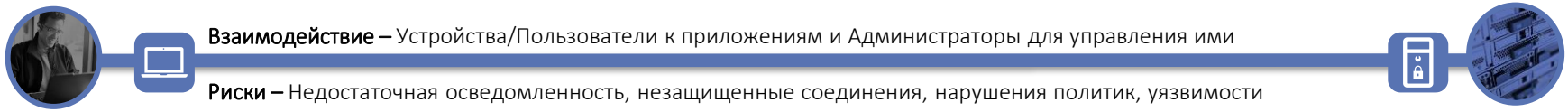
CISCO
SECURE

The bridge to possible

Защита удаленного пользователя

Михаил Кадер
mkader@cisco.com
08.07.2021

Взаимодействие и риски

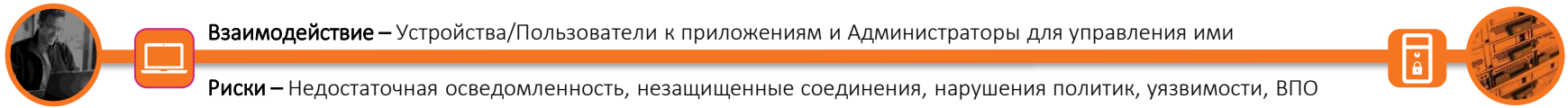


Взаимодействие – Устройства/Пользователи к приложениям и Администраторы для управления ими

Риски – Недостаточная осведомленность, незащищенные соединения, нарушения политик, уязвимости

Удаленное рабочее место

Приложения (ЦОД)

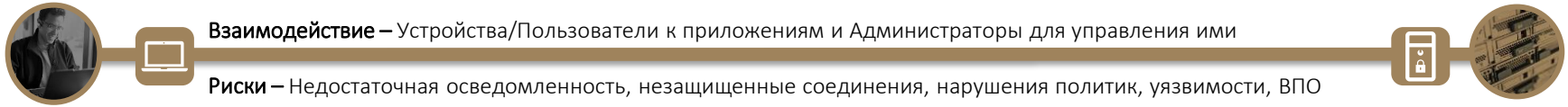


Взаимодействие – Устройства/Пользователи к приложениям и Администраторы для управления ими

Риски – Недостаточная осведомленность, незащищенные соединения, нарушения политик, уязвимости, ВПО

Удаленное рабочее место

Приложения (Публичное облако)

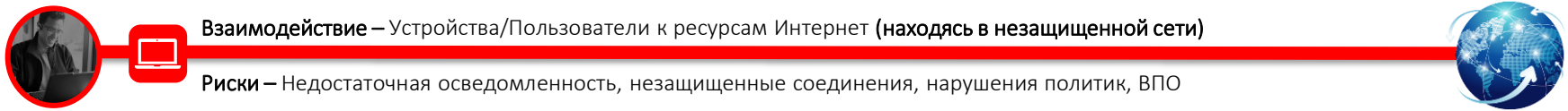


Взаимодействие – Устройства/Пользователи к приложениям и Администраторы для управления ими

Риски – Недостаточная осведомленность, незащищенные соединения, нарушения политик, уязвимости, ВПО

Удаленное рабочее место

Приложения (Гибридное облако)



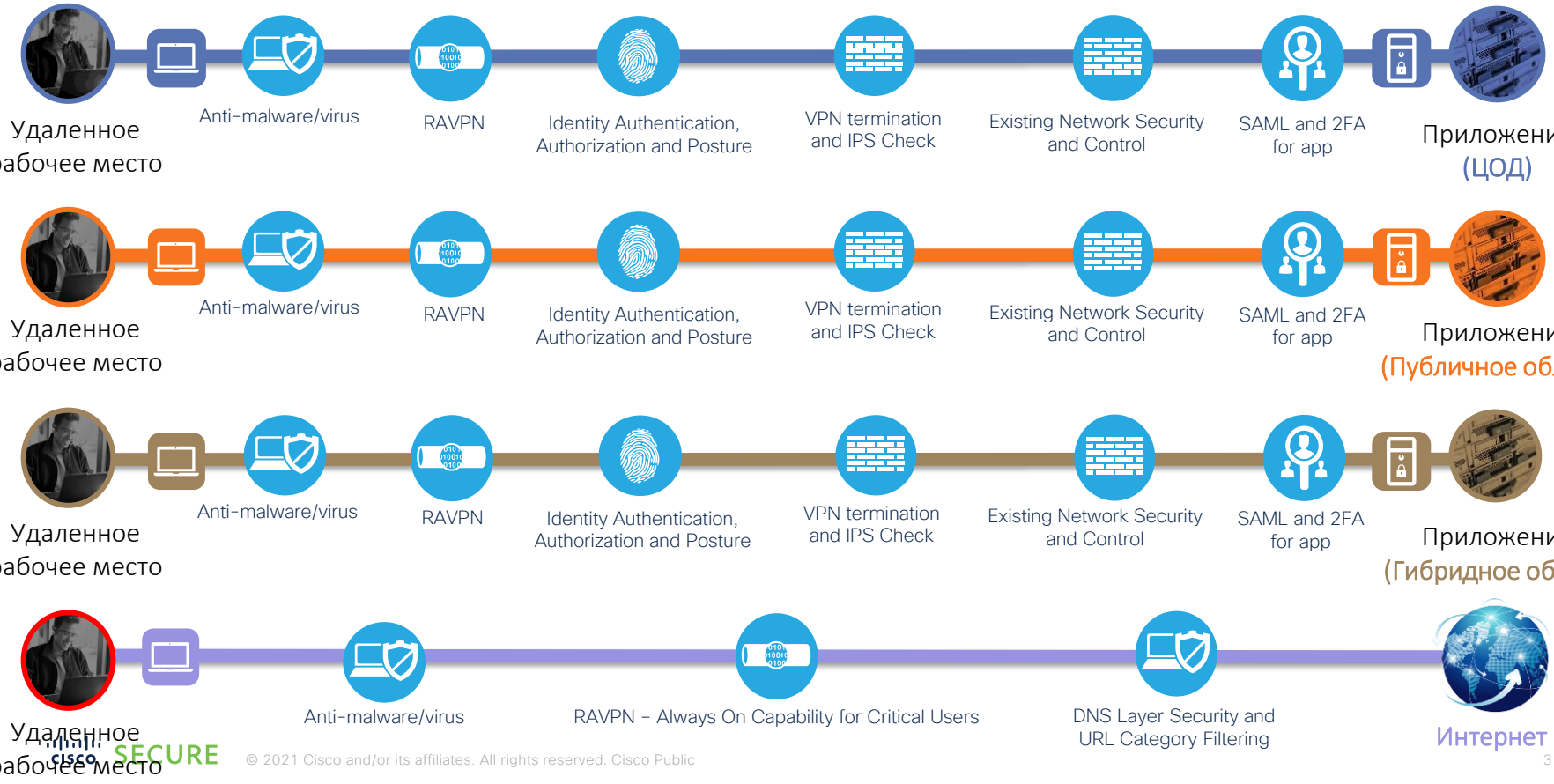
Взаимодействие – Устройства/Пользователи к ресурсам Интернет **(находясь в незащищенной сети)**

Риски – Недостаточная осведомленность, незащищенные соединения, нарушения политик, ВПО

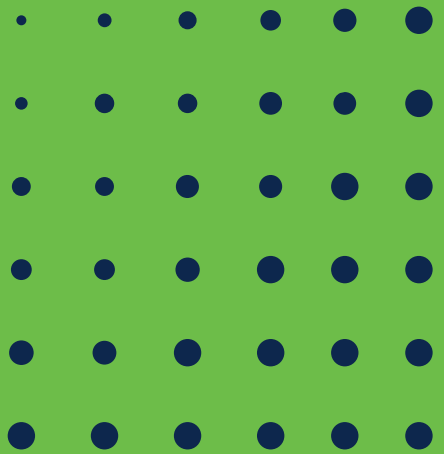
Удаленное рабочее место

Интернет

Защитные средства



Сценарии



Удаленный пользователь подключается в ЦОД

Удаленный сотрудник

AWS

VPC

Cisco ASAv/NGFWv

internet gateway

VPC Attachment

AWS Transit Gateway

VPC

EC2

EC2

VPC Attachment

VPC

EC2

EC2

INTERNET

Data Center

HA or Clustering with VPN Load Balancing

Cisco ASA/NGFW or CISCO ASAv/NGFWv on Hypervisior

IPSEC S2S VPN

Colo (Hybrid Cloud)

