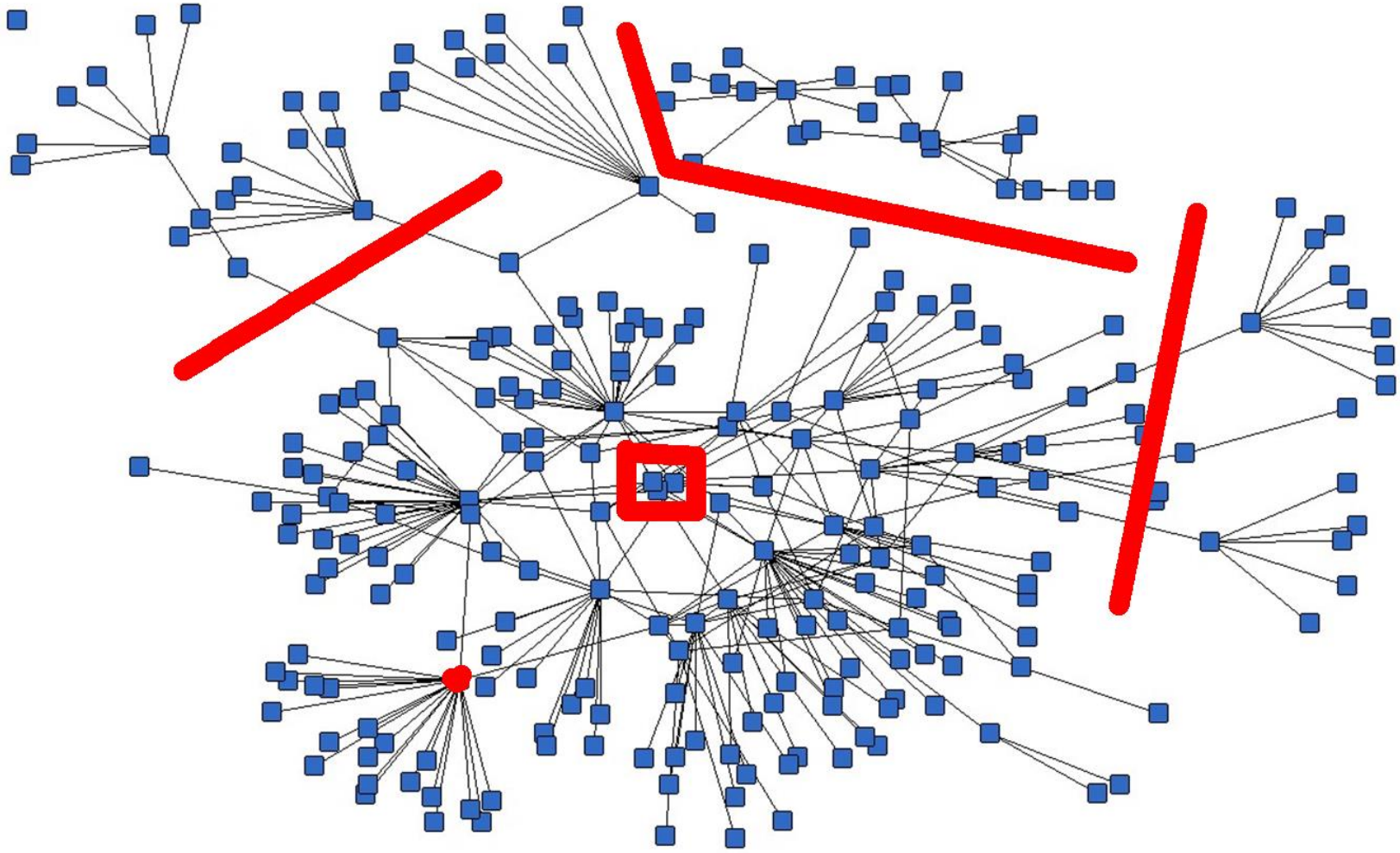
Рис.1

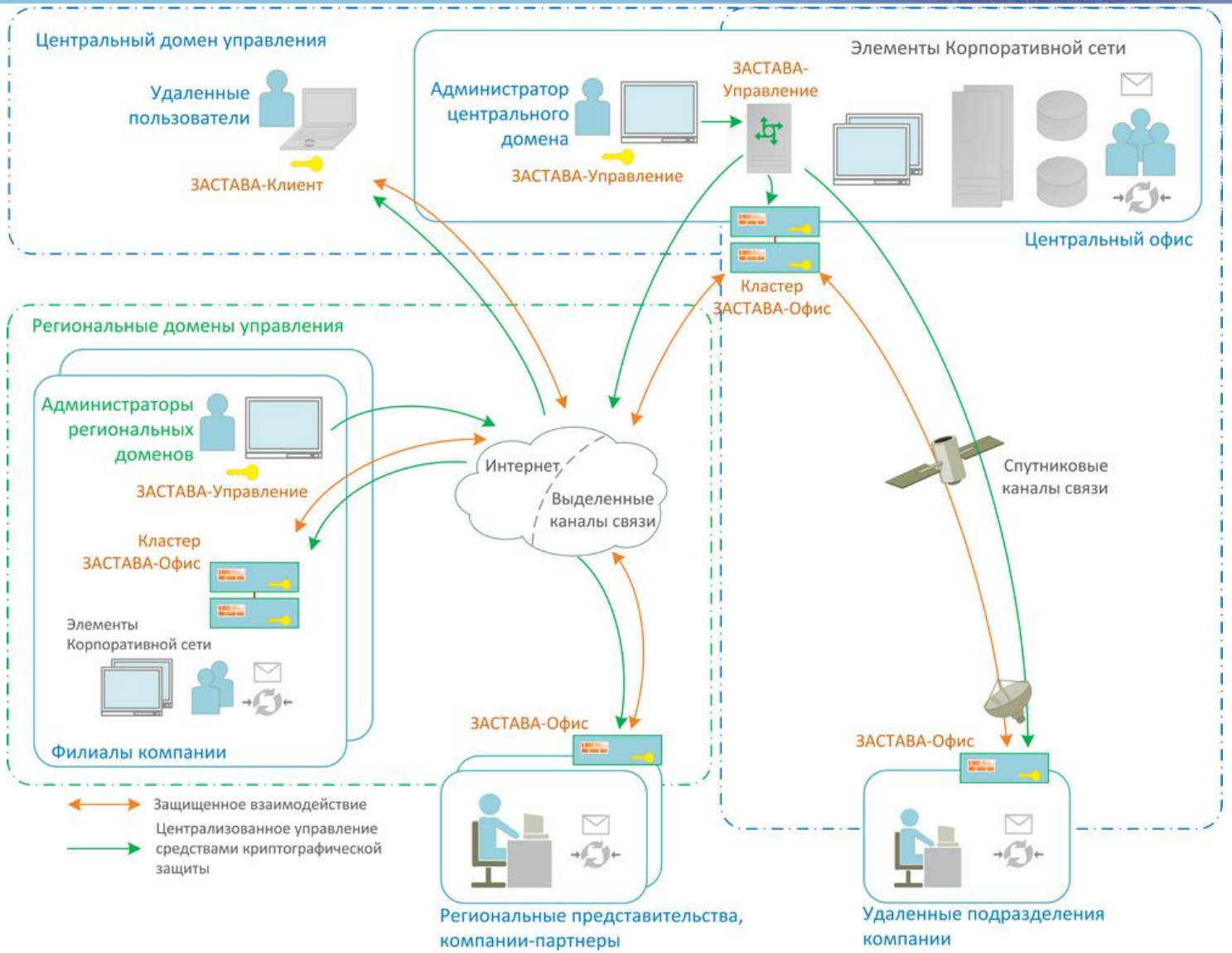
$$P_{\Delta ABC} = 2a + b$$





Промежуточные периметры





