

FORTINET[®]



FortiNAC

Решение класса Network Access Control

Юрий Захаров
Системный инженер

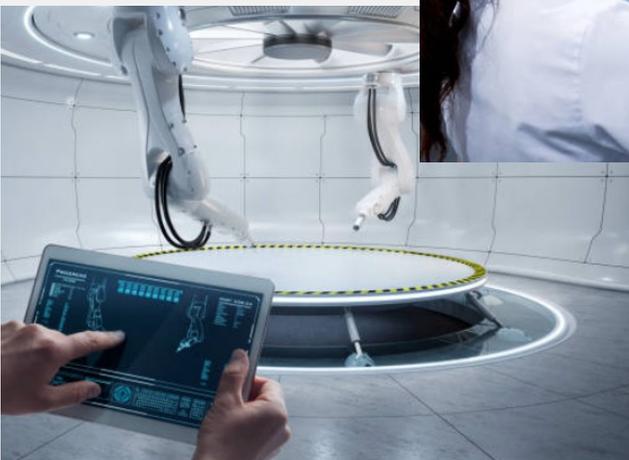


cis@fortinet.com
cis_se@fortinet.com

14 декабря 2021



Драйверы рынка



Ожидается более 30.9млрд IoT устройств в мире к 2025. (Источник: *Business Insider, IoT Analytics, Gartner, Intel, Statista*)

93% организаций внедряют технологии Интернета вещей (Source: *Fierce Electronics, Security Today*)

Количество атак злоумышленников увеличилось на 54% в 2019 (в том числе на устройства IoT)





FortiNAC

ВЫ НЕ КОНТРОЛИРУЕТЕ ТО,
ЧТО НЕ МОЖЕТЕ ВИДЕТЬ



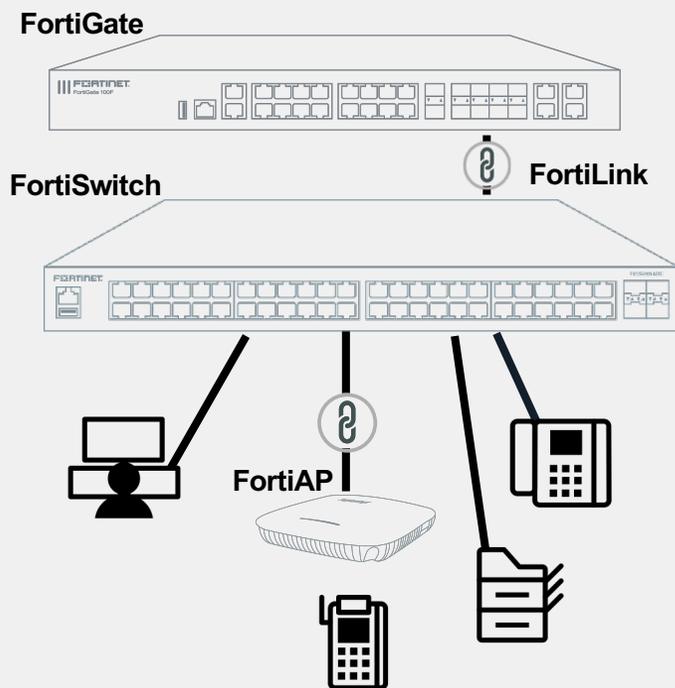
Принципы «нулевого» доверия

1. Знание сети (в т.ч. пользователей, устройств, сервисов и данных)
2. Оценка поведение пользователей, состояние устройств и сервисов
3. Использование политик аутентификации и авторизации доступа
4. Мониторинг пользователей, устройств и сервисов
5. Не доверяйте никакой сети, в том числе своей
6. Поддержка принципов «нулевого» доверия при проектировании сервисов



NAC предоставляет видимость и контроль

FortiLink NAC



Бесплатен в архитектуре Fortinet LAN Edge



FortiNAC



Выделенное решение с поддержкой устройств сторонних производителей

Fortinet Security Fabric

Комплексная

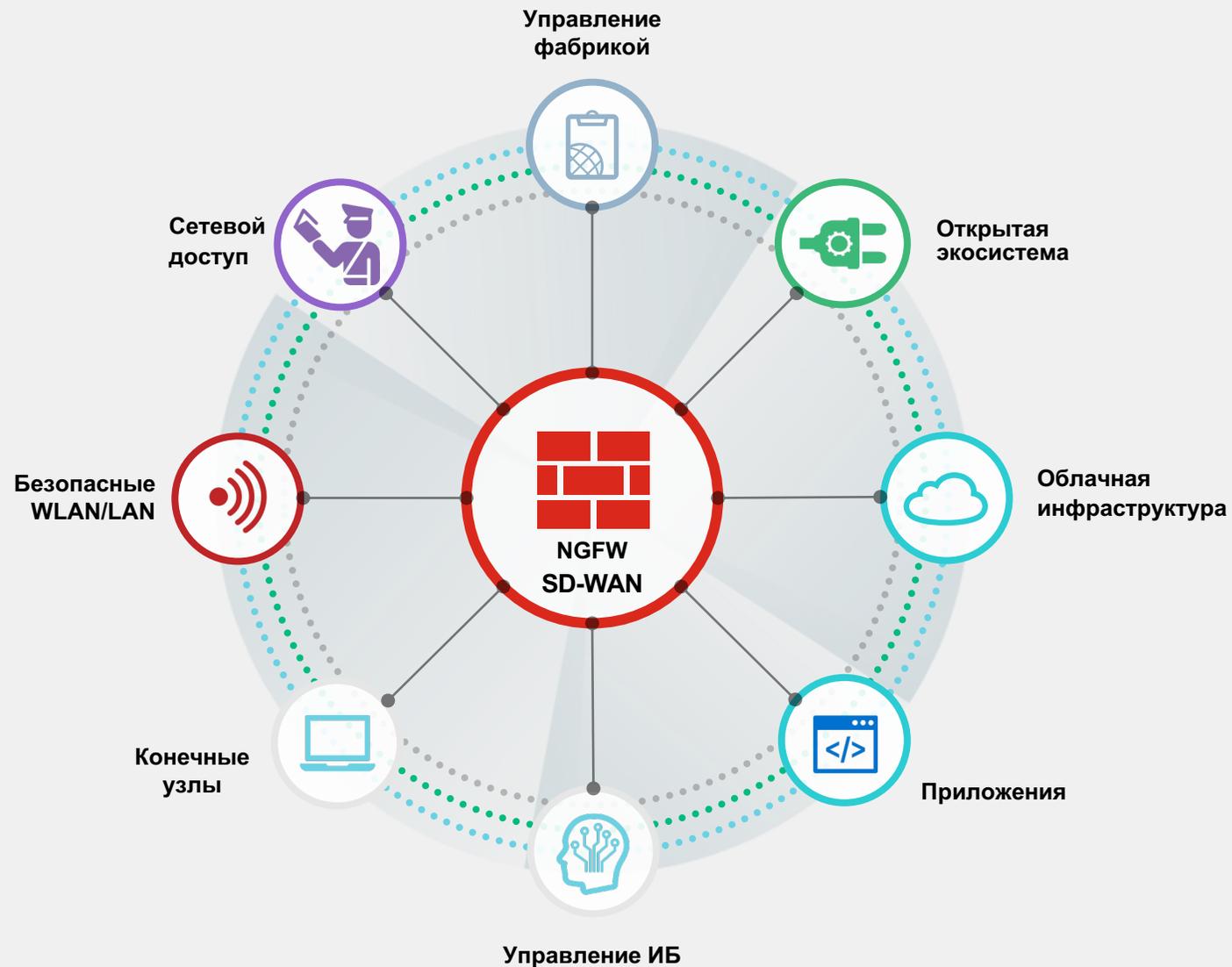
Обеспечение полной видимости поверхности цифровой атаки для лучшего управления рисками ИБ

Интегрированная

Уменьшение сложности сопровождения множества разнородных продуктов

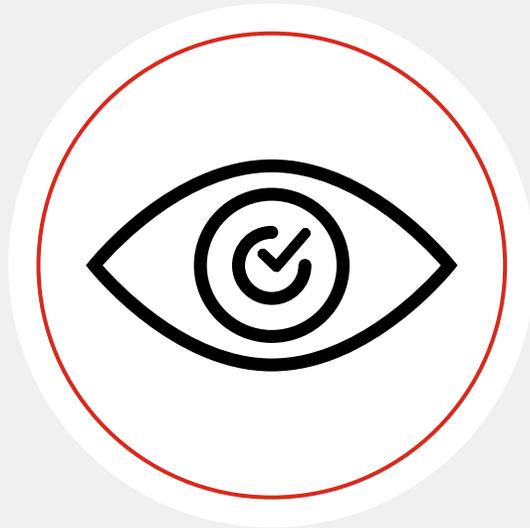
Автоматизированная

Увеличение скорости управления и отклика



FortiNAC в архитектуре доступа с нулевым доверием

Видимость



Определить и
оценить

Контроль



Сегментация и
«наименьший»
доступ

Реагирование



Обнаружение и
предотвращение

FortiNAC в архитектуре доступа с нулевым доверием

Видимость



Определить и
оценить

Agentless Multi-Vendor Discovery and Data Collection

- Идентифицирует и профилирует каждое устройство (в т.ч. IoT, пользователей и приложения)
- Взаимодействует с точками доступа, коммутаторами, маршрутизаторами, МСЭ, SIEM, IPS/IDS, а также с FortiGate в роли сенсора
- Использует API, CLI, RADIUS, SNMP, Syslog, MDM, DHCP, LDAP



FortiNAC в архитектуре доступа с нулевым доверием

Контроль



Сегментация и
«наименьший»
доступ

Сетевая микро-сегментация

- Сегментация на основе типов устройств
- Минимально необходимый уровень доступа для устройств помогает от east-west атак
- Поддержка сценариев безопасного подключения новых устройств к сети
- Оценка состояния устройств при подключении, в том числе удаленных vpn пользователей (без FortiClient)

Аутентификация и авторизация

- Применение параметров: роль, местоположение, время, тип устройства

FortiNAC в архитектуре доступа с нулевым доверием

Реагирование



Обнаружение и предотвращение

Инструмент NOC и SOC

- Динамическая оценка риска и автоматическое применение мер противодействия, в том числе для устройств сторонних производителей
- Быстрая автоматическая сортировка событий безопасности
- Ускорение расследования угроз и предотвращение **НОВЫХ**
- Возможность настройки действий