Azure

vNET

Cisco ASAv/NGFWv

Azure VPN Gateway

vNET Peering

vNET

VM

VM

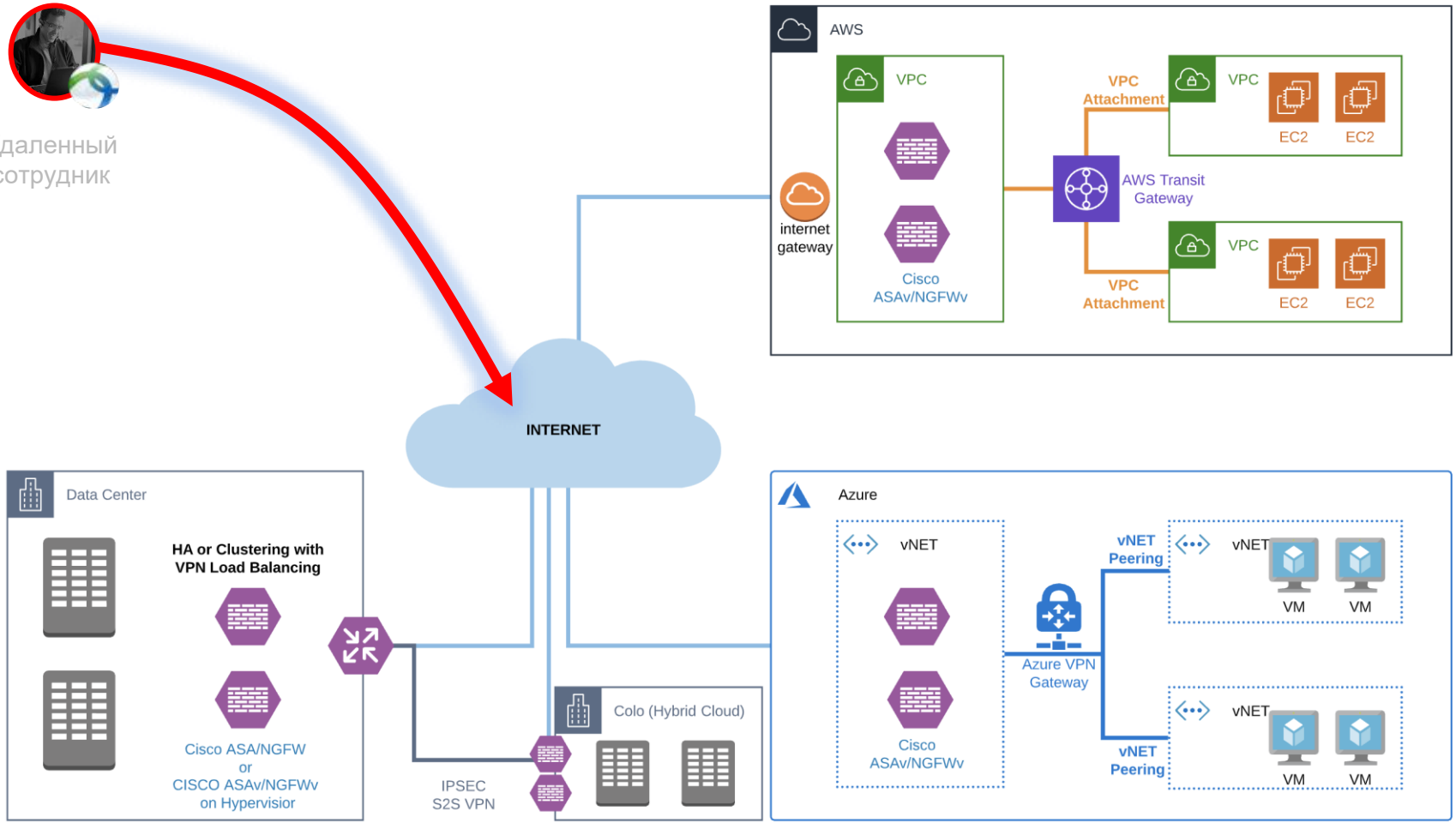
vNET Peering

vNET

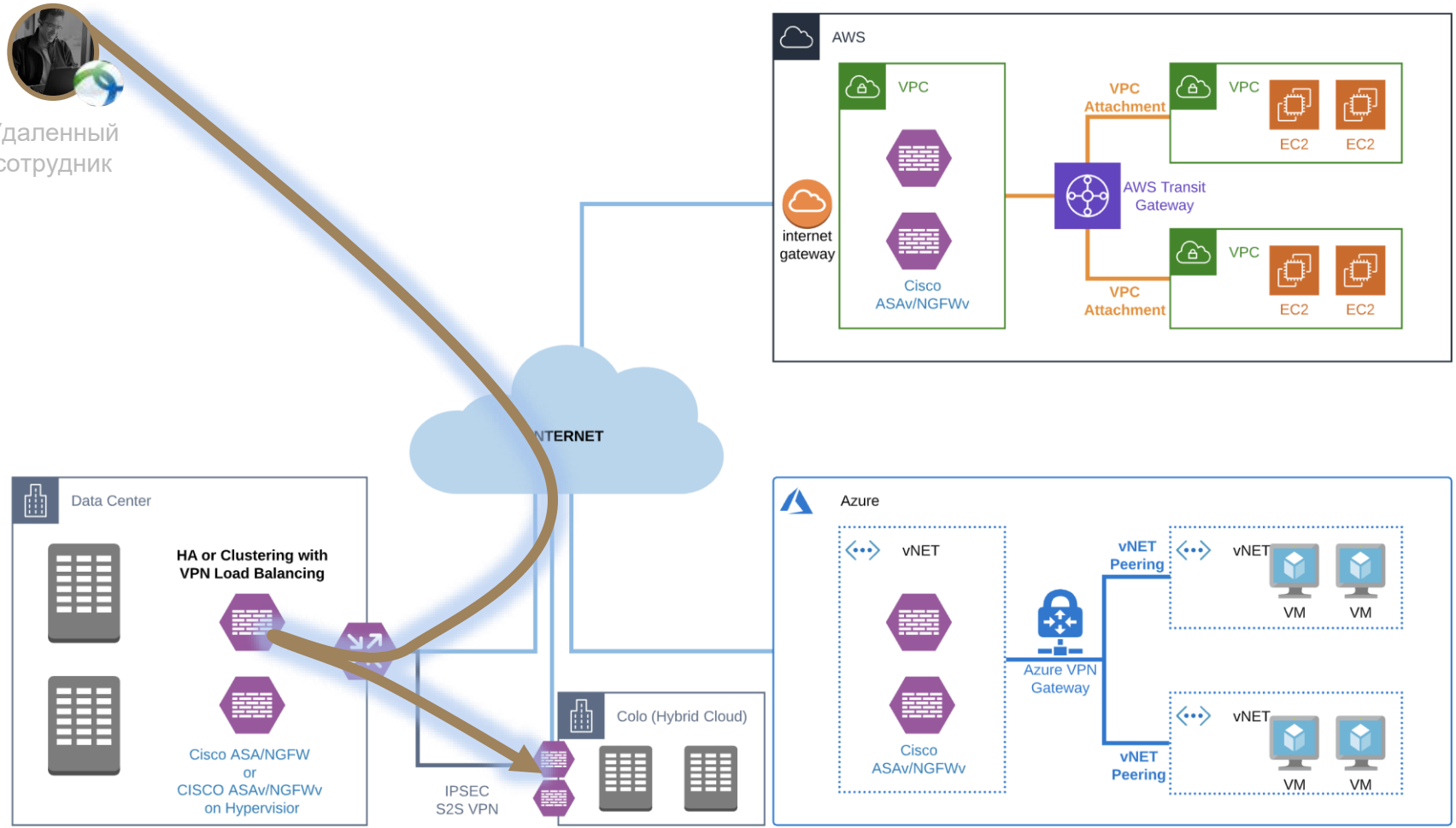
VM

VM