99%

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

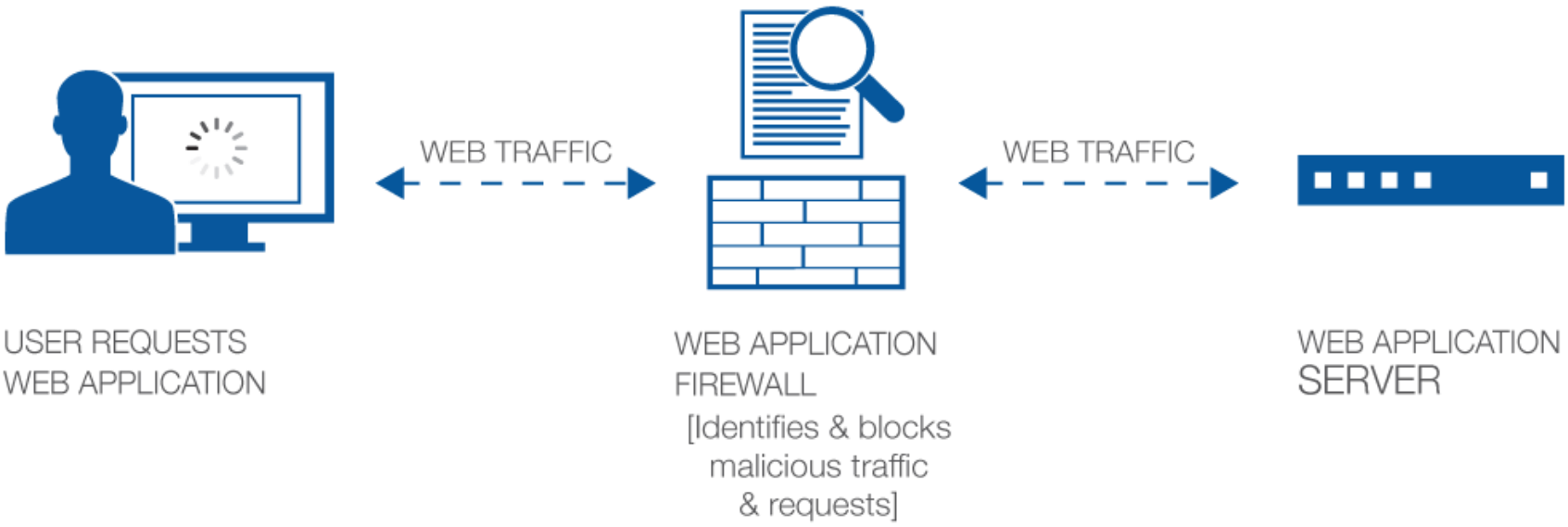
Не должно быть
бесконтрольного доступа.
Что не разрешено — запрещено!

Традиционные межсетевые экраны обычно предлагают либо удобство, либо безопасность.

NGFW решают эту проблему.