Интеграции в рамках Security Fabric

FortiAuthenticator



FortiEDR



FortiSIEM



FortiDeceptor



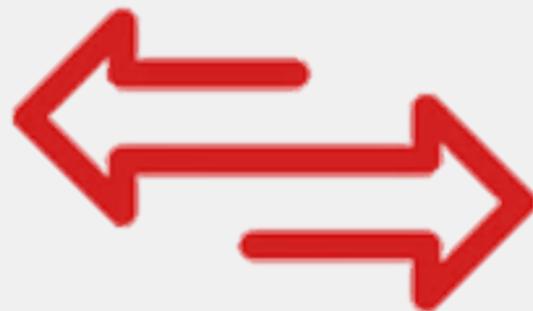
FortiAnalyzer



FortiClient EMS



FortiSandbox



FortiNAC



Сценарии применения NAC

- **Динамическое профилирование устройств**



- **Сдерживание угроз MAC Spoofing**



FortiNAC

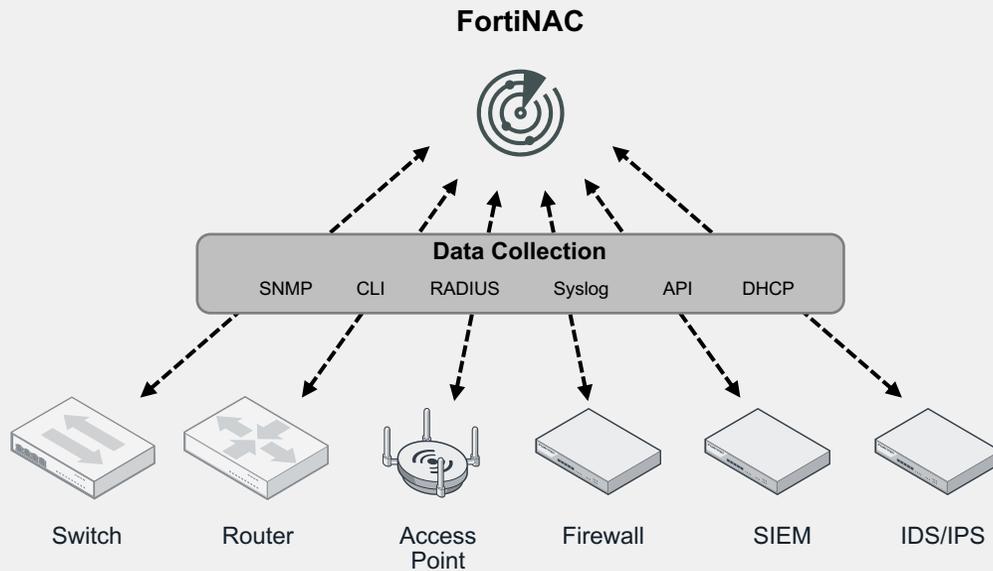
Идентификация и
динамический контроль



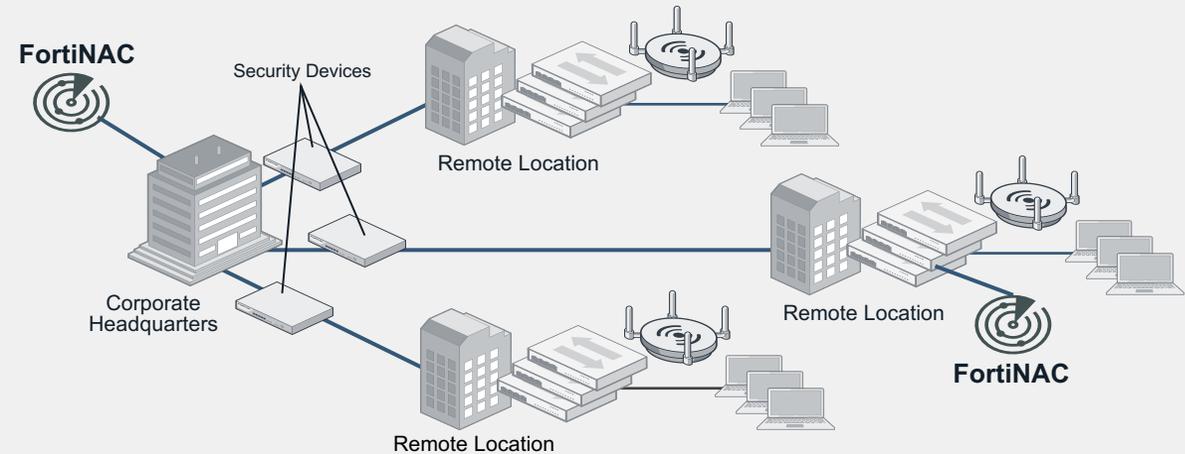
Как работает FortiNAC



FortiNAC – интеграция с инфраструктурой



Используются стандартные протоколы для сбора информации и интеграции с инфраструктурой доступа



FortiNAC поддерживает как централизованную, так и распределенную архитектуру



FortiNAC

Комплексная безопасность сети



Видимость

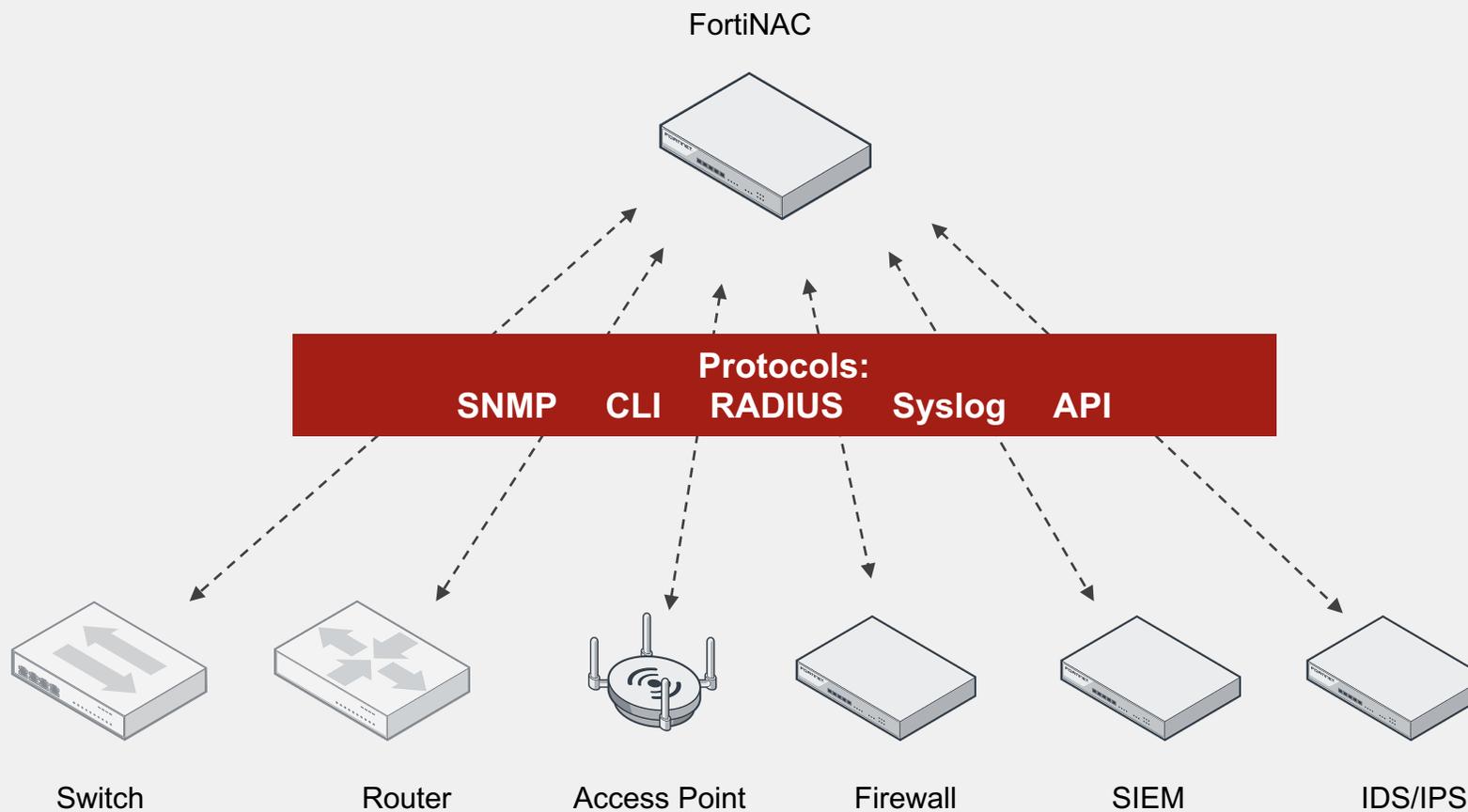
- Обнаружение всех конечных устройств, IoT устройств, пользователей, и приложений
 - Источниками могут быть RADIUS, CLI, SNMP, Syslog, MDM, DHCP, LDAP и т.д.
 - Поддержка работы более чем с 2,300 сетевыми устройствами
- Поддержка проводного и беспроводного оборудования различных вендоров
 - Возможность оперативного добавления поддержки для любого оборудования и вендора
- Идентификация и профилирование каждого подключенного устройства
 - Возможность создания различных правил и политик для каждого типа устройств
 - Расширяет возможности управления уязвимостями и исправлениями для пользователей даже без установленных Endpoint продуктов от Fortinet
 - Использует FortiGate для пассивной идентификации через изучение трафика от устройства
- Порталы для самостоятельной регистрации при подключении и упрощение управления гостевым доступом



Видимость



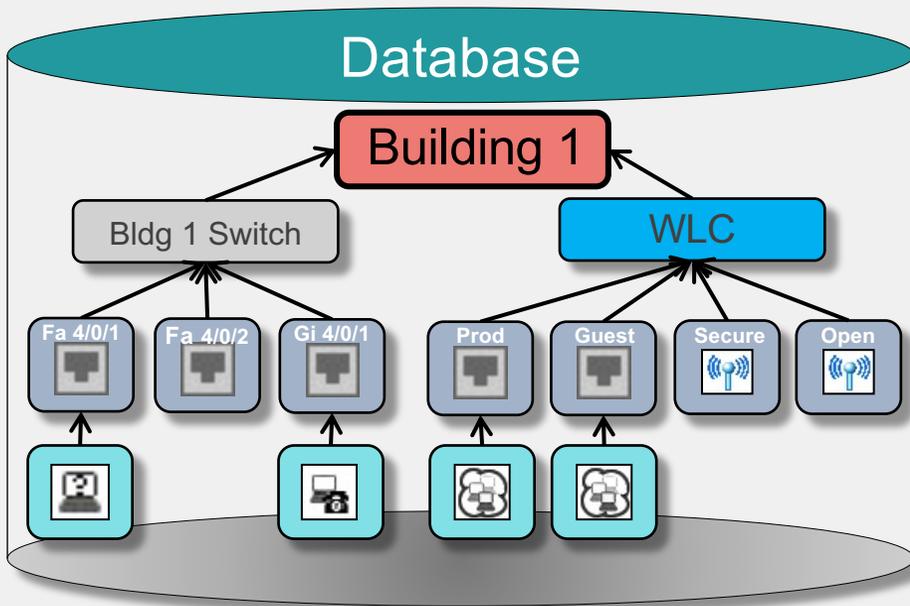
Сбор данных без использования агентов из различных источников



Видимость: как это работает

- Моделирование - это представление устройства и его соответствующей конфигурации в базе данных FortiNAC.
- Процесс моделирования выполняется путем настройки на FortiNAC IP адреса и учетных данных устройства инфраструктуры.

