

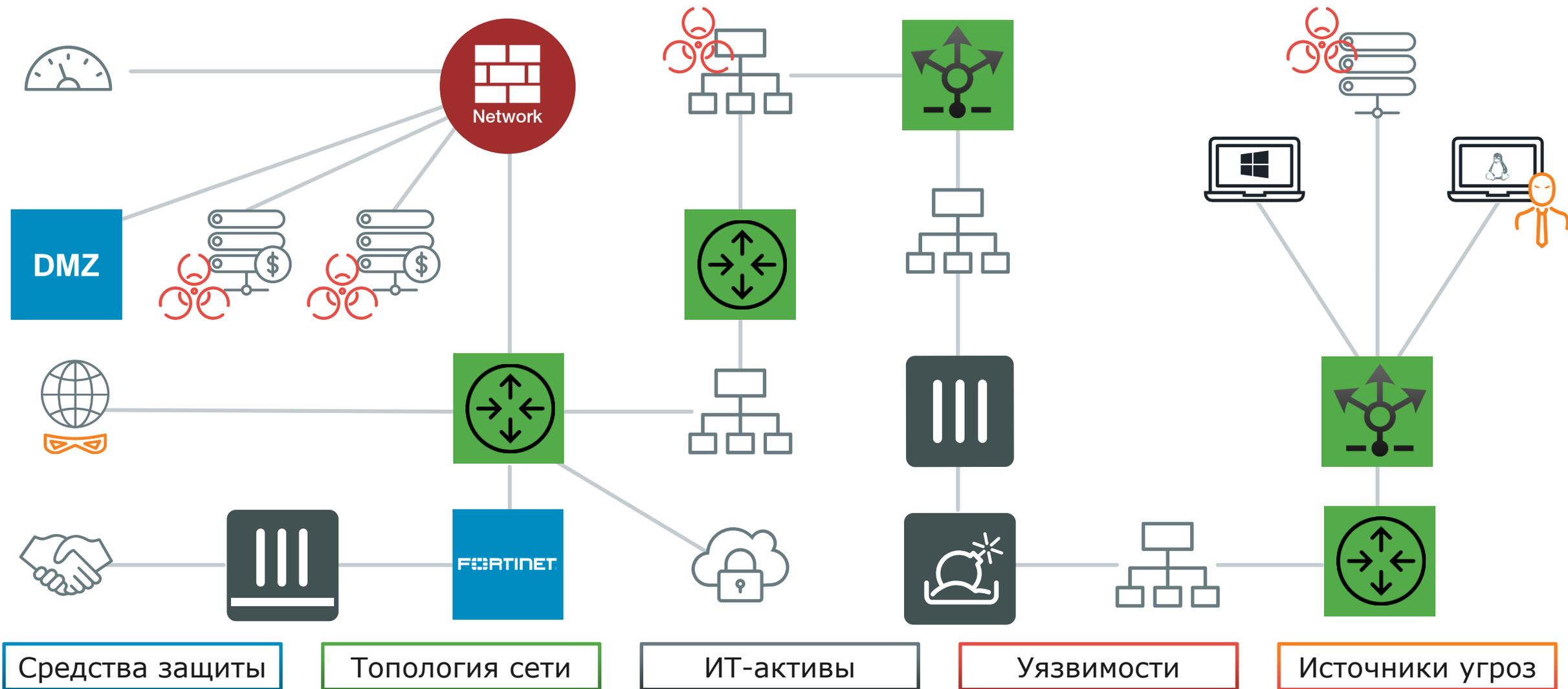
Адаптивная защита Fortinet Security Fabric на основе индикаторов угроз от Skybox Security