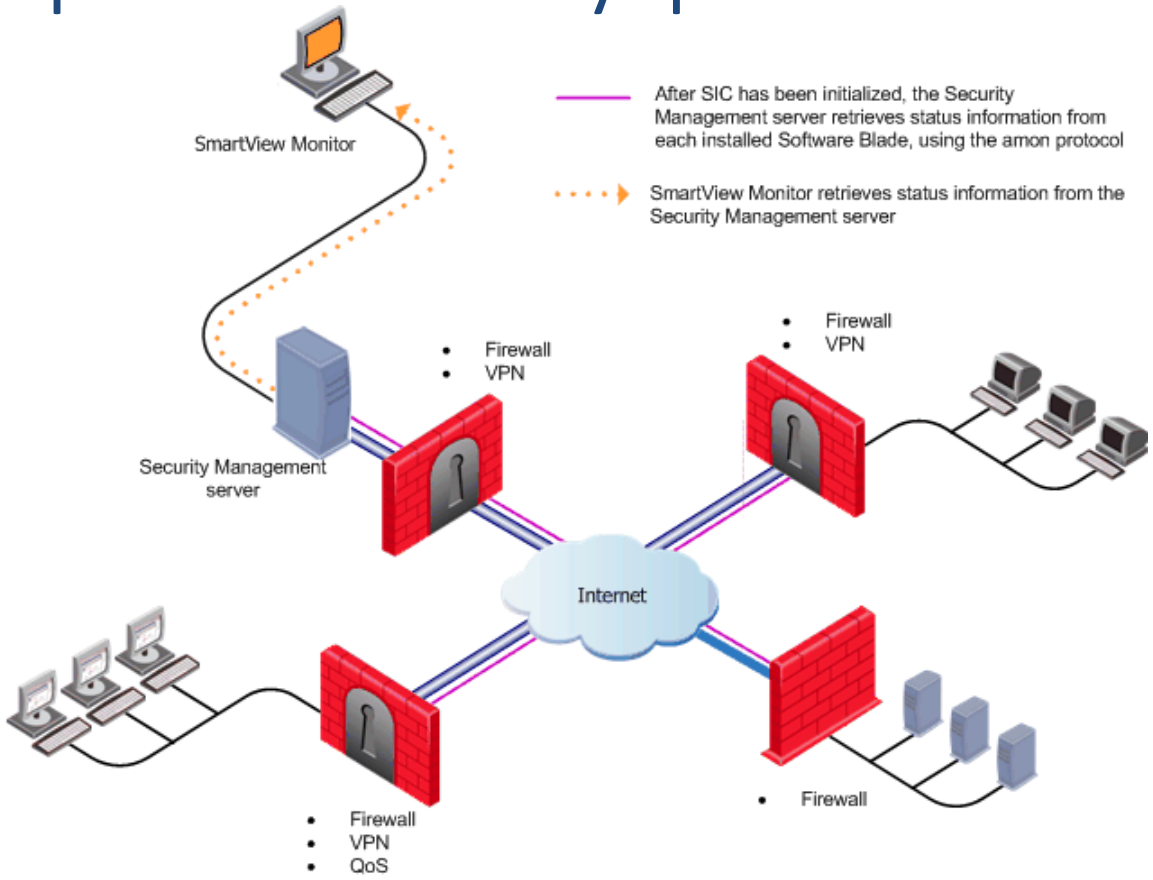
Palo Alto NG FW, Cisco ASA-X, HP TippingPoint NGFW, McAfee NGFW, CheckPoint, Fortinet FortiGate

WEB APPLICATION FIREWALL



Positive Technologies Application Firewall, Imperva Web Application Firewall , F5