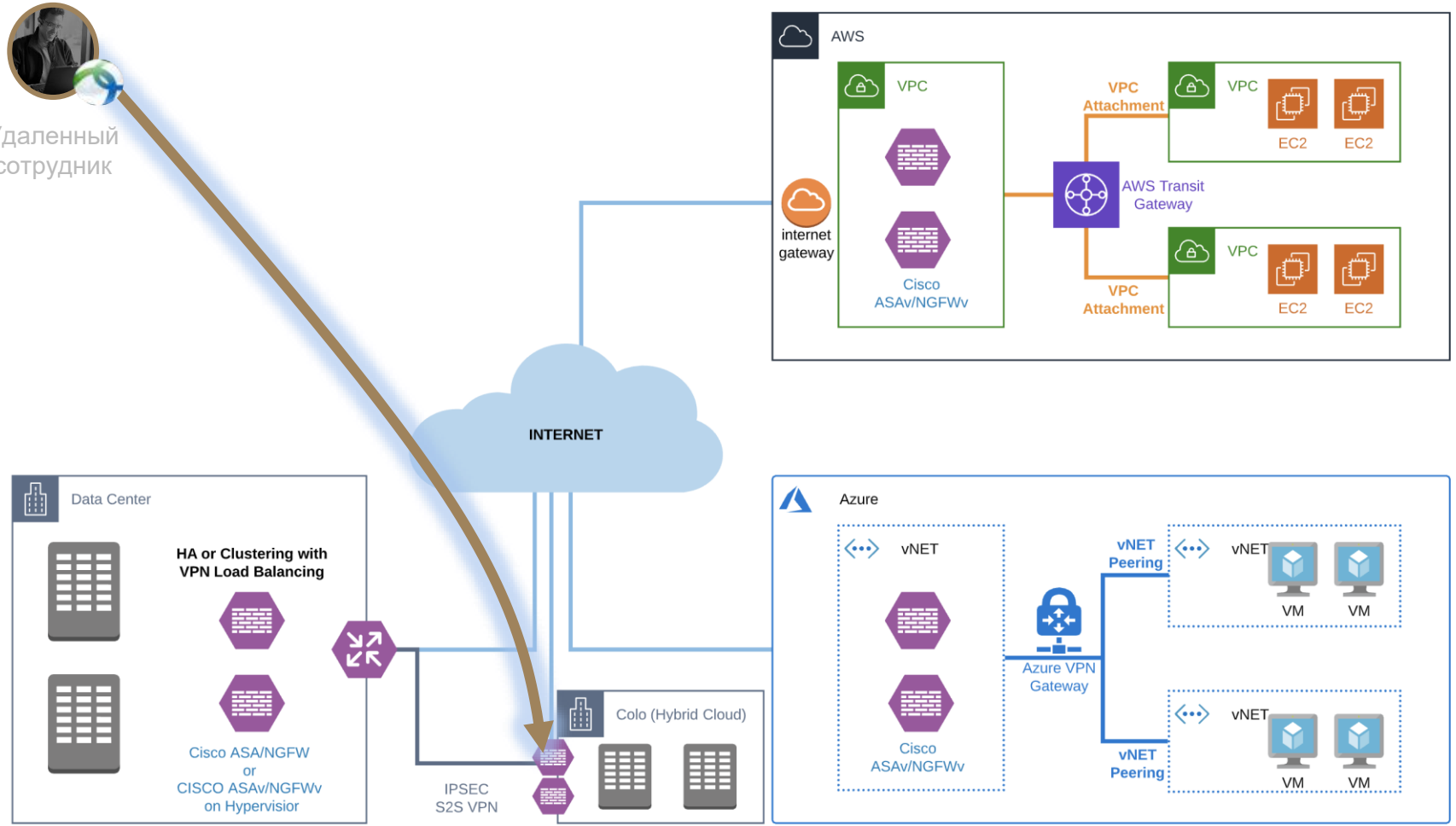
Удаленный пользователь подключается в Интернет



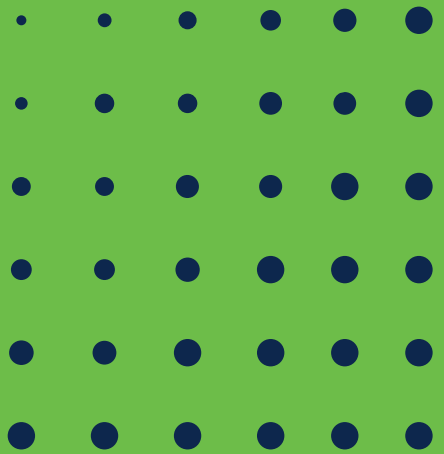
Удаленный пользователь подключается в гибридное облако