Юрий Черкас

20 сентября 2018

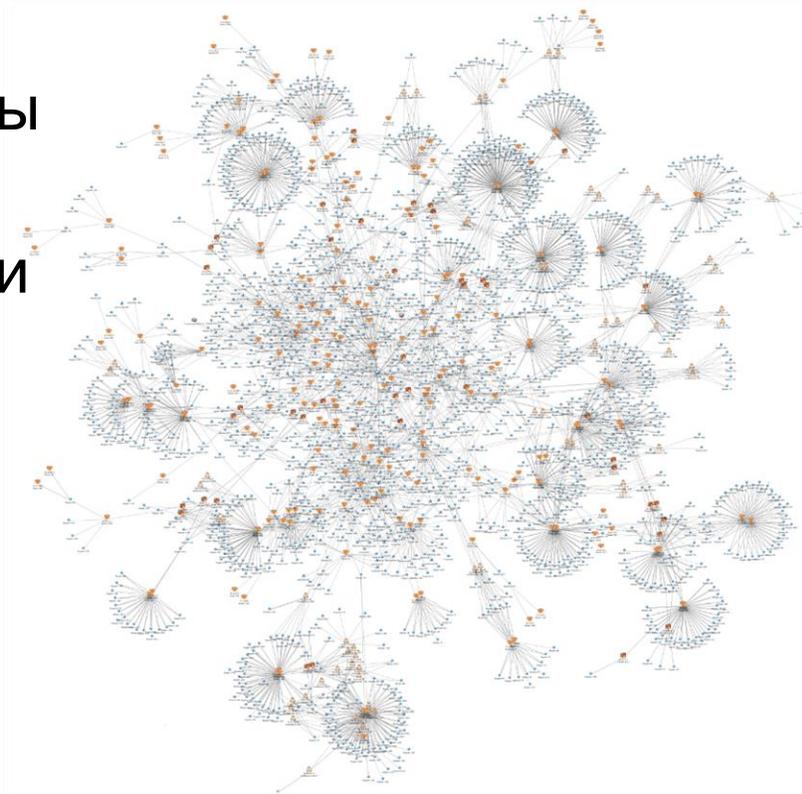
SECURITYDAY

Моделирование вектора атаки



Сложности

- Наша цель – защитить ИТ-активы, но:
 - » ИТ-инфраструктура динамически меняется и мы не знаем как выглядит наша сеть прямо сейчас
 - » Зачастую мы настраиваем защитные механизмы сети без учета уязвимостей на хостах
 - » Мы не знаем о новых уязвимостях в период до и между сканированиями
 - » Мы учитываем только критичные уязвимости
 - » Мы не всегда знаем какие уязвимости достижимы в нашей сети



Подход Skybox Security



Идея Skybox Security



Построение модели сети

Возможные сценарии

Построение сетевой модели



- Network Assurance – видимость сети

Интерактивная карта сети

Автоматическая проверка соответствия стандартам конфигурирования

Автоматическая проверка соответствия политикам сегментирования

Как Это Работает



1

Сбор и нормализация



2

Моделирование



3

Детальный анализ



Дружба с Fortinet

- Технологическое сотрудничество с 2010 года
- Skybox обязуется поддерживать новые версии Fortinet
- Взаимодействие на уровне разработчиков



Skybox Security and Fortinet Integration

Supported Products and Features

FortiGate: Support for versions FGT60B-3.8 and greater

FortiGate Supported Features:

Online:	Fully supported
SSH/Telnet:	Fully supported
SOAP:	Fully supported
Import:	Fully supported
Directory:	Fully supported
Basic:	Fully supported
OS info:	Fully supported
Interfaces:	Fully supported
Routing:	Fully supported
Dynamic routing:	Fully supported
Access:	Fully supported
NAT:	Fully supported
LB:	Fully supported
VRF:	Fully supported
PBR:	Fully supported
Layer 2:	Fully supported
VPN:	Fully supported
Users:	Fully supported
Virtual contexts:	Fully supported
IPS policy signatures:	Fully supported
Change tracking events:	Fully supported
Traffic logs:	Fully supported

FortiManager: Support for versions 5.0.6-build0310 140205 (GA) through 5.4.2

FortiManager Supported Features:

Information extraction via XML API (SOAP) and SSH

Since 2010 Skybox and Fortinet have had a well-established relationship and continue to upgrade and improve connectivity as each company's product line evolve. Fortinet and Skybox are actively involved in reciprocal Technical Alliance Programs.