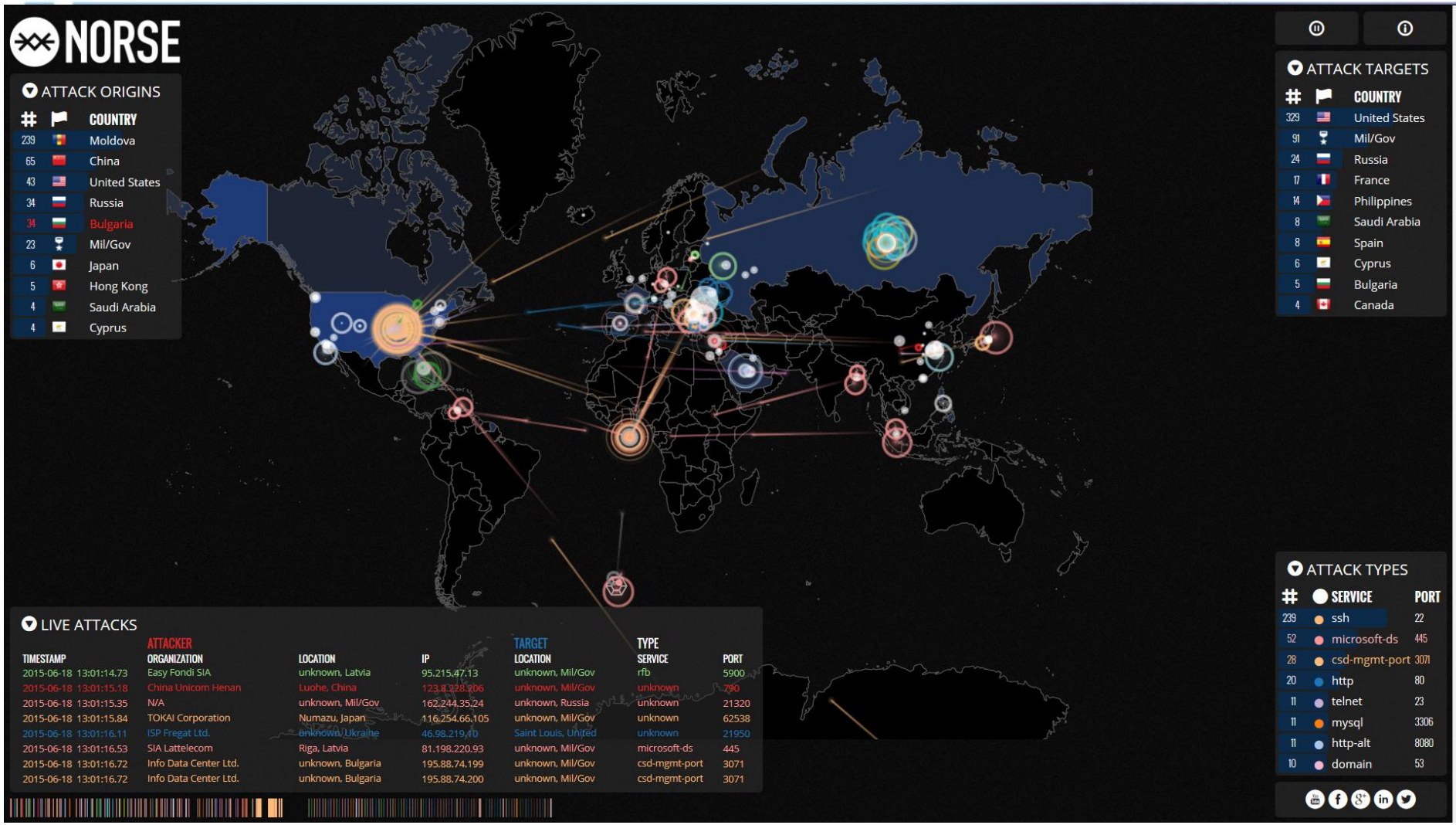
Централизованное управление защитой



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

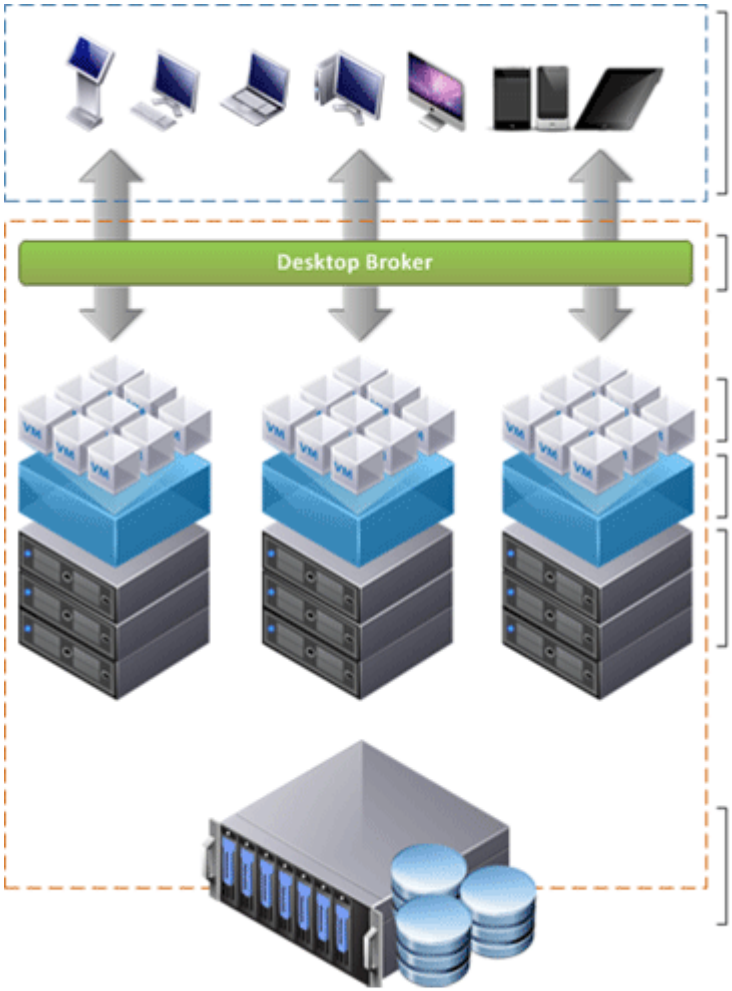
Palo Alto NG FW, Cisco FirePower, IBM XGS, HP TippingPoint, McAfee Network Security Platform