Удаленный пользователь подключается в гибридное облако



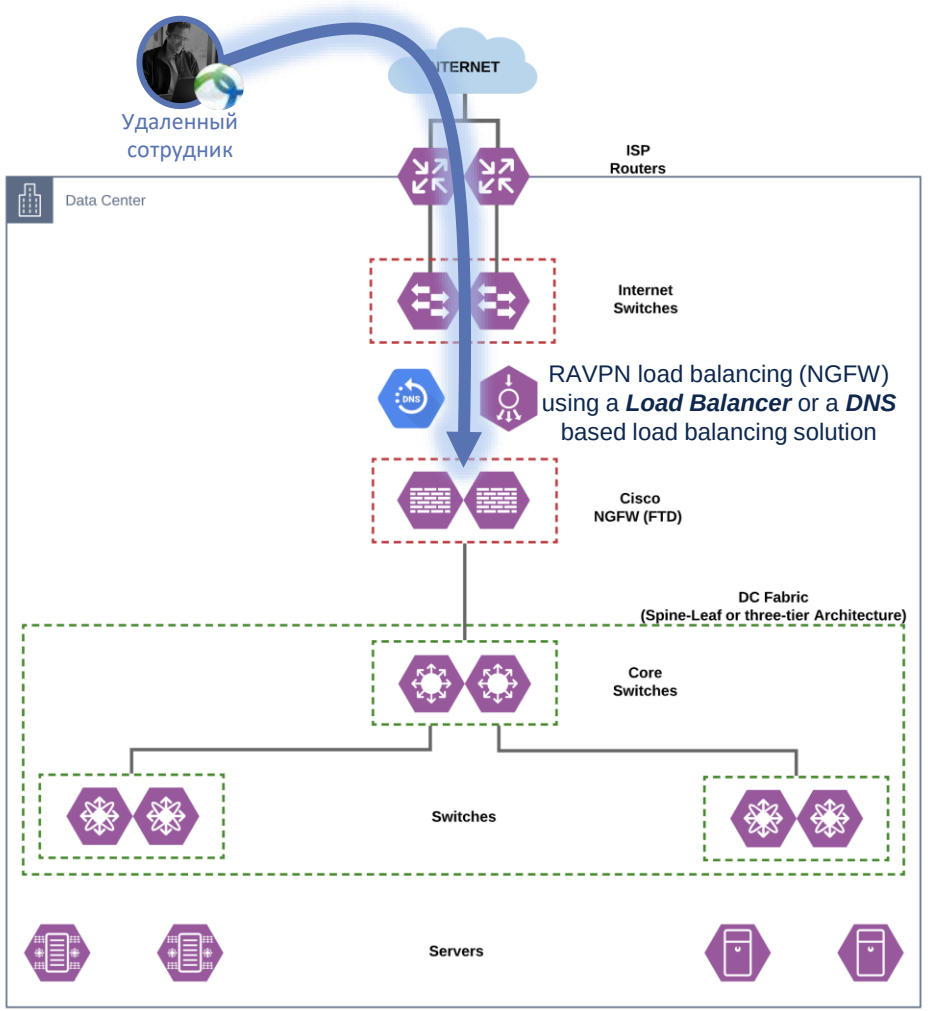
Балансировка трафика



ЦОД

Шлюз VPN поддерживает высокую доступность и кластеризацию для масштабируемости

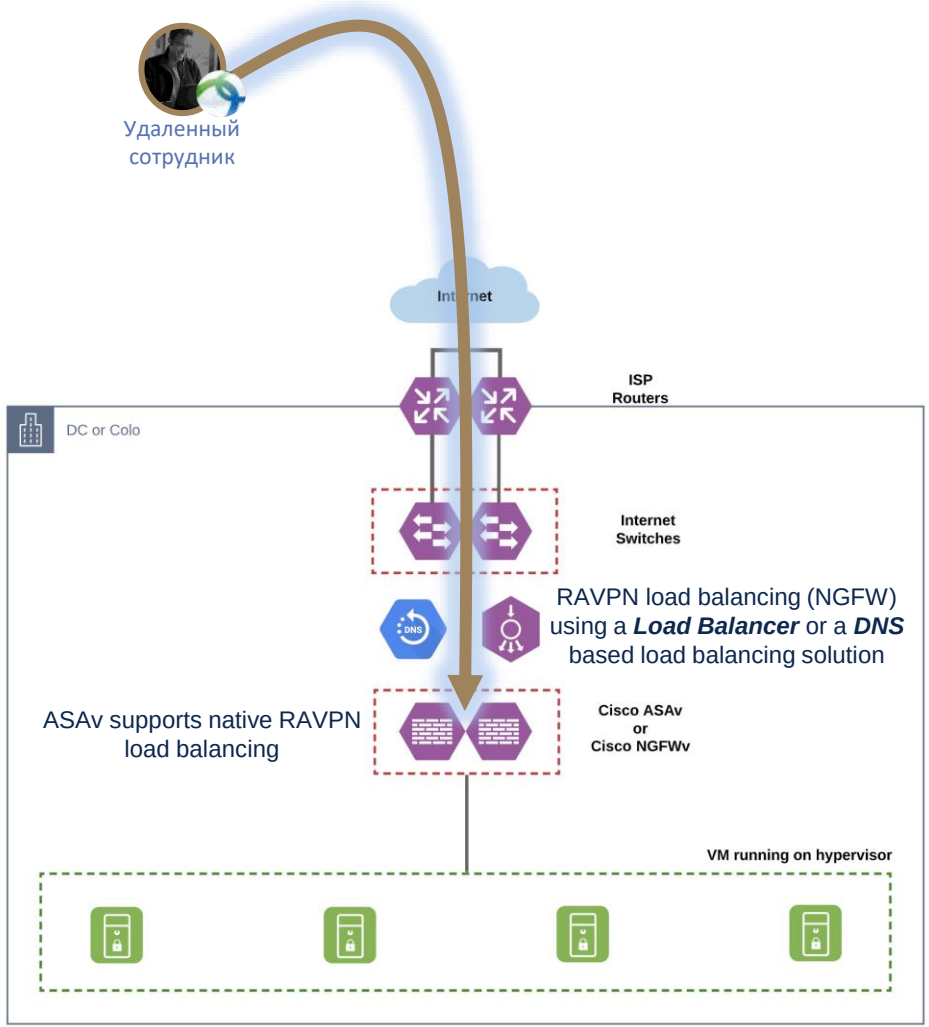
Балансировка соединений VPN или работает как часть кластера или требует внешнего балансировщика или распределения трафика за счет использования DNS



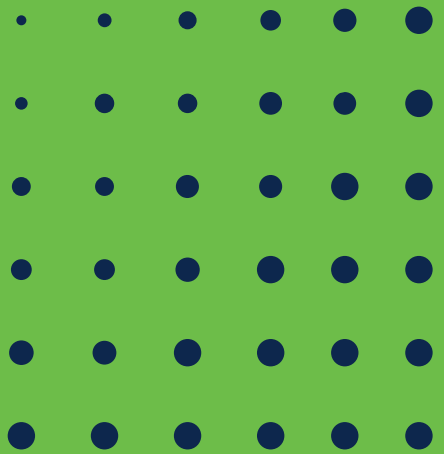
Гибридное облако

Высокая доступность и кластеризация для отказоустойчивости

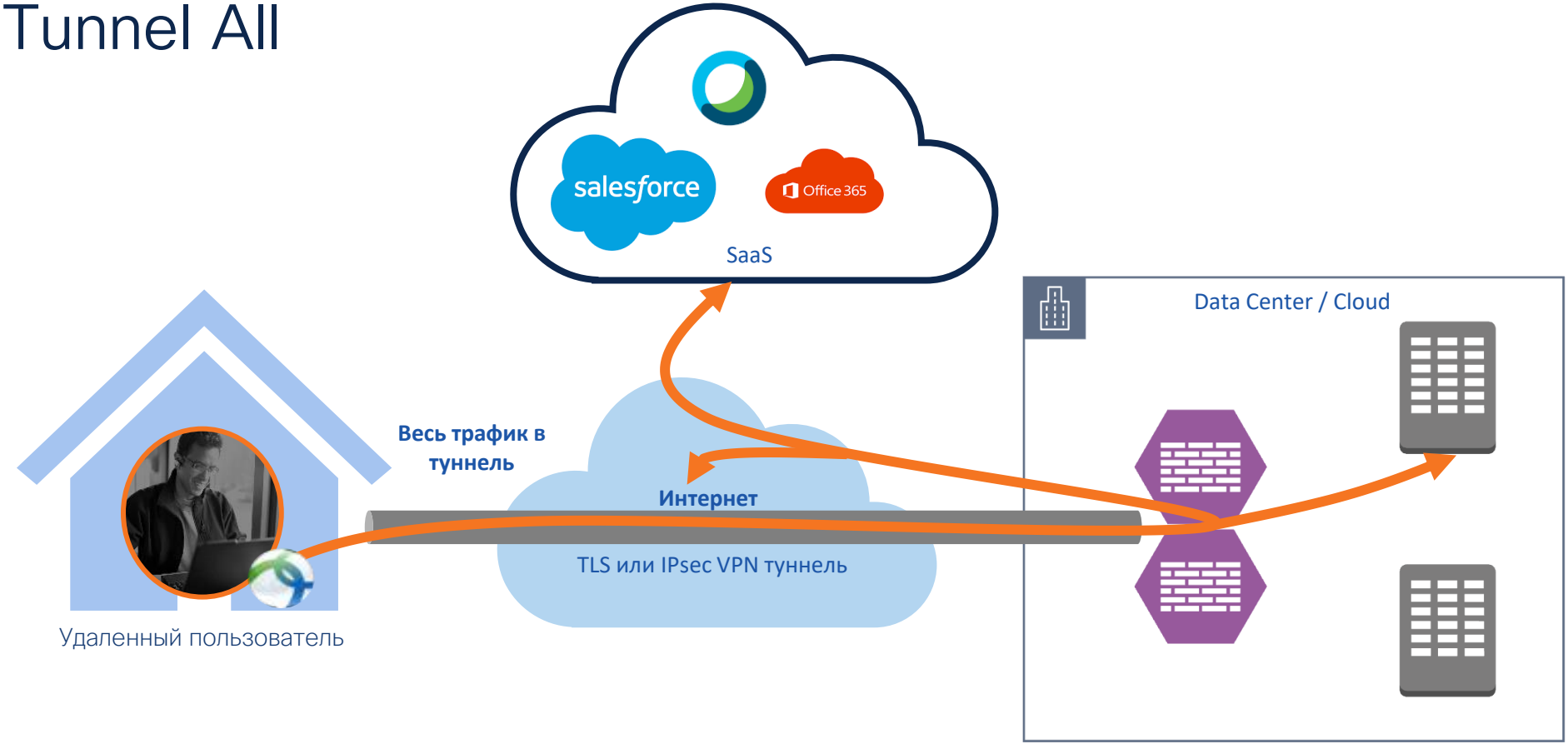
- Технология создания кластеров с динамической балансировкой
- Балансировка VPN за счет внешнего балансировщика или распределения трафика за счет использования DNS