SNMP v2c



Add Device

Add to Container: Chicago

IP Address: 10.23.5.25

SNMP Settings

SNMP Protocol: SNMPv2c

Security String: Chicago-RW

CLI Settings

User Name: admin

Password: [masked]

Enable Password: [empty]

Protocol Type: SSH 2

Validate Credentials

OK Cancel

SNMP v3-AuthPriv

Add Device

Add to Container: Houston

IP Address: 10.29.5.21

SNMP Settings

SNMP Protocol: SNMPv3-AuthPriv

User Name: SamHouston

Authentication Protocol: SHA1

Authentication Password: [masked]

Privacy Protocol: AES-128

Privacy Password: [masked]

CLI Settings

User Name: admin

Password: [masked]

Enable Password: [empty]

Protocol Type: SSH 2

Validate Credentials

OK Cancel

Видимость: как это работает

- Собранная информация определяет тип устройства, количество портов и широкий спектр других атрибутов устройства.
- Модель содержит информацию о конечных устройствах и возможности управления

Status	Device	Label	Name
	Switch-2	F0/1	Switch-2 Fa0/1
	Switch-2	F0/2	Switch-2 Fa0/2
	Switch-2	F0/3	Switch-2 Fa0/3
	Switch-2	F0/4	Switch-2 Fa0/4
	Switch-2	F0/5	Switch-2 Fa0/5
	Switch-2	F0/6	Switch-2 Fa0/6
	Switch-2	F0/7	Switch-2 Fa0/7

Ports - Displayed: 24 Total: 24

<< first < prev 1 next > last >> 300

Ports | **Element** | System | Polling | Credentials | Model Configuration

Name: Switch-1.bradford-training.local

Type: Cisco Switch

IP Address: 192.168.102.11

Vendor: 1.3.6.1.4.1.9

Version: 2950.IOS.12.1

VLAN Switching Enabled

PA Optimization Enabled (VLAN Switching Optimization with Persistent Agent)

MAC Filtering Enabled

Role:

Description: Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6K2L2Q4-M),
Version 12.1(22)EA13, RELEASE SOFTWARE (fc2)

Note:

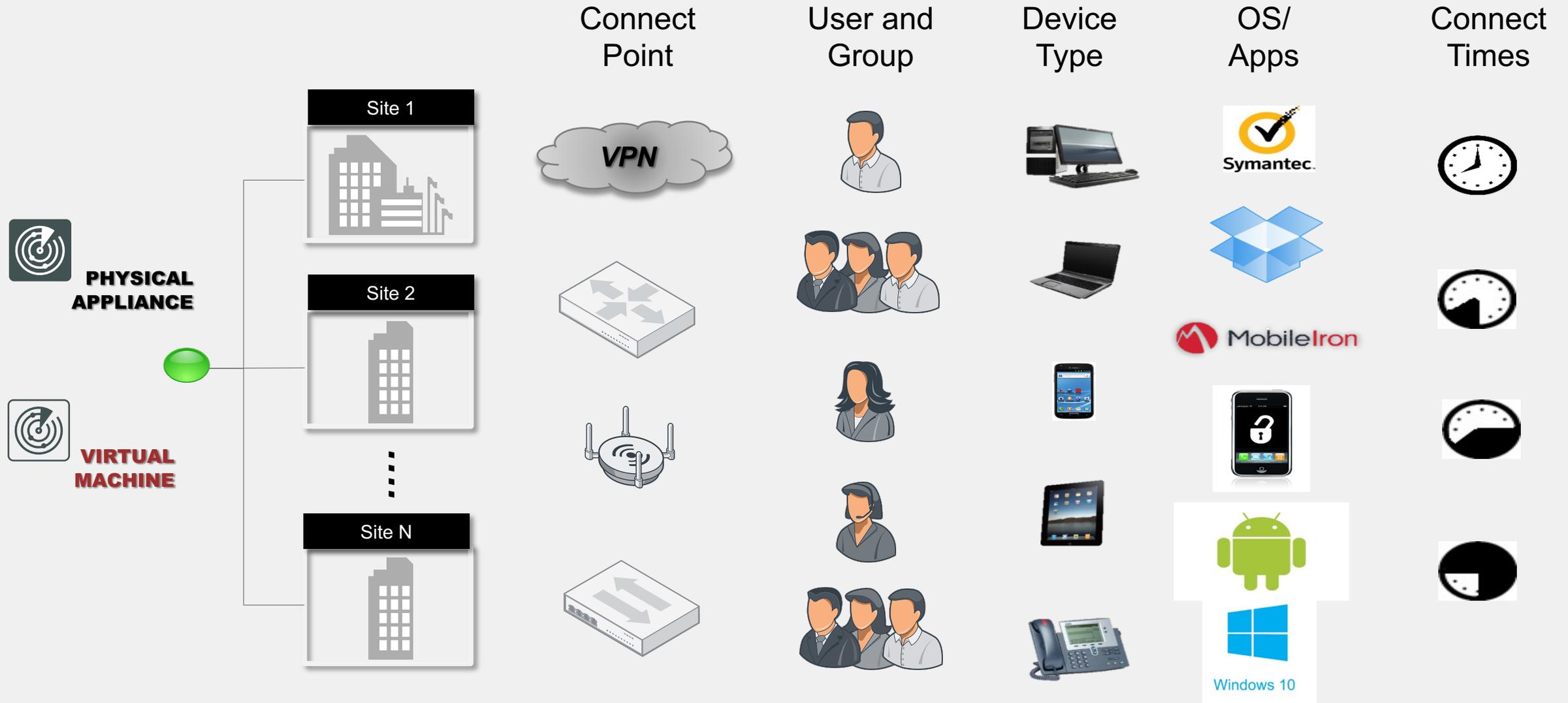
Advanced

Group Membership

Save

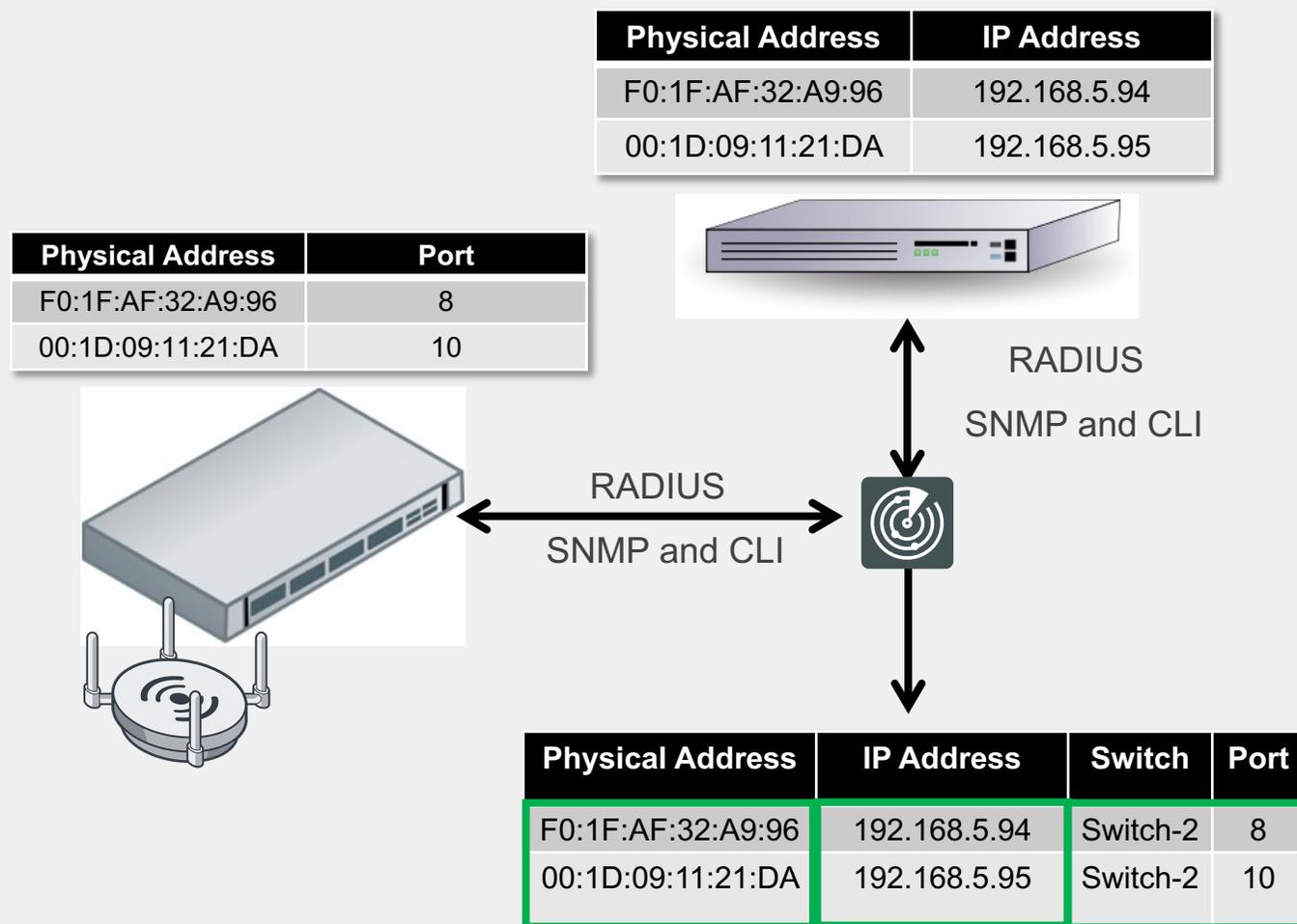


Сбор информации путем взаимодействия с инфраструктурой доступа



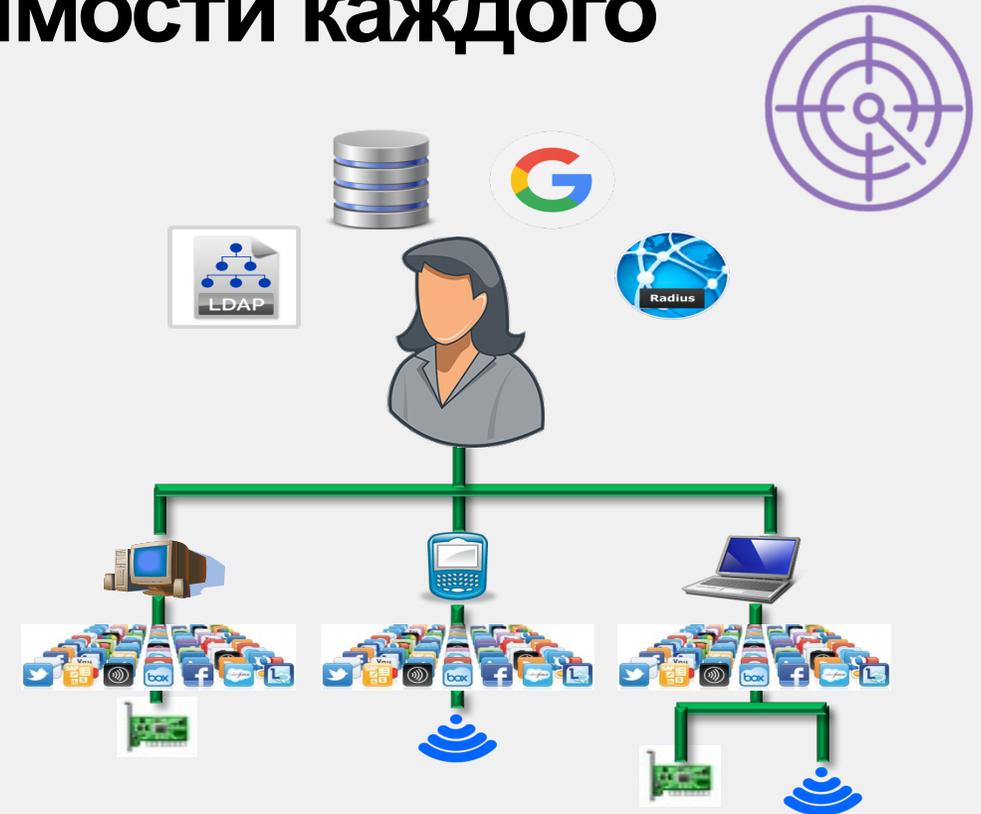
Получение сетевой видимости

- Данные собираются с помощью:
 - L2 polling (MAC to port), SNMP traps, RADIUS
 - L3 polling (IP to MAC)
- «ЧТО, ГДЕ, КОГДА»
 - Физический и IP адреса
 - Интерфейс или SSID
 - Подключено или не подключено