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



digitalattackmap.com **map.ipviking.com**

Arbor Networks, Qrator Labs, Kaspersky DDoS Prevention



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

Брокер клиентских подключений

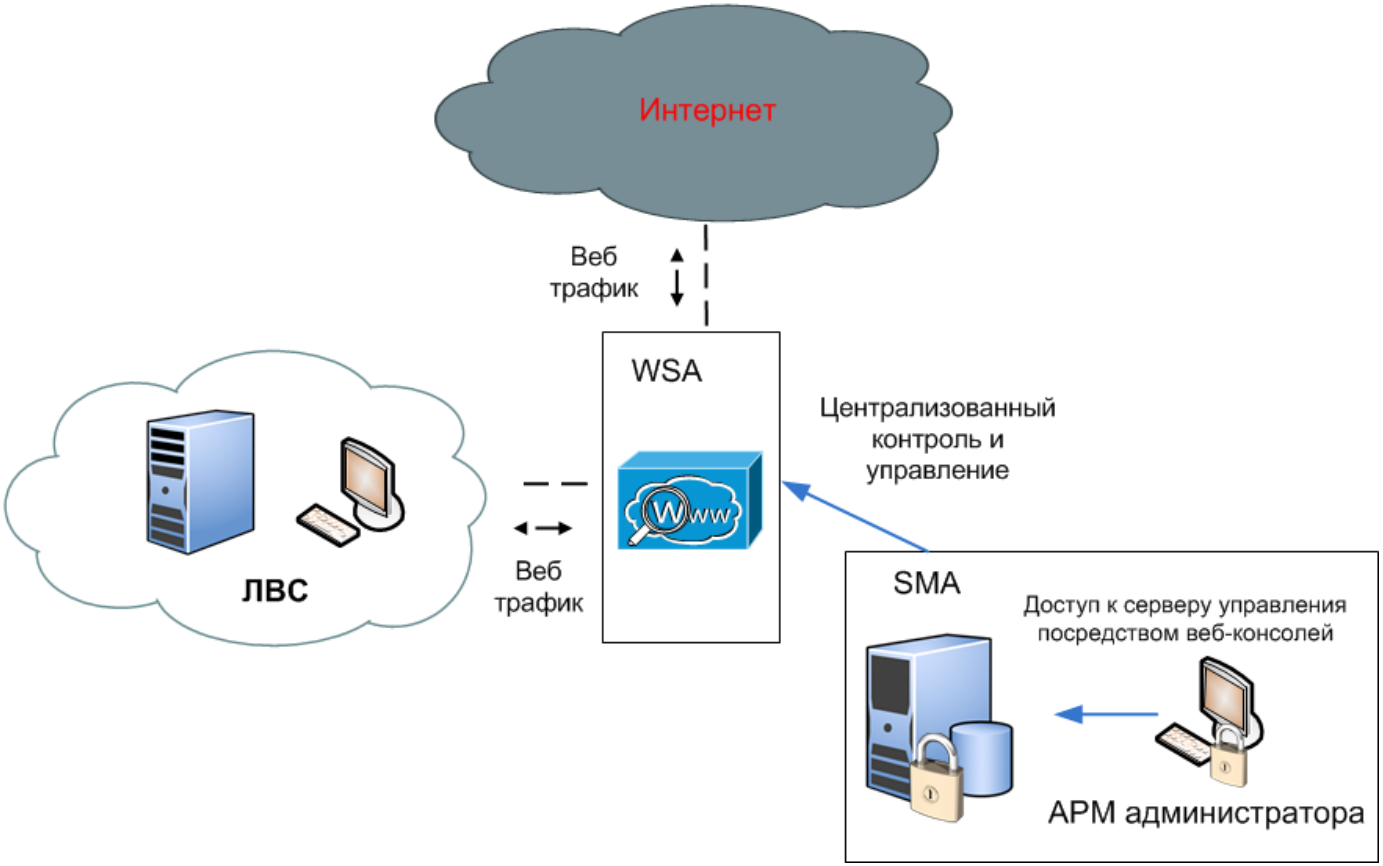
Виртуальные машины

Гипервизор