Защита пользователя

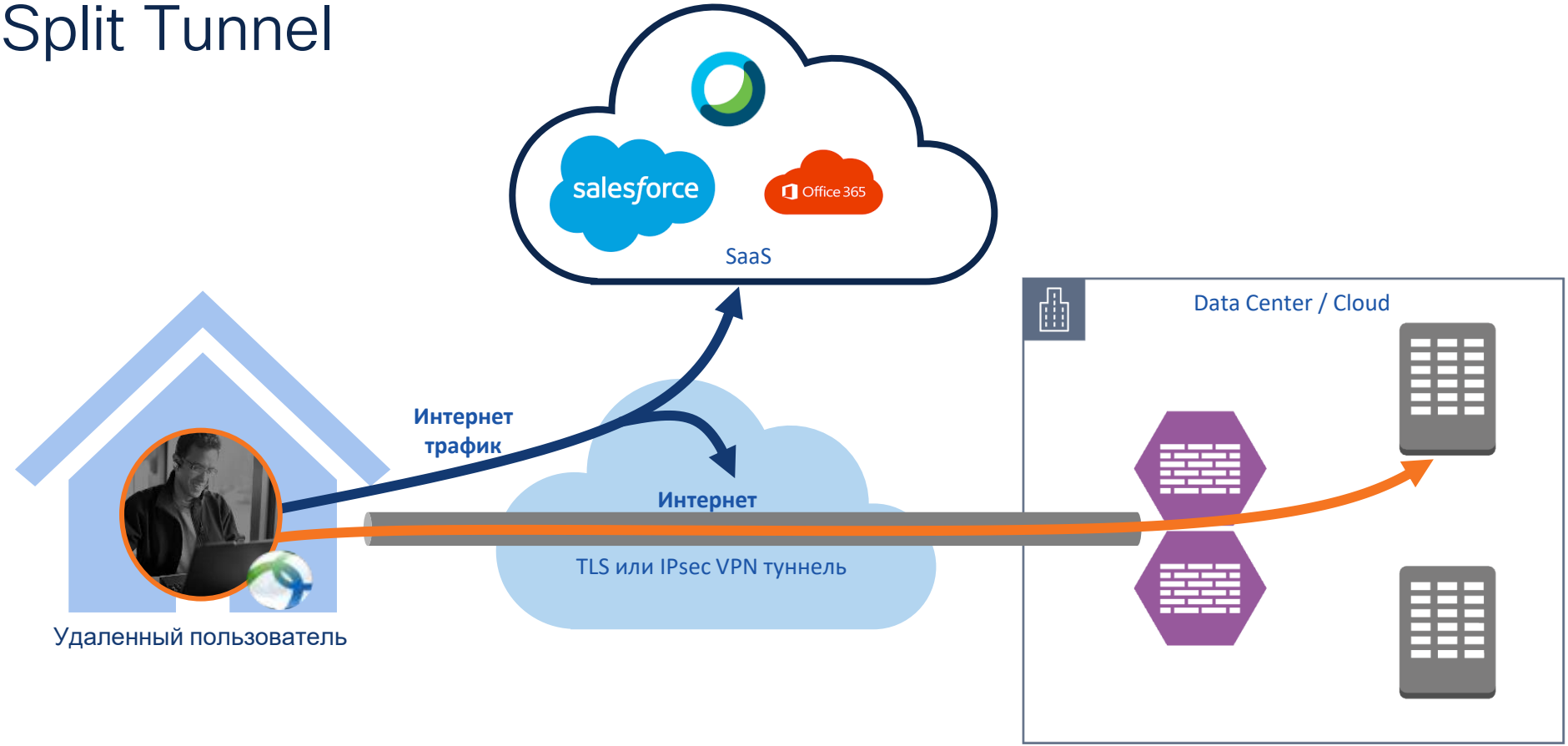


Tunnel All



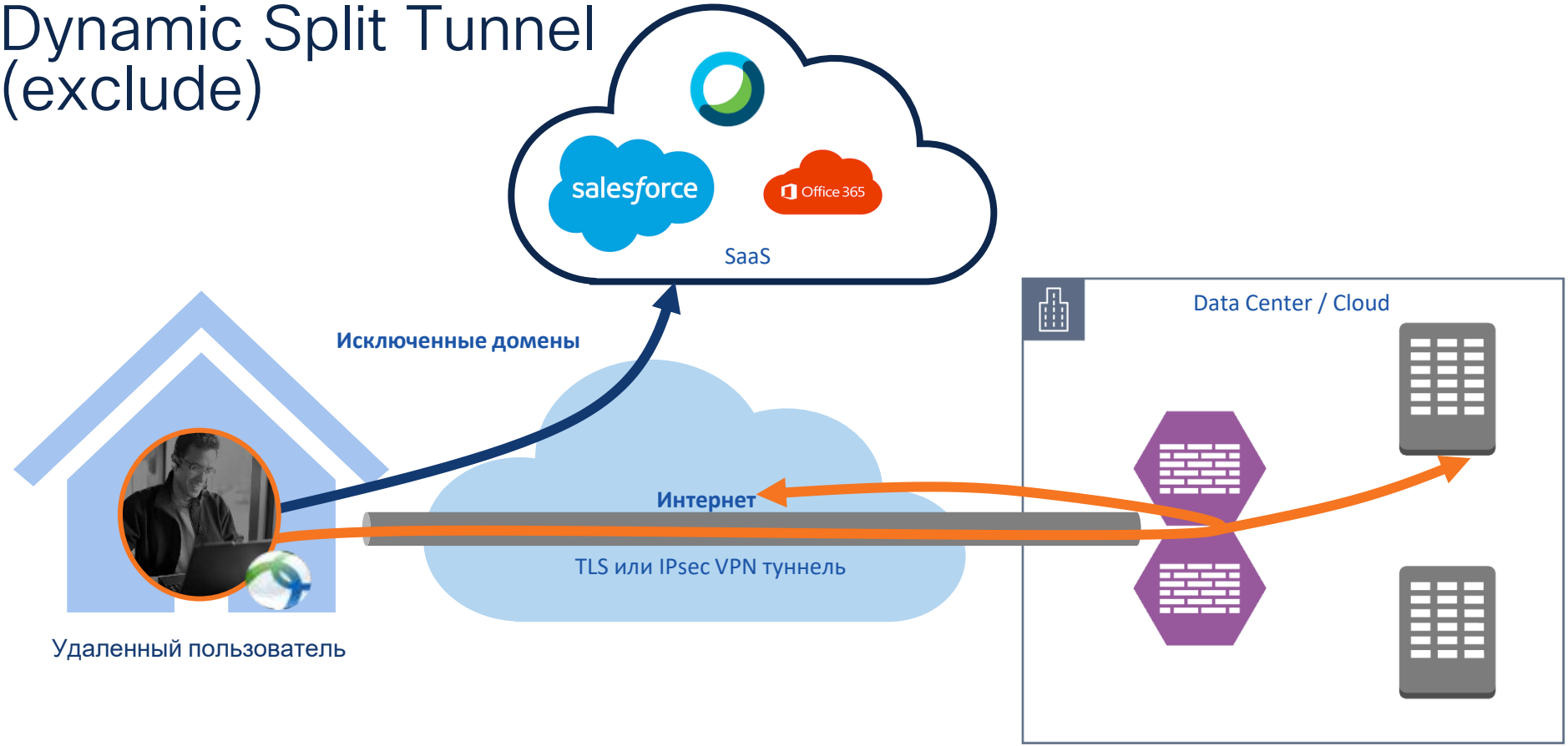
Маршрут по умолчанию в туннель – зашифровать все