FortiNAC – обеспечение видимости каждого устройства

- Кто подключен – User
 - Current logged on user
 - BYOD, Guest, Contractor
- С какого устройства – Host/Device
 - Сетевой адаптер
 - MAC и IP адреса
 - Media Type
 - Производитель
 - Hostname
 - Операционная система
 - Приложения
- Где подключен - Location
- Когда подключен – Connection Times

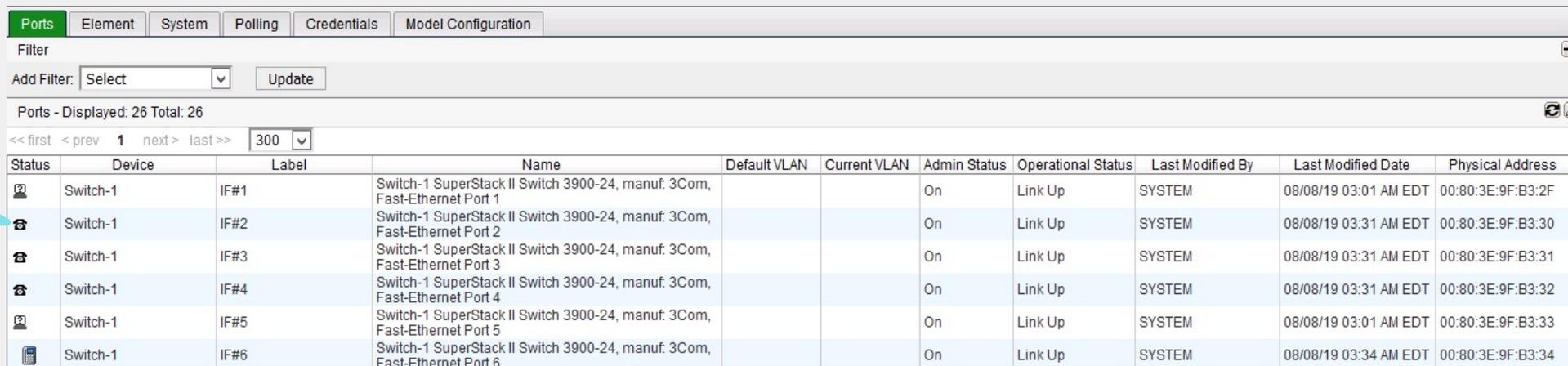


DEVICE ID	
IP Address:	192.168.5.95
Physical Address:	00:1D:09:11:21:DA
Vendor Name:	Dell Inc.
Status:	Disconnected
Location:	Concord AP Secure
Connect Time:	10/23/16 07:57 AM EDT
Disconnect Time:	10/23/16 04:55 PM EDT



Принцип работы

- Опрашивая сетевые устройства NAC имеет snapshot информации, где подключены конечные точки
- NAC проводит идентификацию и классификацию конечных устройств
- Отслеживает их состояние и регулярно обновляет информацию, имея актуальный перечень подключенных устройств



Connected Endpoints

Status	Device	Label	Name	Default VLAN	Current VLAN	Admin Status	Operational Status	Last Modified By	Last Modified Date	Physical Address
	Switch-1	IF#1	Switch-1 SuperStack II Switch 3900-24, manuf: 3Com, Fast-Ethernet Port 1			On	Link Up	SYSTEM	08/08/19 03:01 AM EDT	00:80:3E:9F:B3:2F
	Switch-1	IF#2	Switch-1 SuperStack II Switch 3900-24, manuf: 3Com, Fast-Ethernet Port 2			On	Link Up	SYSTEM	08/08/19 03:31 AM EDT	00:80:3E:9F:B3:30
	Switch-1	IF#3	Switch-1 SuperStack II Switch 3900-24, manuf: 3Com, Fast-Ethernet Port 3			On	Link Up	SYSTEM	08/08/19 03:31 AM EDT	00:80:3E:9F:B3:31
	Switch-1	IF#4	Switch-1 SuperStack II Switch 3900-24, manuf: 3Com, Fast-Ethernet Port 4			On	Link Up	SYSTEM	08/08/19 03:31 AM EDT	00:80:3E:9F:B3:32
	Switch-1	IF#5	Switch-1 SuperStack II Switch 3900-24, manuf: 3Com, Fast-Ethernet Port 5			On	Link Up	SYSTEM	08/08/19 03:01 AM EDT	00:80:3E:9F:B3:33
	Switch-1	IF#6	Switch-1 SuperStack II Switch 3900-24, manuf: 3Com, Fast-Ethernet Port 6			On	Link Up	SYSTEM	08/08/19 03:34 AM EDT	00:80:3E:9F:B3:34

Расширенная видимость

Идентификация устройств

The screenshot shows the configuration interface for a device profiling rule. It is divided into two tabs: 'General' and 'Methods'. The 'General' tab is active and contains the following settings:

- Enabled
- Name: Printer
- Description: Corporate Printer Profiling Rule
- Note: Automatically registers when detected, Notifies field tech support group
- Notify Sponsor
- Registration Settings:
 - Registration: Automatic Manual
 - Type: Printer
 - Role: Printer
 - Register as: Device in Host View
 - Add to Group: Printers
 - Access Availability: Always
- Rule Confirmation Settings:
 - Confirm Device Rule on Connect
 - Confirm Device Rule on Interval: 7 Days
 - Disable Device If Rule No Longer Matches Device

Профилирование устройств и регистрация

- Автоматическое и ручное профилирование
 - > Уведомление спонсоров
- Устройство Тип/Роль
- Подтверждение
 - В момент подключения
 - После подключения
 - Периодическое
- Отключить, если не получено подтверждение

20 Методов профилирования

- Чем больше методов= Тем выше доверие*
- Поддерживаются составные правила профилирования
- Использование устраняет зависимость от 802.1x
- Использование агентов, опционально

The screenshot shows the 'Methods' tab of the configuration interface. It contains a list of 20 methods for device profiling, each with a checkbox and a corresponding number in a red box:

- Active
- DHCP Fingerprinting
- FortiGate (8.6)
- FortiGuard (8.8)
- HTTP/HTTPS
- IP Range
- Location
- Network Traffic (8.6)
- ONVIF (8.7)
- Passive
- Persistent Agent
- Script (8.8)
- SNMP
- SSH
- TCP
- Telnet
- UDP
- Vendor OUI
- WinRM (8.5)
- WMI Profile



Видимость устройств: метод WMI

Status	Host Name	Registered To	Logged On User	Host Role	Operating System	Persistent Agent	Agent Version	Serial Number	Hardware Type	System UUID	Asset Tag	Host Created
	harpichord			NAC-Default	Microsoft Windows 10 Pro 10.0.17134 1803			6R4ZJS1	Dell Inc. OptiPlex 990 01	4c4c4544-0052-3410-805a-b6c04f4a5331		02/06/19 04:59 PM EST
<u>Status</u>	<u>IP Address</u>	<u>Physical Address</u>	<u>Media Type</u>	<u>Location</u>	<u>Actions</u>							
	10.12.12.16	D4:BE:D9:96:76:49	Wired									
		00:15:5D:30:80:D8	Wired									
	2k19test			NAC-Default	Microsoft Windows Server 2019 Standard 10.0.17763 1809			6857-0034-3603-2043-0550-9807-84	Microsoft Corporation Virtual Machine Hyper-V UEFI Release v3.0	594ff3dc-b2fd-488d-b0b8-3f66931cbd87	6857-0034-3603-2043-0550-9807-84	02/11/19 11:51 AM EST
<u>Status</u>	<u>IP Address</u>	<u>Physical Address</u>	<u>Media Type</u>	<u>Location</u>	<u>Actions</u>							
	10.12.12.23	00:15:5D:0A:B0:46	Wired									
	win81-test				Microsoft Windows 8.1 Pro N 6.3.9600			VMware-42 2c 63 2c fe 99 b7 b8-6a 01 47 3b 41 2e f3 20	VMware, Inc. VMware Virtual Platform None	2c632c42-99fe-b8b7-6a01-473b412ef320	No Asset Tag	02/11/19 03:33 PM EST
<u>Status</u>	<u>IP Address</u>	<u>Physical Address</u>	<u>Media Type</u>	<u>Location</u>	<u>Actions</u>							
	10.12.12.18	00:50:56:AC:4D:B0	Wired									
W	tester-pc			NAC-Default	Microsoft Windows 7 Ultimate 6.1.7601			1403-5400-7839-3472-3725-9775-30	Microsoft Corporation Virtual Machine 7.0	17a29048-a6e4-483e-acca-2d0268040800	1403-5400-7839-3472-3725-9775-30	02/13/19 04:37 PM EST
<u>Status</u>	<u>IP Address</u>	<u>Physical Address</u>	<u>Media Type</u>	<u>Location</u>	<u>Actions</u>							
	10.12.12.27	00:15:5D:0A:B0:49	Wired									
		00:15:5D:0A:B0:24	Wired									



Правила профилирования устройств (Device Profiling Rules)

- Классифицирует неизвестные устройства при их подключении к сети

Настройки регистрации классифицируют устройства

The 'General' tab shows the following configuration:

- Enabled
- Name: Printer
- Description: Corporate Printer Profiling Rule
- Note: Automatically registers when detected, Notifies field tech support group
- Notify Sponsor
- Registration Settings:
 - Registration: Automatic Manual
 - Type: Printer
 - Role: Printer
 - Register as: Device in Host View
 - Add to Group: Printers
 - Access Availability: Always
- Rule Confirmation Settings:
 - Confirm Device Rule on Connect
 - Confirm Device Rule on Interval: 7 Days
 - Disable Device If Rule No Longer Matches Device

- Для получения точных результатов можно использовать различные методы идентификации.

Методы используются для идентификации подключаемых устройств

The 'Methods' tab shows the following configuration:

- Active
- DHCP Fingerprinting
- HTTP/HTTPS
- IP Range
- Location
- Passive
- Persistent Agent
- SNMP
- SSH
- TCP
- Telnet
- UDP
- Vendor OUI
- WinRM
- WMI Profile
- Network Traffic
- FortiGate

The 'Vendor OUI' method is selected, and the 'Vendor OUI' sub-tab is active. It shows a table of Vendor OUIs:

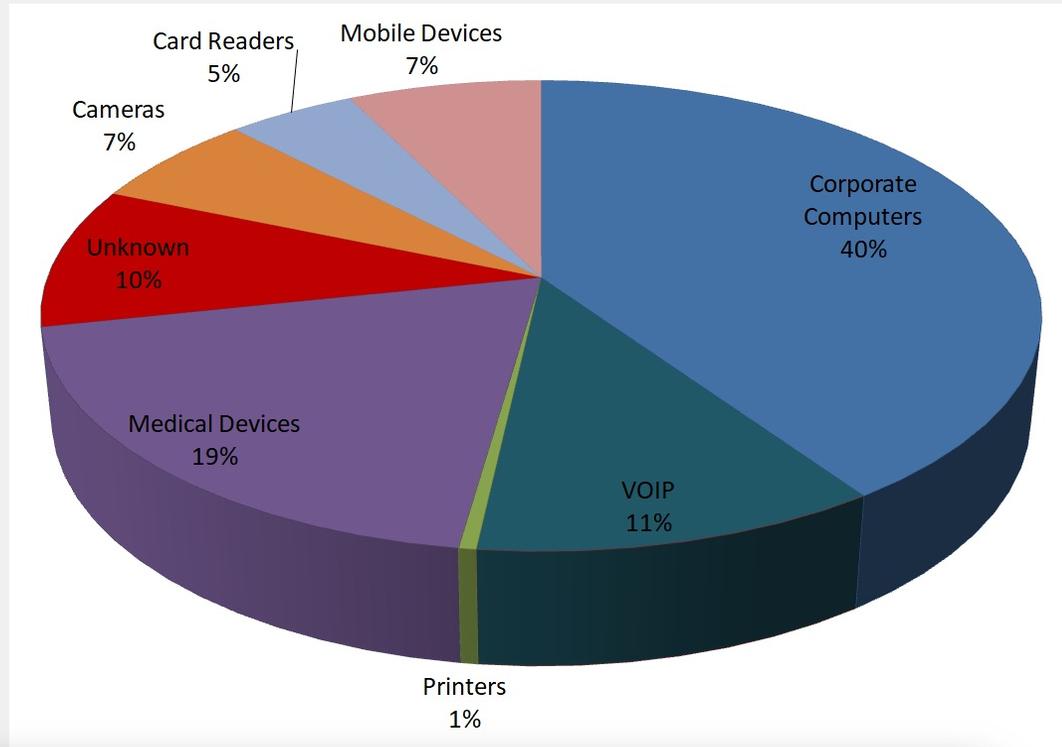
Field	Value
Vendor Name	XEROX CORPORATION
Vendor Name	KYOCERA CORPORATION
Vendor Name	HEWLETT PACKARD

Buttons: Add, Modify, Delete



Профилированные устройства

- Когда неклассифицированные устройства подключаются к сети, они оцениваются выбранными методами, используемыми в правилах профилирования устройств.