Физические сервера

Система хранения данных

VMware VDI, Citrix XenDesktop



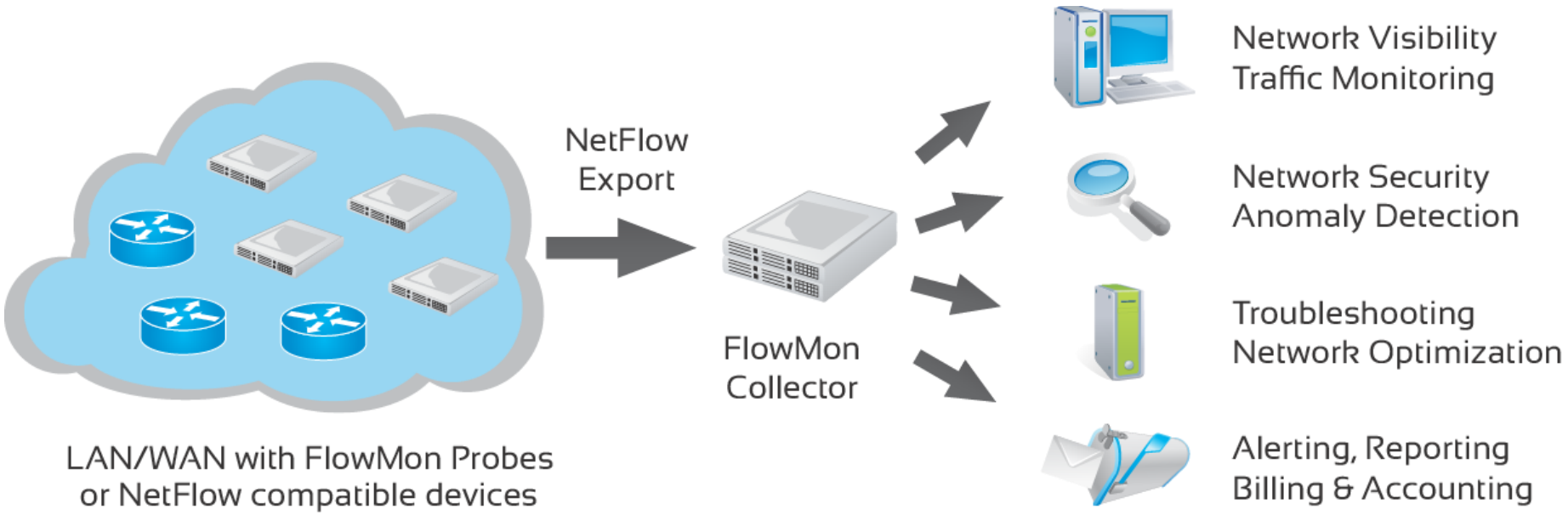
McAfee Web Gateway + McAfee Email Gateway, Cisco Web Security Appliance + Cisco Email Security Appliance, Blue Coat Secure Web Gateway, устройства из NG FW

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?