Split Tunnel



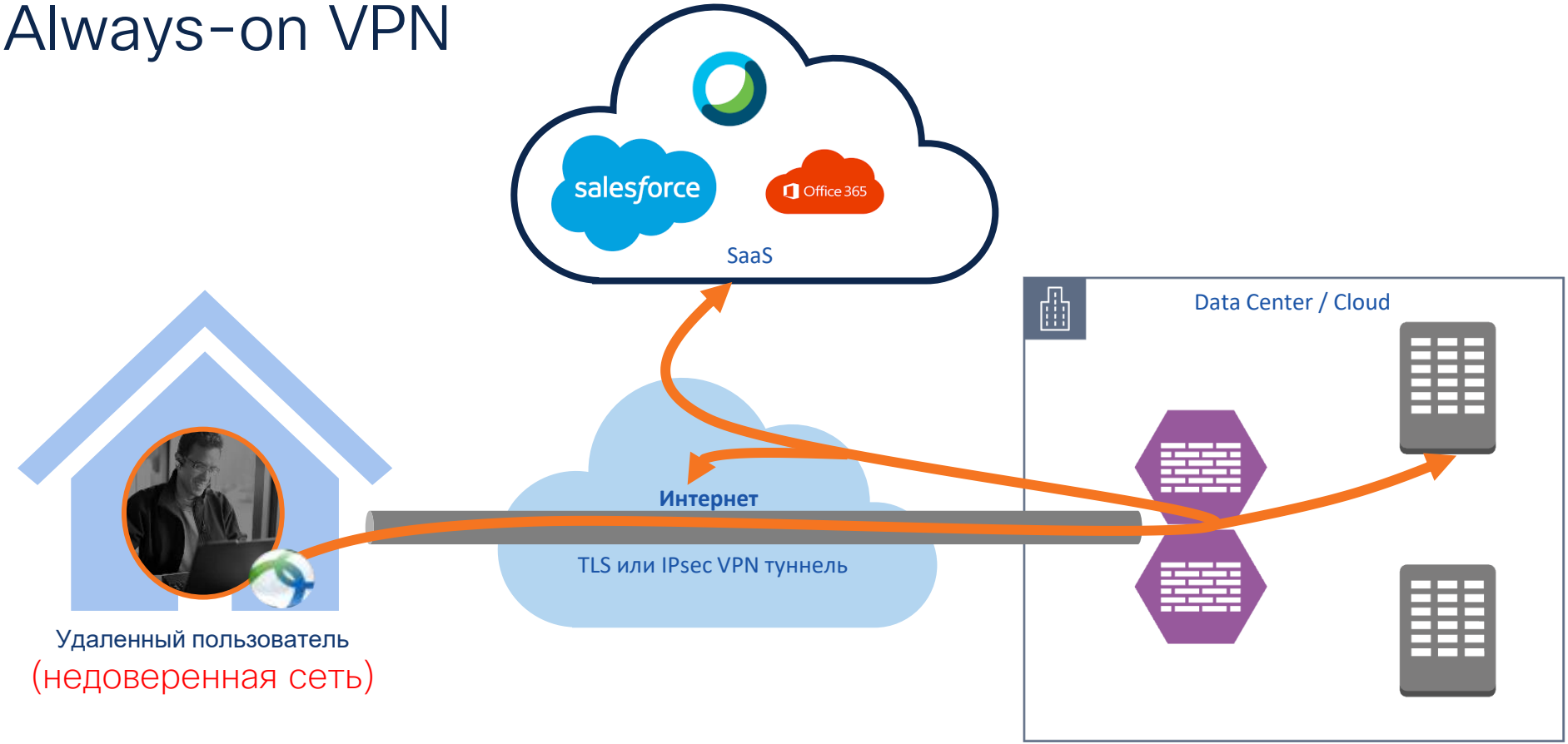
Маршруты, определенные SPLIT ACL, отправлены на клиента RA VPN

Dynamic Split Tunnel (exclude)



Маршруты для исключенных доменов передаются на клиента RAVPN

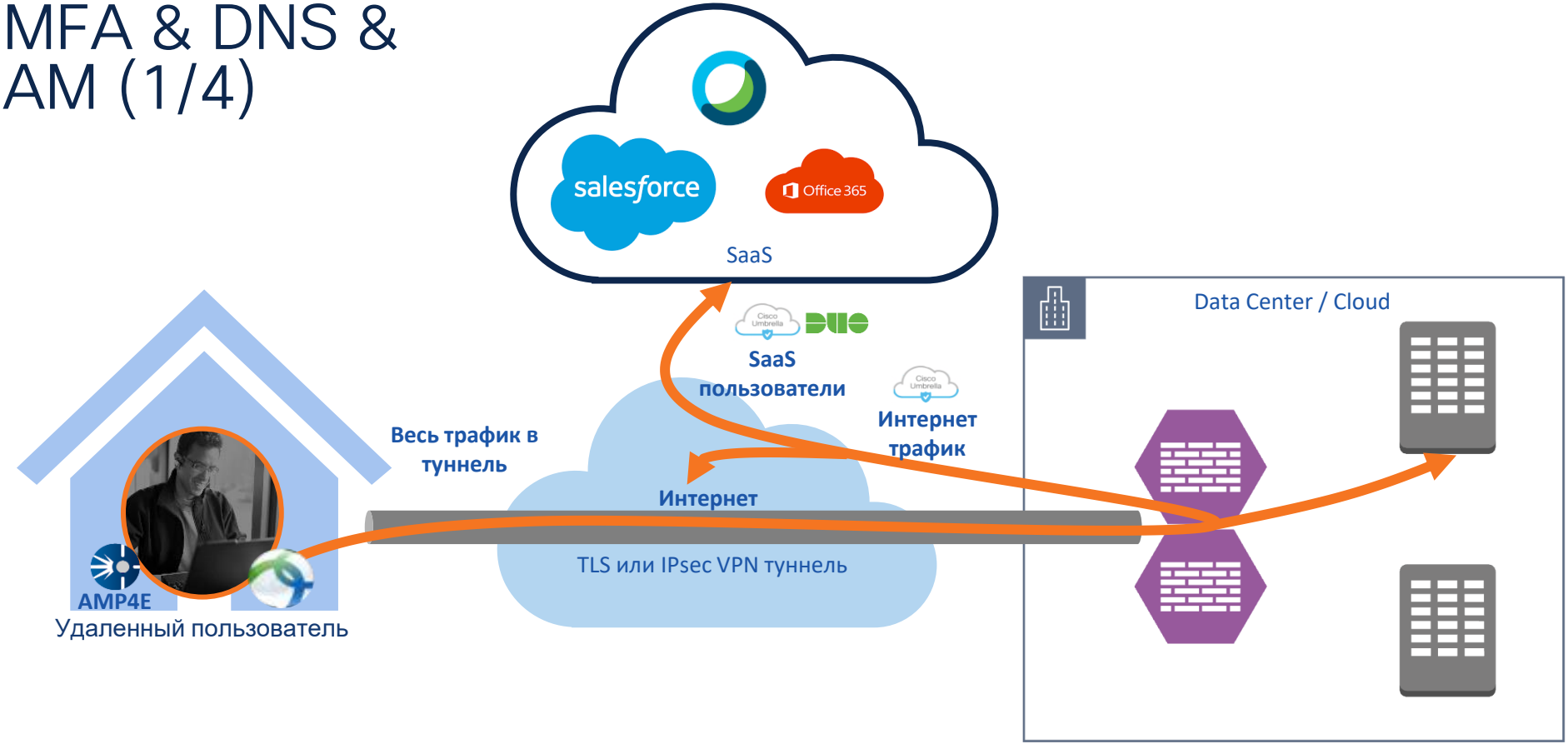
Always-on VPN



Always-On предотвращает прямой доступ в Интернет, когда компьютер не в доверенной сети