Roadmap Discussions and Information Exchange Between Fortinet and Skybox

Besides being close neighbors in the Silicon Valley, Skybox and Fortinet have had a strong technology relationship since 2010 and are active participants in each other's [Technical Alliance Programs](#). There is continuous mutual support for product lines from both companies.

- Skybox is committed to providing support for all future versions. Fortinet is one of the top five leading firewall platforms
- Fortinet shares information via our mutual Technical Alliance relationship
- We have full access to the Fortinet Development Network (FNDN)
- We also have direct access to Fortinet development key engineering personnel, in case escalation is required
- Skybox assesses platform enhancement on an ongoing basis

Проверка конфигураций

- Загружаем конфигурации всех сетевых устройств
- Строим карту сети
- Анализируем корректность конфигураций на:
 - » Соответствие лучшим практикам
 - » Соответствие собственным политикам конфигурирования

The screenshot displays the 'Compliance' section of the Skybox Security Firewall & Network Assurance interface. The header shows 'SKYBOX SECURITY | Firewall & Network Assurance' and 'Compliance'. Below the header, there's a 'Configuration Policies' section with a view filter set to 'All Configuration Checks' and a 'Sort:' dropdown. A table lists various configuration checks under the '2.6 Fortinet FW Standard Policy (33)' category. Each row includes a check ID, severity, and a search path for the configuration.

Check	Check Details
2.6 Fortinet FW Standard Policy (33)	
2.6.17 Confirm Central Management Section Critical	Search in Entire Configuration for: ^config system central-management
2.6.20 Confirm System Logging Section Critical	Search in Entire Configuration for: ^config log syslogd setting
2.6.23 Confirm Fortianalyzer Section Critical	Search in Entire Configuration for: ^config log fortianalyzer setting
2.6.10 Existance of HA Configuration High	Search in Entire Configuration for: ^config system ha
2.6.14 HA Password Encrypted High	Search in HA Configuration block for: set password ENC \S+
2.6.16 HA Session Replication High	Search in HA Configuration block for: set session-pickup enable
2.6.19 Ensure CM FMG Setting High	Search in System Management block for: set fmg "\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}"
2.6.21 Ensure Logging Enabled High	Search in System Logging block for: set status enable
2.6.22 Ensure Logging Host High	Search in System Logging block for: set server "\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}"

Проверка доступа на лету

Analysis Results

Show: Accessible Destinations | Group By: Network | Authentication: N...

- developmentWindowsWS [192.170.17.0 / 24] [256 IPs; 1 TCP port]
- developmentUnixWS [192.170.18.0 / 24] [256 IPs; 1 TCP port]
 - 192.170.18.0-192.170.18.255 [256 IPs; 1 TCP port]
- 21 (TCP)
- developmentServers [192.170.19.0 / 24] [256 IPs; 1 TCP port]
- dmz [192.170.33.0 / 24] [256 IPs; 6 TCP/UDP ports]

Routes | **View** | **Current Map**

Show Routing Rules

Access Route
From Internet (cloud) To developmentUnixWS (192.170.18.0/24)

#	Step	Inbound	Access Rule
	Source:		
	Internet (cloud)		
	Source IP range(s): 16.0.0.0-16.0.0.0, 16.0.0.2-16.255.255.255		
	Sending To IP range(s): 192.170.18.0-192.170.18.255		
	Sending to service(s): 21/TCP		
1.	main_FW (16.0.0.1)		(ACC) - All
2.	Main Router (192.169.1.2)		
3.	Internal Router (192.170.8.2)		
4.	dev FW (192.170.1.1)		(ACC) - All

Проверяем наличие доступа в 2 клика

Проверка доступа на лету

Analysis Results

Show: Blocked Destinations Group By: Network

developmentWindowsWS [192.170.17.0 / 24] [256 IPs; Any protocol]
192.170.17.0-192.170.17.255 [256 IPs; Any protocol]
Any Internet Protocol

Routes: 1 << < > >> 4 View: [Icons]

Current Map: Organizati... Show Route Map

Detail Level: Display all blocking rules

Access Route
From Internet (cloud) To developmentWindowsWS (192.170.17.0/24)
(maximal number of routes (4) is reached)