Profiled Devices - Displayed: 12 Total: 12

Enable: Rogue Evaluation Queue Size: 0

<< first < prev 1 next > last >> 200

Name	Rule Name	Type	Role	Location	Physical Address	Notes	Registered	Confirm Rule on Connect	Confirm Rule Interval
Johnson Controls, Inc.	Card Readers		NAC-Default	Switch-1 SuperStack II Switch 3900-24, manuf: 3Com, Fast-Ethernet Port 19	00:10:8D:08:9E:18	No	Yes	<input checked="" type="checkbox"/>	2 Days
Cisco 7942	Lab IP Phones		NAC-Default	Switch-1 SuperStack II Switch 3900-24, manuf: 3Com, Fast-Ethernet Port 18	00:13:19:CE:37:EA	No	Yes	<input checked="" type="checkbox"/>	1 Days
Johnson Controls, Inc.	Card Readers		NAC-Default	Switch-1 SuperStack II Switch 3900-24, manuf: 3Com, Fast-Ethernet Port 13	00:10:8D:69:41:A4	No	Yes	<input checked="" type="checkbox"/>	2 Days
Cisco 7942	Lab IP Phones		NAC-Default	Switch-1 SuperStack II Switch 3900-24, manuf: 3Com, Fast-Ethernet Port 13	00:03:E3:69:47:CF	No	Yes	<input checked="" type="checkbox"/>	1 Days
Cisco 7942	Lab IP Phones		NAC-Default	Switch-1 SuperStack II Switch 3900-24, manuf: 3Com, Fast-Ethernet Port 13	00:03:E3:69:48:42	No	Yes	<input checked="" type="checkbox"/>	1 Days
Intel Corporation	IP Cameras		NAC-Default	Switch-1 SuperStack II Switch 3900-24, manuf: 3Com, Fast-Ethernet Port 13	00:03:47:D8:EE:C1	No	Yes	<input checked="" type="checkbox"/>	None



Интеграция с системами MDM

Modify MDM Service

MDM Vendor: Fortinet EMS

Name: FortiNAC EMS Server Integration

Request URL: https://fortinac-ems

User ID: jhilfiker

Password: jhi03825! Hide

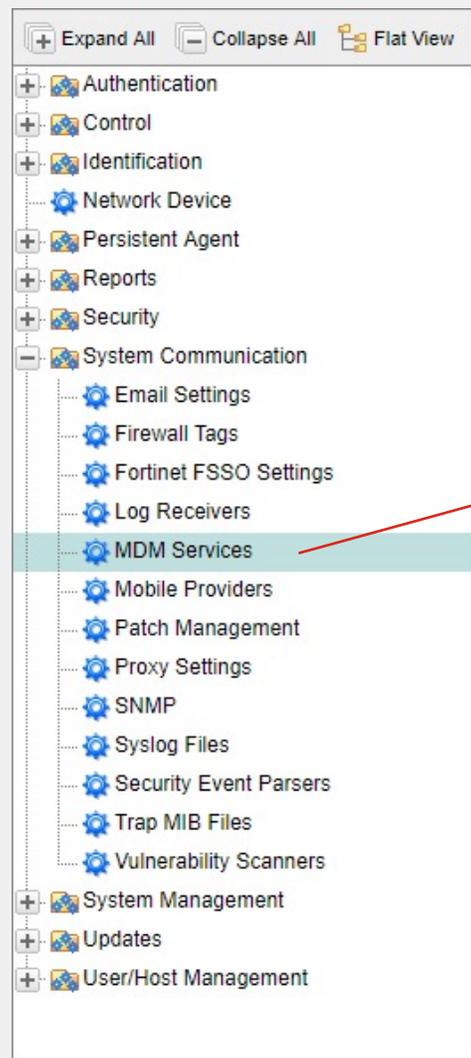
Enable On Demand Registration
 Revalidate Health Status on Connect

Remove Hosts Deleted from MDM Server

Enable Application Updating

Enable Automatic Registration Polling 1 Hours

OK Cancel



Add MDM Service

MDM Vendor: Microsoft InTune

Name: Air Watch

Request URL: Fortinet EMS

User ID: Google GSuite

Password: MaaS360

Identifier: Microsoft InTune

Enable On Demand Registration
 Revalidate Health Status on Connect

Remove Hosts Deleted from MDM Server

Enable Application Updating

Enable Automatic Registration Polling 1 Hours

Show

v8.6



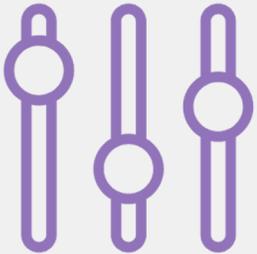
FortiNAC

Контроль



FortiNAC

Комплексная безопасность сети

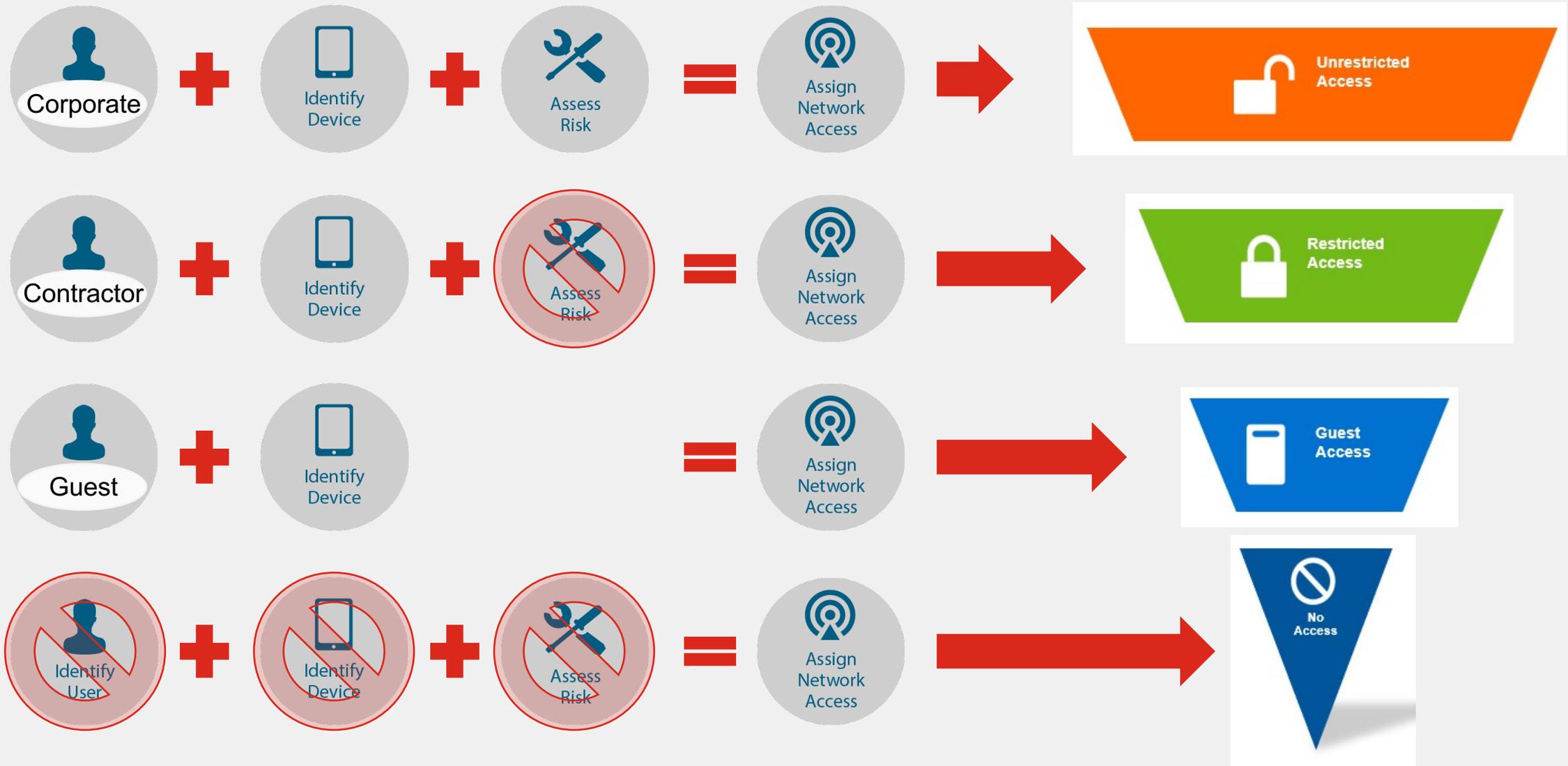


Контроль

- Автоматическая аутентификация и авторизация
 - Профилирование пользователей и устройств обеспечивает автоматический вход в сеть без угрозы для компании
 - Возможность использования для принятия решений о подключении информации о роли, местоположении, времени суток, метрик устройства и т.д.
- Динамическое управление и контроль доступа к сети
 - Настройте доступ устройства к сетевым ресурсам на основе изменений в активности или профиле
- Микросегментация сети
 - Идентификация устройств и пользователей позволяет определять гранулированно доступ только к нужным ресурсам (FSSO)
 - Устройства имеют ограниченный доступ для предотвращения заражения и изоляции в случае необходимости. Доступ может динамически меняться при изменении состояния устройства



Контроль и сегментация доступа



Первое подключение BYOD устройств

Портал с
возможностью
кастомизации

- Устройства BYOD могут быть подключены к сети владельцем устройства через Captive портал.
- Неизвестные устройства BYOD, которые подключаются к сети, будут изолированы в процессе подключения и направлены на портал
- Конечный пользователь может подключить устройство к сети, указав учетные данные при соблюдении всех настроенных политик.
- После успешной регистрации устройства FortiNAC предоставит соответствующий доступ.

FortiNAC: Network Access Control

FORTINET

FORTINET SECURITY FABRIC

Network Access Control Registration

User Registration

Each user is required to verify that their BYOD Device will meet established End-Point Compliance Policies prior to connecting to the network.