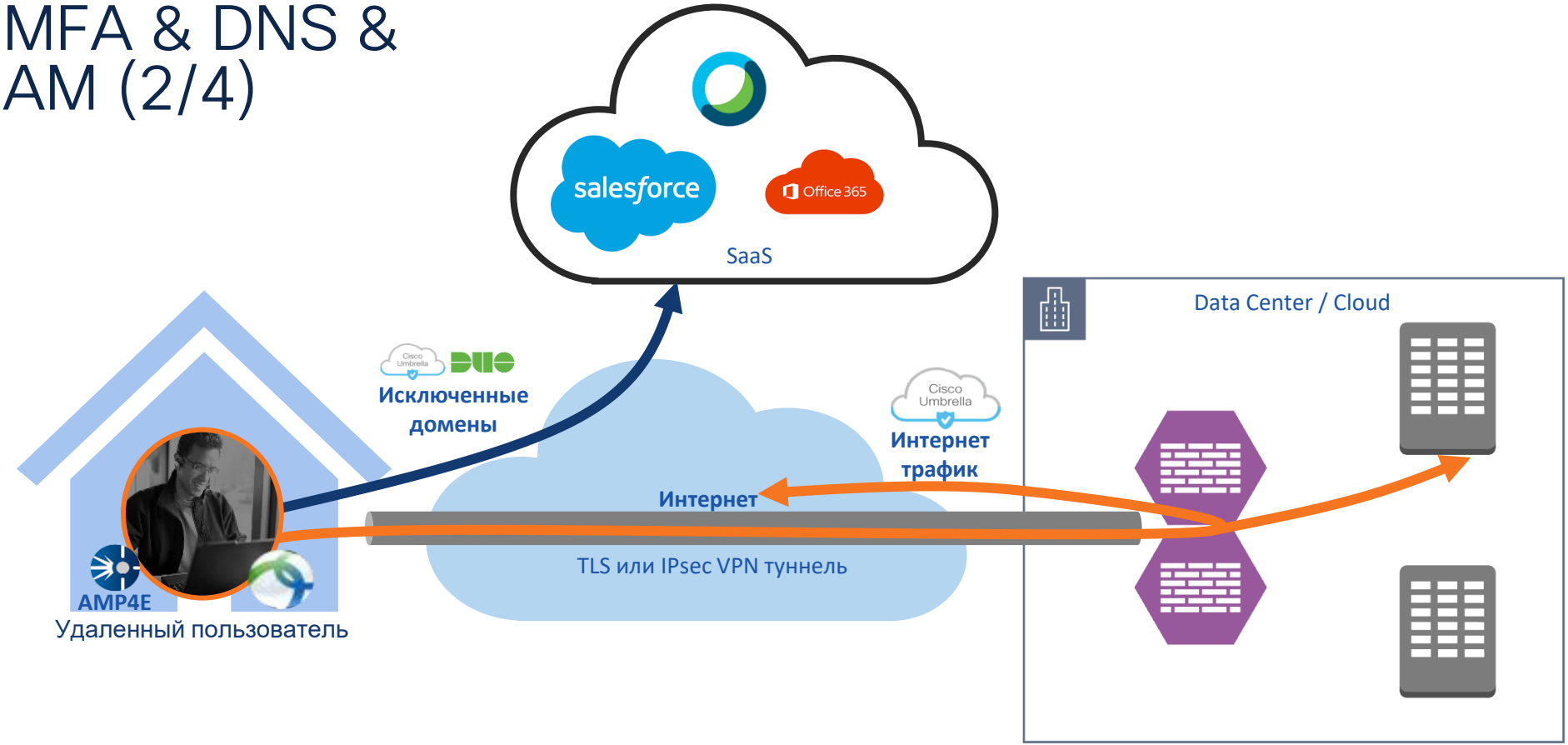
MFA, Контроль DNS & Anti-malware

MFA & DNS & AM (1/4)



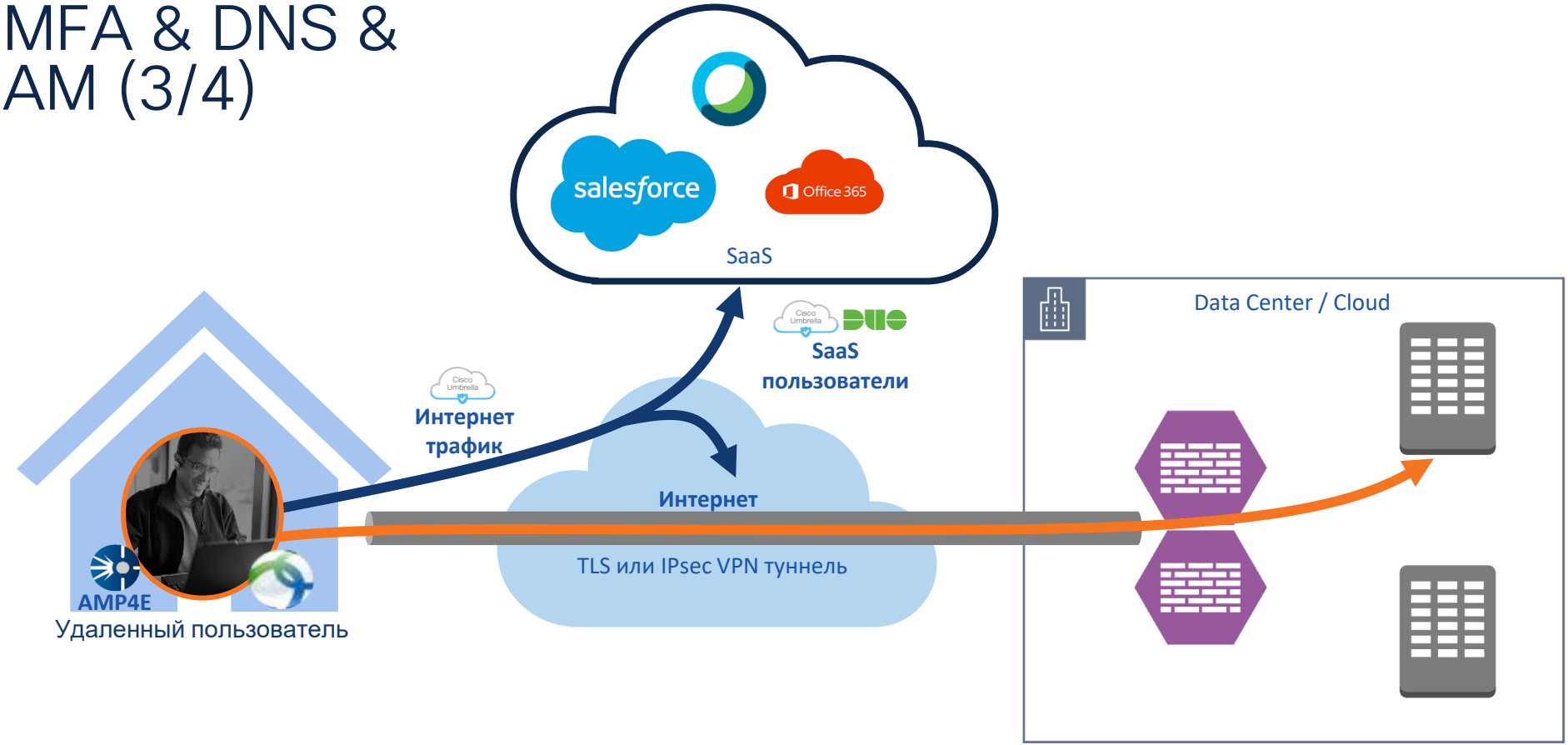
SaaS и Интернет пользователи защищены Umbrella –Tunnel All

MFA & DNS & AM (2/4)



