

Сеть без риска: контроль доступа для защиты данных и устройств

Алексей Брыляков

Менеджер по развитию решения
по сетевой безопасности



Предпосылки к NAC



Увеличение числа удаленных подключений и некорпоративных пользователей



Работа на собственных устройствах при подключении к сети



Рост числа подключенных IoT устройств



Shadow IT



ZERO TRUST и Контроль доступа к сети



Злоумышленники
повсюду



Нет доверенных
устройств



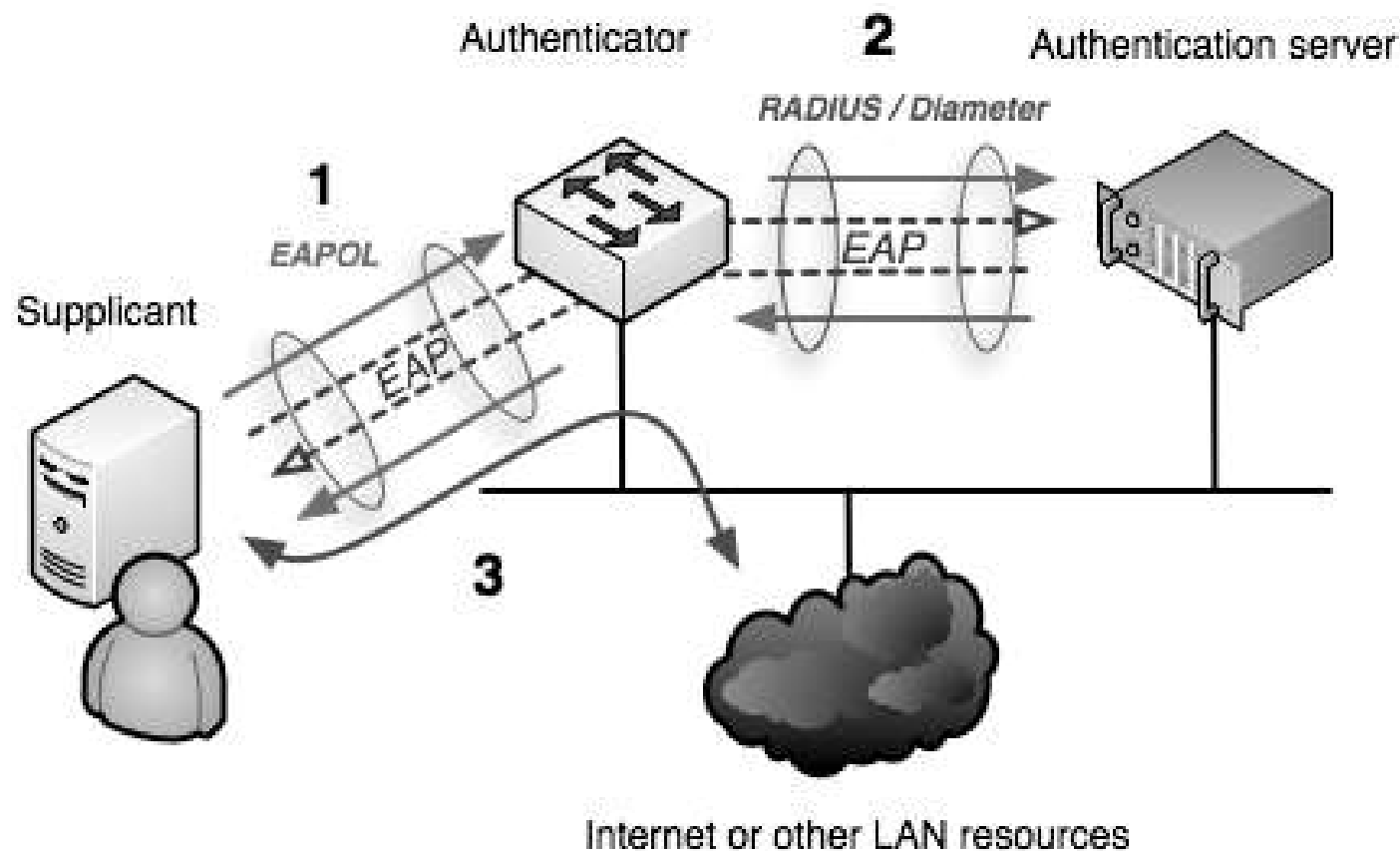
Минимум
доступа



Постоянная оценка
и мониторинг



802.1X Port-Based Network Access Control





Варианты реализации NAC

01

Применение отдельных разрозненных решений для организации доступа в сеть:

- Пользователи внутри «периметра» подключаются без проверок или используется 802.1X и FreeRADIUS
- VPN шлюзы для удаленных подключений
- Доступ для гостей отсутствует или есть Wi-Fi с WPA2 паролем
- PKI отсутствует или OpenSSL

02

Использование продуктов класса NAC (контроль доступа к сети) иностранных вендоров, таких как:

- Cisco ISE
- FortiNAC
- Portnox
- Aruba ClearPass



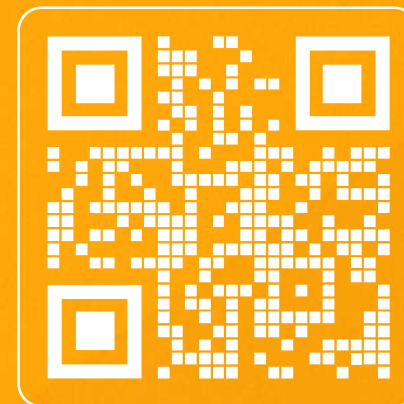
DEFENCE OPERATIONS
NETWORK ACCESS CONTROL (NAC)



USSC.RU

Спасибо за внимание!

Вопросы?



Алексей Брыляков
Менеджер по развитию
решения по сетевой
безопасности

abrylyakov@ussc.ru