You must already have a company Active Directory account in order to register.

- If you know your username and password fill out the form below and click the download button.
- If you do not know your username and password, contact the Help Desk.

When you have filled out the form, you may be prompted to download and run a security scan to verify that your PC will meet these policies. The process will take approximately one to two minutes. Do not interrupt this process while it is running.

Enter your username and password. Then click the Continue button.

[Instructions](#)

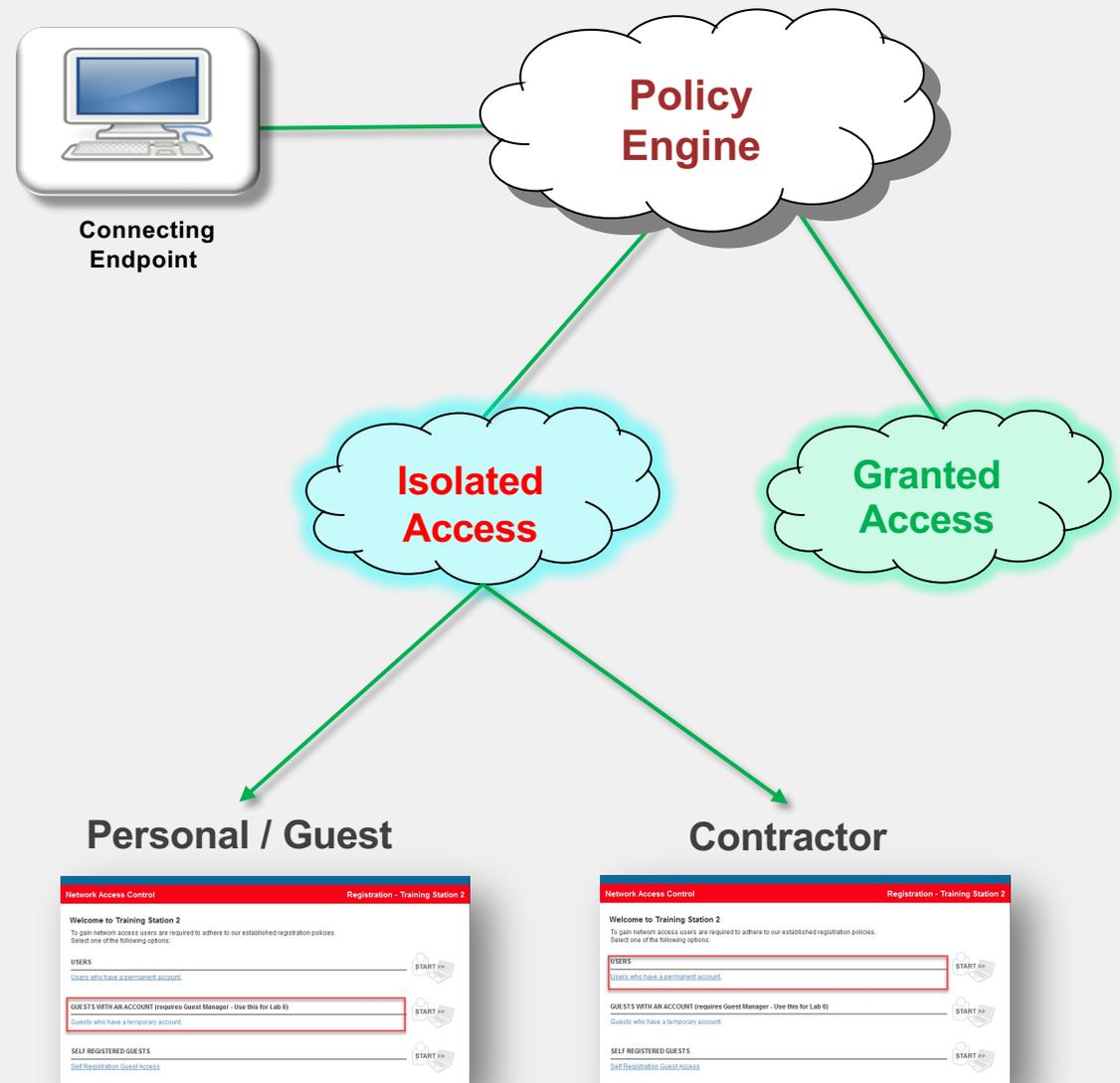
Username

Password



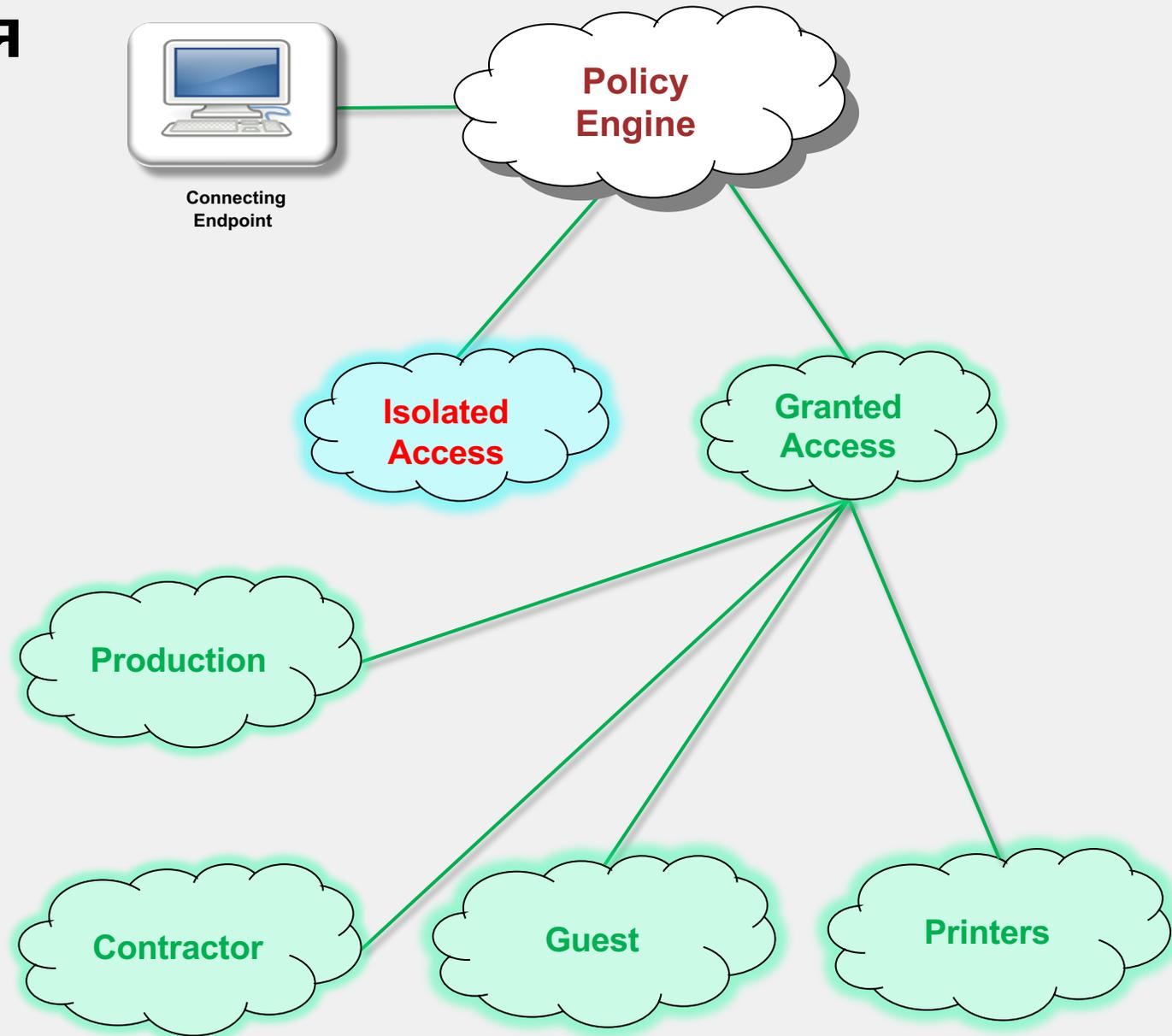
Оценка хоста до подключения и первое подключение к сети

- Изоляция устройств
 - Неизвестные устройства могут быть изолированы
 - Устройства, не прошедшие проверку на соответствие политикам, могут быть изолированы
 - Устройства могут быть изолированы администратором
- Первое подключение (Onboarding)
 - Аутентификация пользователя
 - Оценка состояния (Posture evaluation)
 - Кастомизируемый портал



Оценка после подключения

- FortiNAC policy engine постоянно оценивает хосты
- Политики безопасности:
 - Использует информацию о том, кто, что, где и когда, чтобы динамически предоставлять соответствующий доступ
 - Проверяет состояние безопасности конечной точки и при необходимости изолирует



Профили

- Подключенные и подключающиеся хосты постоянно проверяются на соответствие профилям пользователя / хоста:
 - Где
 - Кто
 - Что
 - Когда
- Профили пользователей / хостов являются компонентами политик безопасности

Add Network Access Policy

Name: Contractor Access - Wired

User/Host Profile: Contractor Production - Wired

Network Access Configuration: Contractor Production - Wired VLAN

Note: Provisions all contractors to the appropriate VLAN when they connect via a wired interface

OK Cancel

Name: Contractor Production - Wired

Where (Location): Chicago Wired Ports

Who/What by Group: Any

Who/What by Attribute: Host [Role: Contractor]

When: Specify Time Edit Time
M,Tu,W,Th,F 8:00 AM - 6:00 PM

Note: Contractor access on wired ports in Chicago facility. Allows access weekdays 8am-6pm only.

Select... Select... Add Modify Delete

Настройка Security Policy: Logical Networks

- Профили пользователей / хостов и конфигурации политик объединяются для создания политик безопасности

Add Network Access Configuration

Name: Printers - Wired - Logical Configuration

Logical Network Direct Configuration

Printers

Note:

OK Cancel

Selected Logical Network

Add Network Access Policy

Enabled

Name: Printers using logical configuration

User/Host Profile: Printers - Wired - Use Logical

Network Access Configuration: Printers - Wired - Logical Configuration

Note: Leverages the logical networks defined at specific locations

OK Cancel

Configuration Type



Logical Networks

- Логическая сегментация сети для политик доступа
- Централизованные конфигурации устройств
- Значения доступа к сети для конкретных устройств в каждой логической сети
- Связывает конфигурацию с устройством (ами)

Logical networks это уровень абстракции между именем, созданным пользователем, и определенным значением доступа.