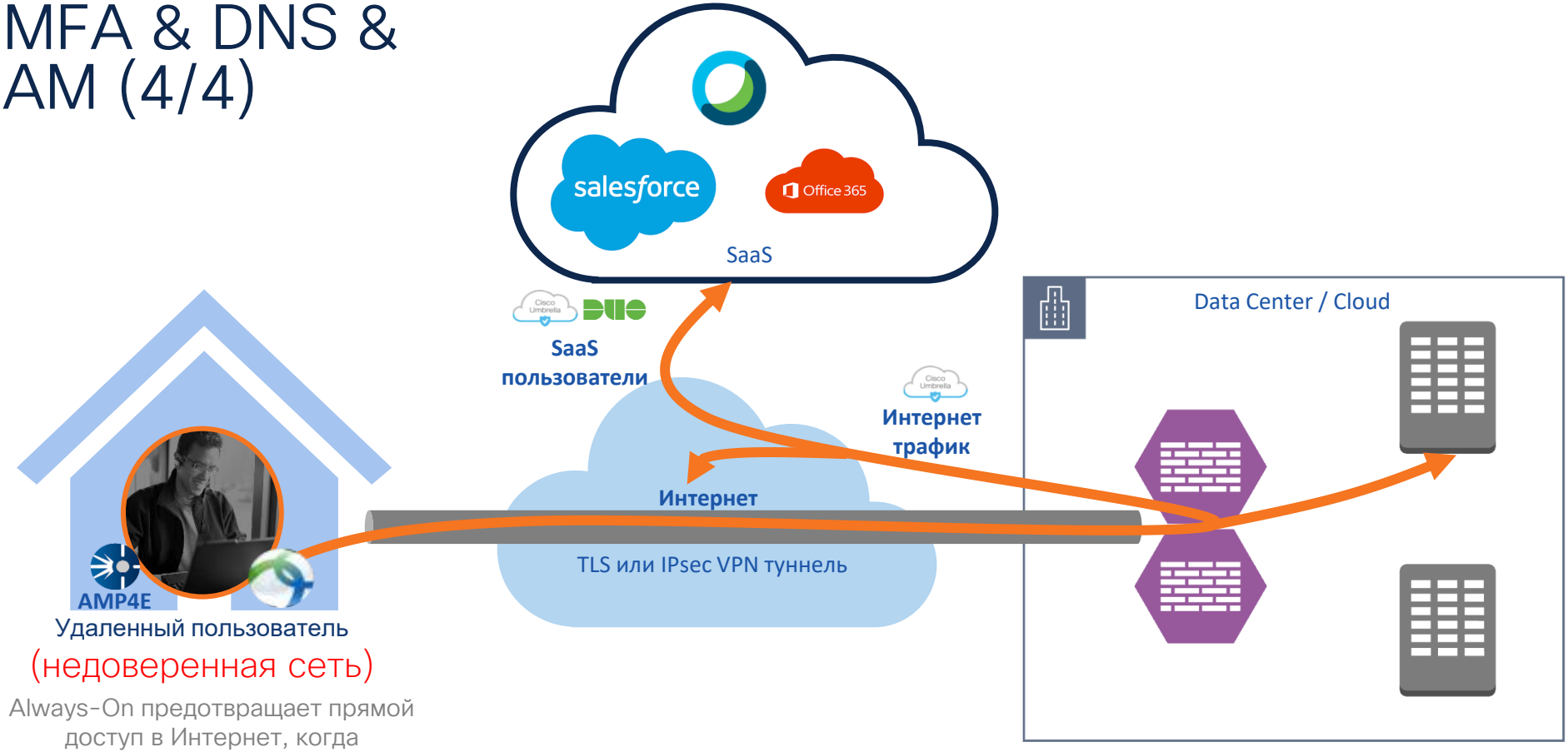
SaaS и Интернет пользователи защищены Umbrella – Exclude Domain

MFA & DNS & AM (3/4)



SaaS и Интернет пользователи защищены Umbrella – Split Tunnel

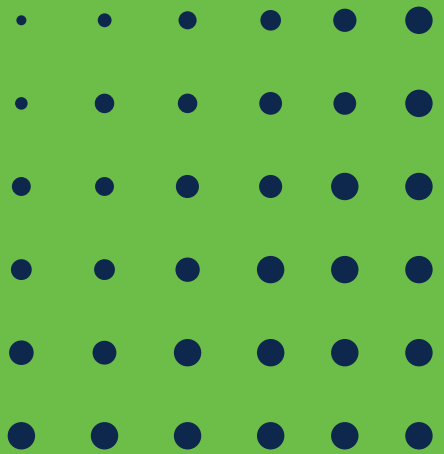
MFA & DNS & AM (4/4)



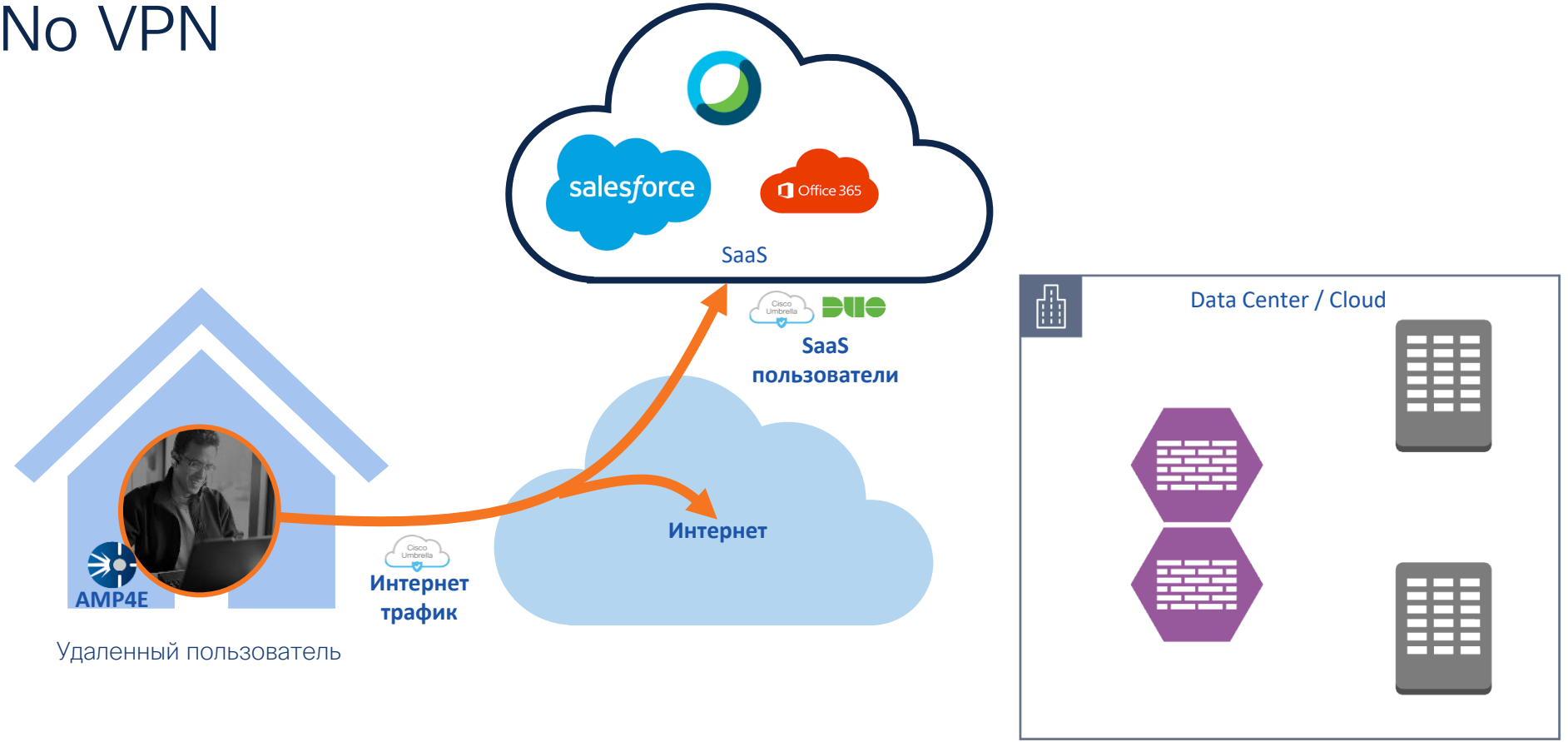
Always-On предотвращает прямой доступ в Интернет, когда компьютер не в доверенной сети

SaaS и Интернет пользователи защищены Umbrella – Always-on VPN

А без VPN?



No VPN



Сотрудник защищен даже без VPN – AM, DNS, MFA

Дополнительная информация

Можно еще посмотреть

- Подробные архитектурные руководства по внедрению систем удаленного доступа и не только: https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_safe.html#~tab-design

- Много технических публикаций на https://habr.com/ru/company/cisco/


cisco
SECURE