Logical Network: **Guest**

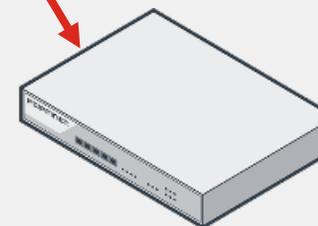
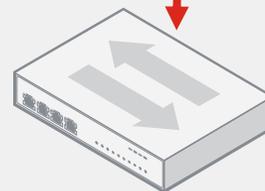
Access Configuration

Access Configuration

Access Configuration

Access Configuration

Каждая logical network может быть определена для каждого устройства



FortiNAC

Автоматизированная
ответная реакция



FortiNAC

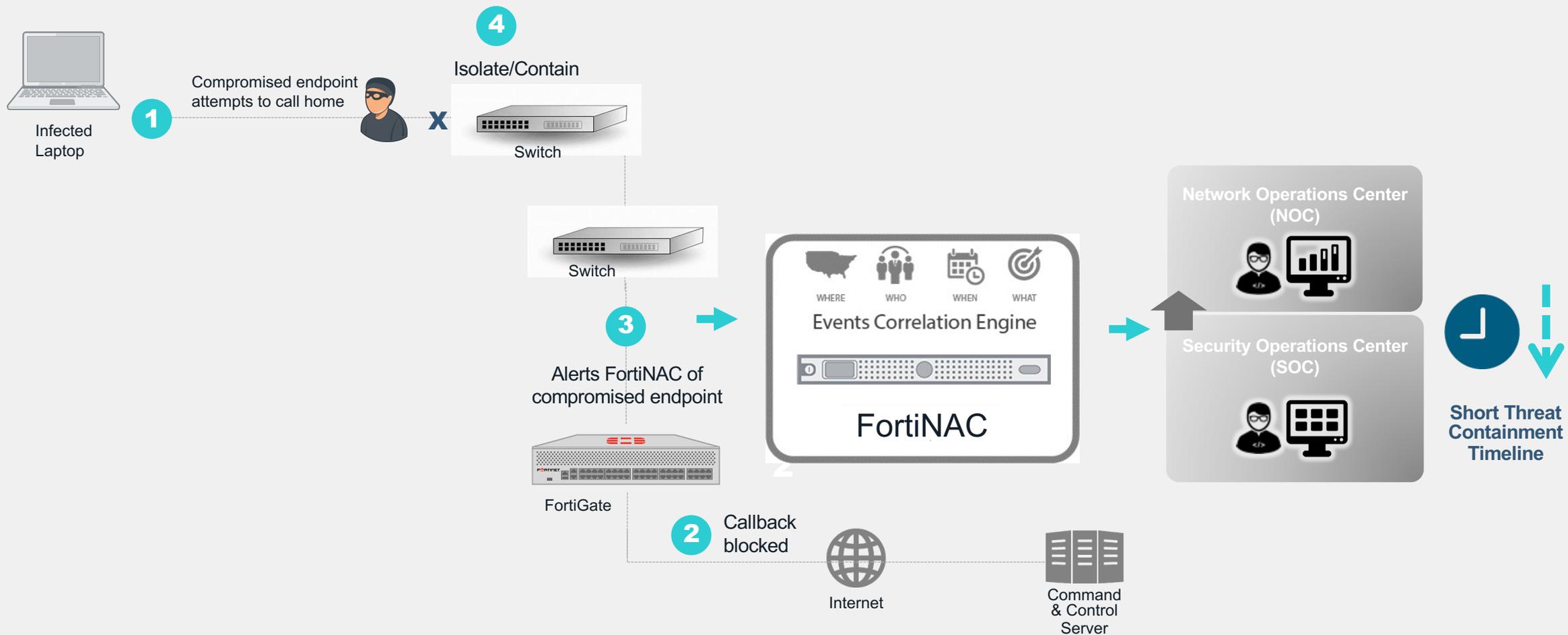
Комплексная безопасность сети



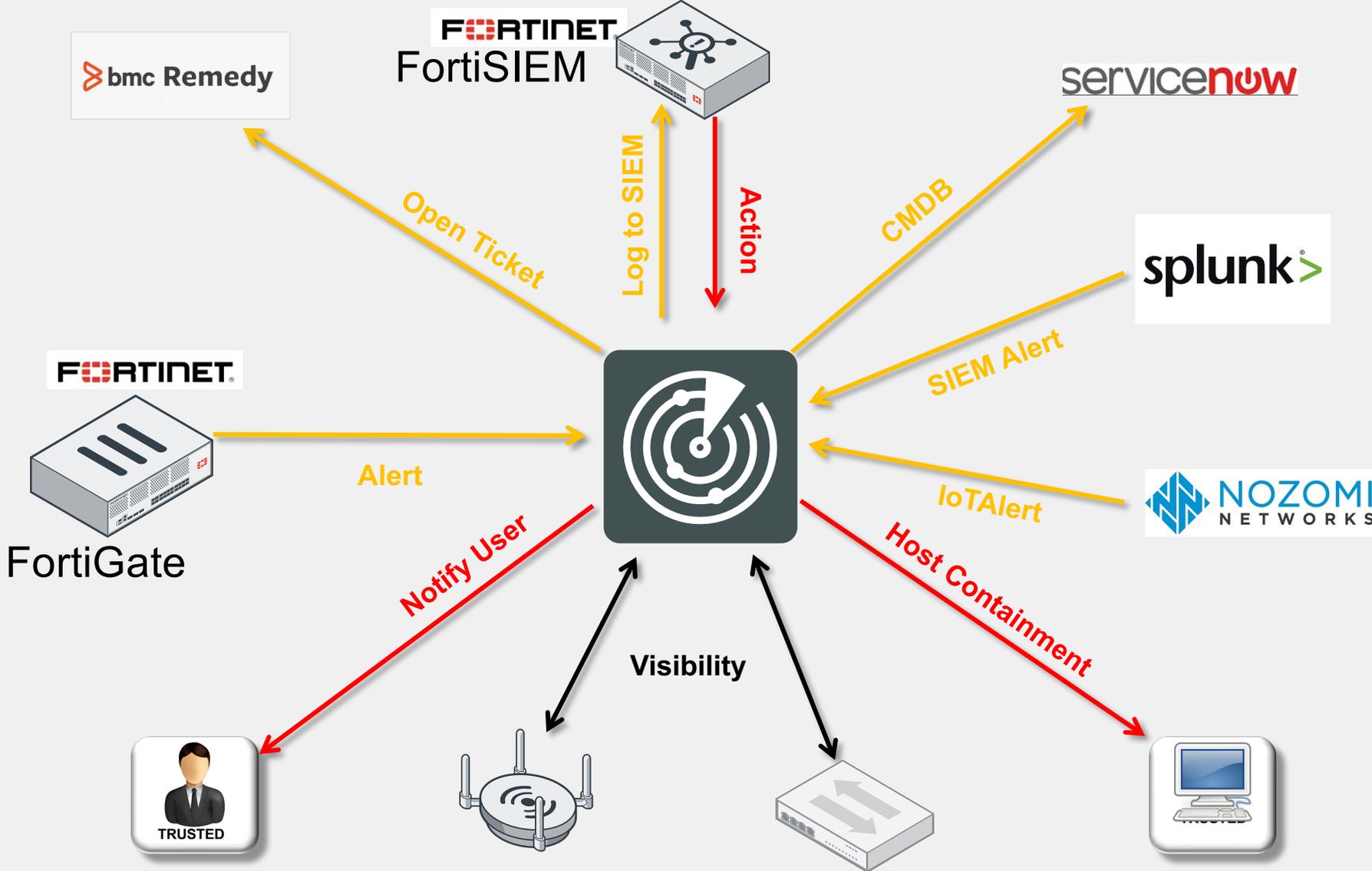
Автоматическая обратная реакция

- FortiNAC является шиной между SOC и NOC
 - Переход от обнаружения к автоматической обратной реакции на инциденты безопасности
- Быстрая автоматическая сортировка событий безопасности
 - Правила автоматизации могут в считанные секунды реагировать на изменения профиля
 - Выявление аномалий в относительно заданной модели поведения, общения
- Ускорение расследования угроз и предотвращение угроз
 - История поведения и данных об устройстве, собранная из нескольких источников, доступна сразу
- Возможность задания произвольной реакции
 - Простейшие примеры: карантин или доступ только к Интернет

Автоматизированная ответная реакция



Автоматизация и связь с другими решениями





Лицензирование

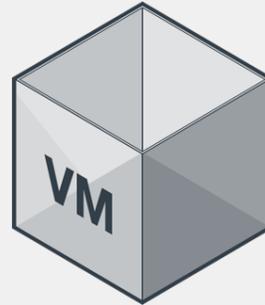


Варианты исполнения FortiNAC



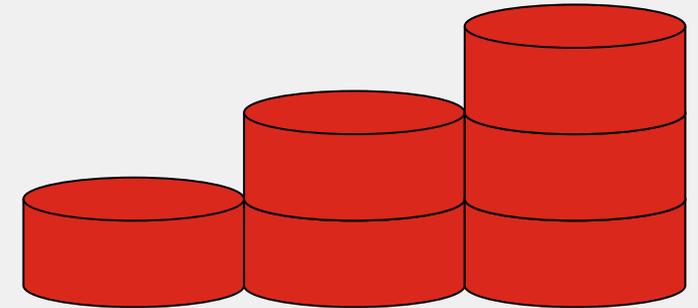
ПАК – программно-аппаратный комплекс

- 3 Control & Application Appliances
- Manager
- FAZ



Виртуальные машины

- Control / Application VM
- Manager VM
- FAZ Analytics VM



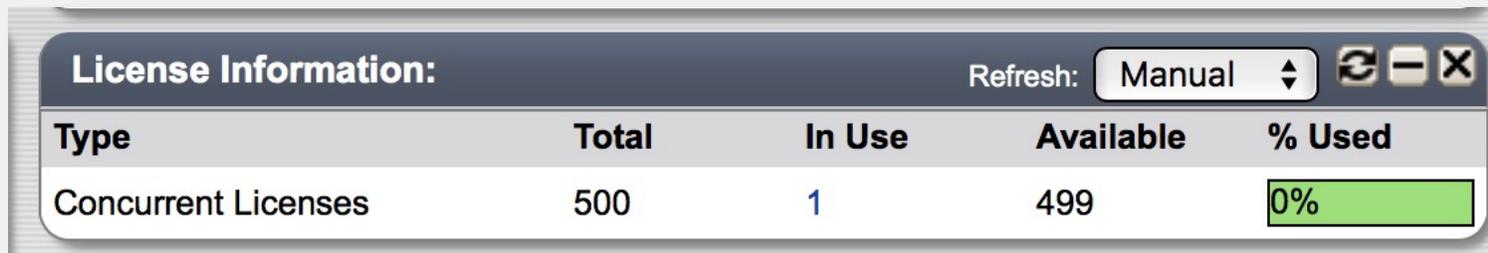
Уровни лицензирования

1. **Base**
 - Детектирование
2. **Plus**
 - Детектирование и контроль
3. **Pro**
 - Детектирование, контроль и реакция



FortiNAC лицензирование

- Лицензирование на основе количества **одновременно подключенных конечных точек**



Type	Total	In Use	Available	% Used
Concurrent Licenses	500	1	499	0%

- Лицензирование основано на **максимальном количестве одновременно подключенных проводных и беспроводных конечных устройств**, исключая инфраструктуру (коммутаторы, точки доступа, межсетевые экраны, маршрутизаторы).
- Вы можете иметь больше зарегистрированных устройств, чем лицензий, если они не подключены одновременно
- Лицензирование **не привязано к количеству портов!**
- Ноутбук может быть подключен как проводным (через док-станцию), так и беспроводным способом, что потребует 2 лицензии (если на ноутбуке не используется агент FNAC)
- Лицензирование на основе количества **одновременно подключенных конечных точек**
- Лицензии постоянные или по подписке



FortiNAC - уровни лицензирования

		FORTINAC LICENSE TYPES	BASE	PLUS	PRO	
Visibility	Network	Network Discovery	✓	✓	✓	
		Rogue Identification	✓	✓	✓	
		Device Profiling & Classification	✓	✓	✓	
	Endpoint	Enhanced Visibility	✓	✓	✓	
		Anomaly Detection	✓	✓	✓	
		MDM Integration	✓	✓	✓	
		Persistent Agent		✓	✓	
	User	Authentication		✓	✓	
		Captive Portal		✓	✓	
	Automation / Control		Network Access Policies	✓	✓	✓
			IoT Onboarding with Sponsor	✓	✓	✓
			Rogue Device Detection & Restriction	✓	✓	✓
		Firewall Segmentation	✓	✓	✓	
		MAC Address Bypass (MAB)	✓	✓	✓	
		Full RADIUS (EAP)		✓	✓	
		BYOD / Onboarding		✓	✓	
		Guest Management		✓	✓	
		Endpoint Compliance		✓	✓	
		Web & Firewall Single Sign-on		✓	✓	
		Event Correlation			✓	
Incident Response			Extensible Actions & Audit Trail			✓
		Alert Criticality & Routing			✓	
		Guided Triage Workflows			✓	
		Inbound Security Events			✓	
Integrations		Outbound Security Events		✓	✓	
		REST API	✓	✓	✓	
Reporting		Customizable Reports	✓	✓	✓	





FortiNAC

Сайзинг решения



Сайзинг



Сайзинг учитывает количество портов инфраструктуры доступа + количество пользователей БЛВС

Суммарно данное значение применяется при подборе аппаратного апплаинса или VM

Пример:

У Компании А имеется:

50 x коммутаторов на 24 порта

25 x коммутаторов на 48 портов

1 x контроллер БЛВС, (2.000 устройств БЛВС)

Итого $1.200 + 1.200 + 2.000 = 4.400$ портов

FNAC – small, до 2.000 портов

FNAC – medium, до 15.000 портов

FNAC – large, до 25.000 портов



Выбор аппаратного NAC



HARDWARE SERVER SIZING

		HARDWARE	
Hardware Server	Type	Target Environment	Capacity
FortiNAC-CA-500C	Standalone Appliance (Integrated Control Server and Application Server)	Small Environments	Manages up to 2,000 ports in the network*
FortiNAC-CA-600C	High Performance Control and Application Server	Medium Environments	Manages up to 15,000 ports in the network*
FortiNAC-CA-700C	Ultra High Performance Control and Application Server	Large Environments with few Persistent Agents	Manages up to 25,000 ports in the network*
FortiNAC-M-550C	Management Appliance (Provides centralized management when multiple appliances are deployed)	Multi-site environments with multiple appliances	Unlimited

* "Ports" in the network = total number of switch ports + maximum number of concurrent wireless connections. FortiNAC sizes the appliance capacity based on total port counts not total number of devices.

<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf>



Выбор NAC VM



VM SERVER RESOURCE SIZING

Network Size	Target Environment	SKU	vCPU**	Memory	Disk
Up to 2,000 ports in the network*	Small Environment	FNC-CA-VM	4	16 GB	100 GB
Up to 15,000 ports in the network*	Medium Environment	FNC-CA-VM	20	32 GB	100 GB
Up to 25,000 ports in the network*	Large Environment	FNC-CA-VM	36	96 GB	100 GB
Unlimited	Large Environment	FNC-M-VM	20	32 GB	100 GB

* "Ports" in the network = total number of switch ports + maximum number of concurrent wireless connections. FortiNAC sizes the appliance capacity based on total port counts not total number of devices.

** The values in the vCPU column are only guidelines. Individual environments may vary.

<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf>



FortiNAC: рекомендации по выбору модели

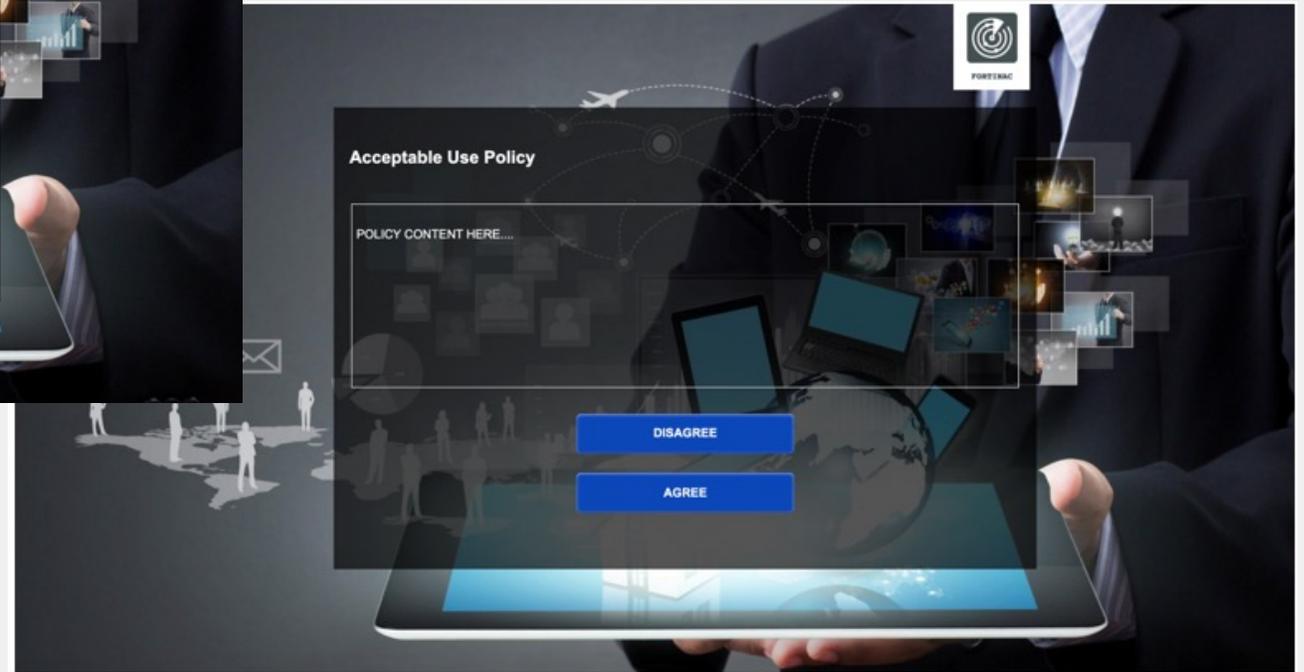
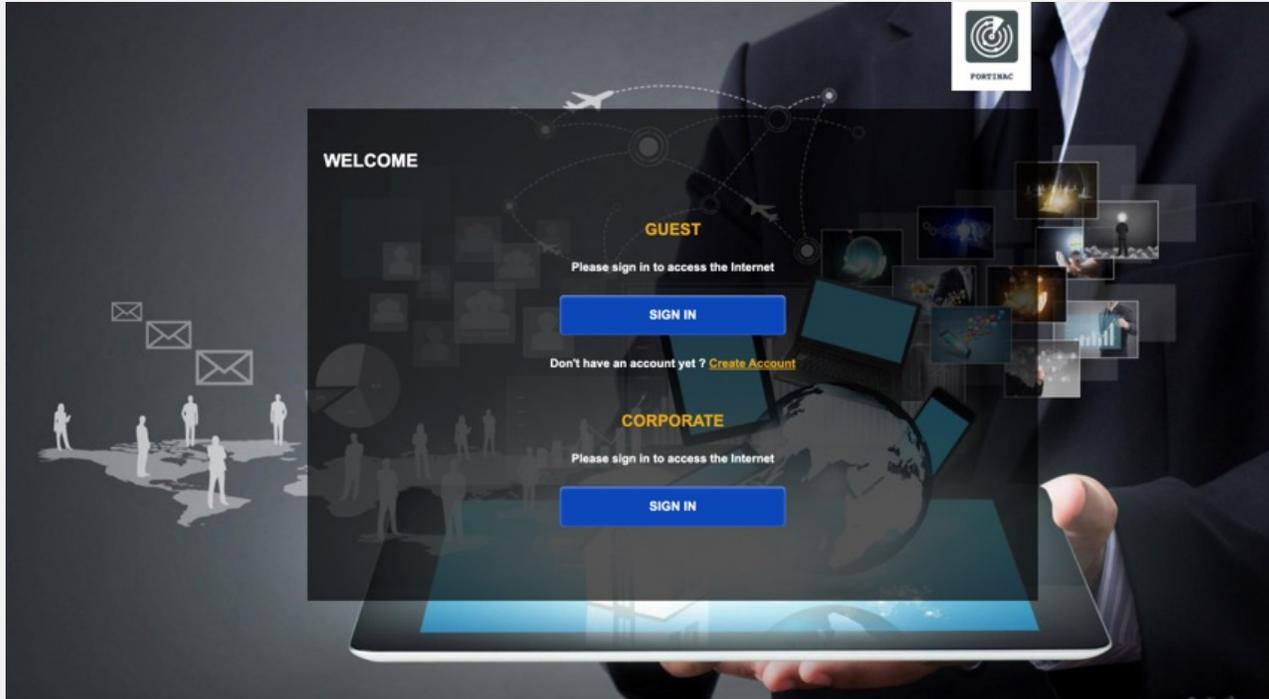


FNAC	Max ports	802.1X	Persistent Agent	При использовании 802.1x + Persistent Agent
FNAC CA 500	2.000	1.800	1.800	1.600
FNAC CA 600	15.000	13.500	13.500	12.000
FNAC CA 700	25.000	22.500	22.500	20.000
FNAC CA VM	25.000	22.500	22.500	20.000

- Масштабирование VM обеспечивается за счет добавления новых VM инстансов
- Рекомендуется закладывать все компоненты NAC и HA конфигурации



Веб-портал FortiNAC





FortiNAC

Истории успеха



История успеха - здравоохранение

Заказчик: Atrius Health

- 10,000 сотрудников
- 36 локаций в Новой Англии (регион на северо-востоке США)
- 740,000 пациентов
- Electronic Medical Record (EMR)

- Сложности: Видимость и контроль
- Просмотреть все устройства в каждом месте
- Защитите все порты и беспроводной доступ
- Соответствие HIPAA

- Вариант лицензирования FortiNAC: Plus
- Сеть построенная на сетевом оборудовании Cisco



История успеха – «умное» здание / IoT

Project: New smart building complex

- 6,000 устройств сотрудников
- 3,000 IoT устройств
 - Контроль окружающей среды
 - Безопасные лифты
 - 1,300 видео камер
 - Сетевое оборудование: Cisco, Arista

Сложности: Видимость и контроль

- Просмотреть все устройства в каждом месте
- Контролировать проводные и беспроводные подключения

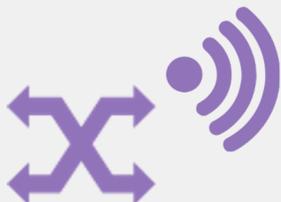


Ключевые преимущества платформы



Большой портфель решений дополняющих NAC (в части обнаружения, блокирования, провижинга, аутентификации, защиты и т.д.)

- Поддержка более чем 2,300 сетевых устройств инфраструктуры
- Двусторонний APIs для интеграции FortiNAC со сторонними решениями (150+ вендоров)
- Идентификация устройств за секунды



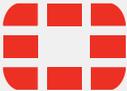
Поддержка проводной и беспроводной среды

- Работает не только с 802.1X для обнаружения или применения политик
- Непрерывная оценка состояния устройства, как для проводных, так и беспроводных устройств

Масштабируемая архитектура

- Архитектура не требует сетевого трафика, таким образом устраняется необходимость развертывания устройства (виртуального или физического) на каждом сайте при защите нескольких сайтов
- Может быть легко развернут поставщиками услуг и MSSP благодаря возможностям развертывания на виртуальной машине и в облаке.



F**RTINET**®