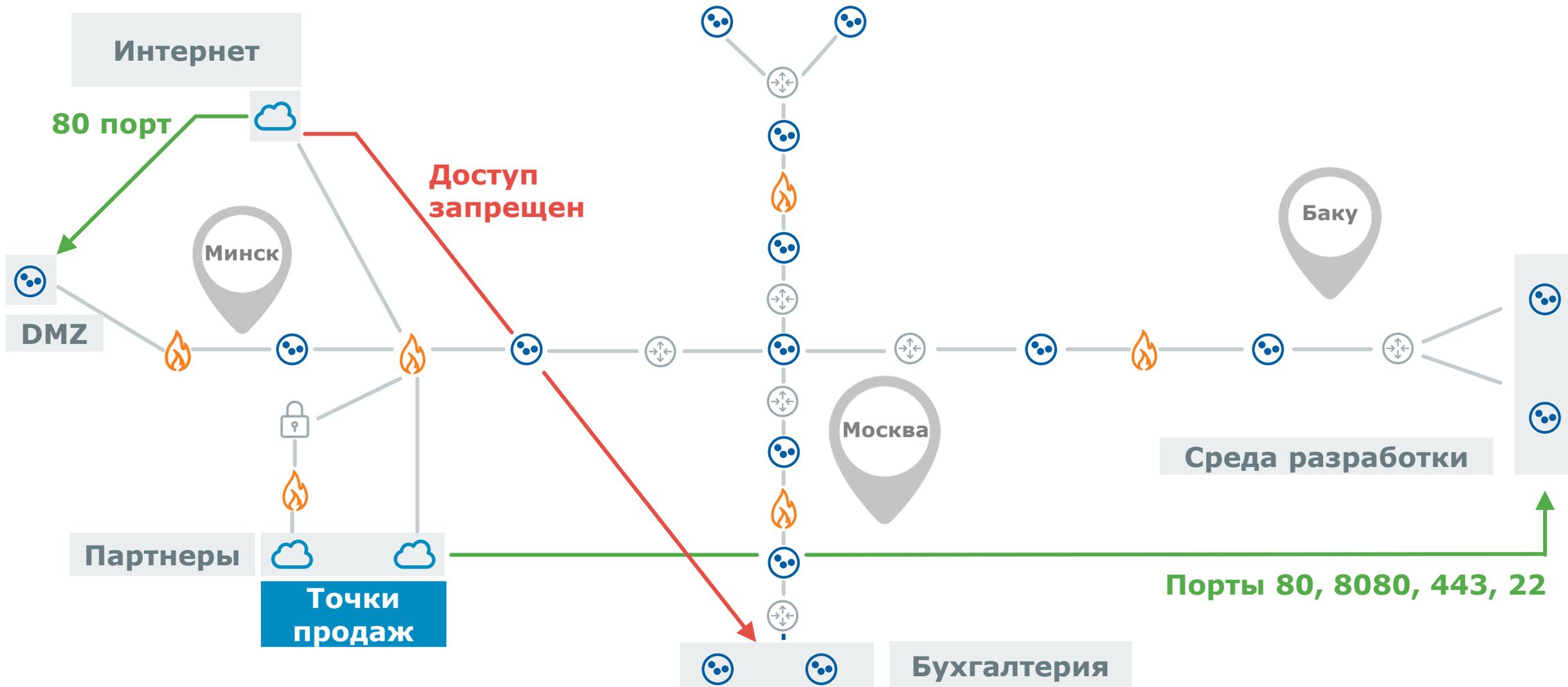
#	Step	In	Ac	Rt
1.	main_FW (16.0.0.1)			
2.	Main Router (192.169.1.2)			
3.	Internal Router (192.170.8.2)			
4.	dev FW (192.170.1.1)			

Source:
Internet (cloud)
Source IP range(s): 200.160.3.1-200.160.3.1
Sending To IP range(s): 192.170.17.0-192.170.17.255
Sending to service(s): 0-255/ICMP, 0-255/IGMP, 0/CGP, 0/PIIP, 0/ST, 1-20/TCP, 22-36/TCP, 38-78/TCP, 80-65535/TCP, ...

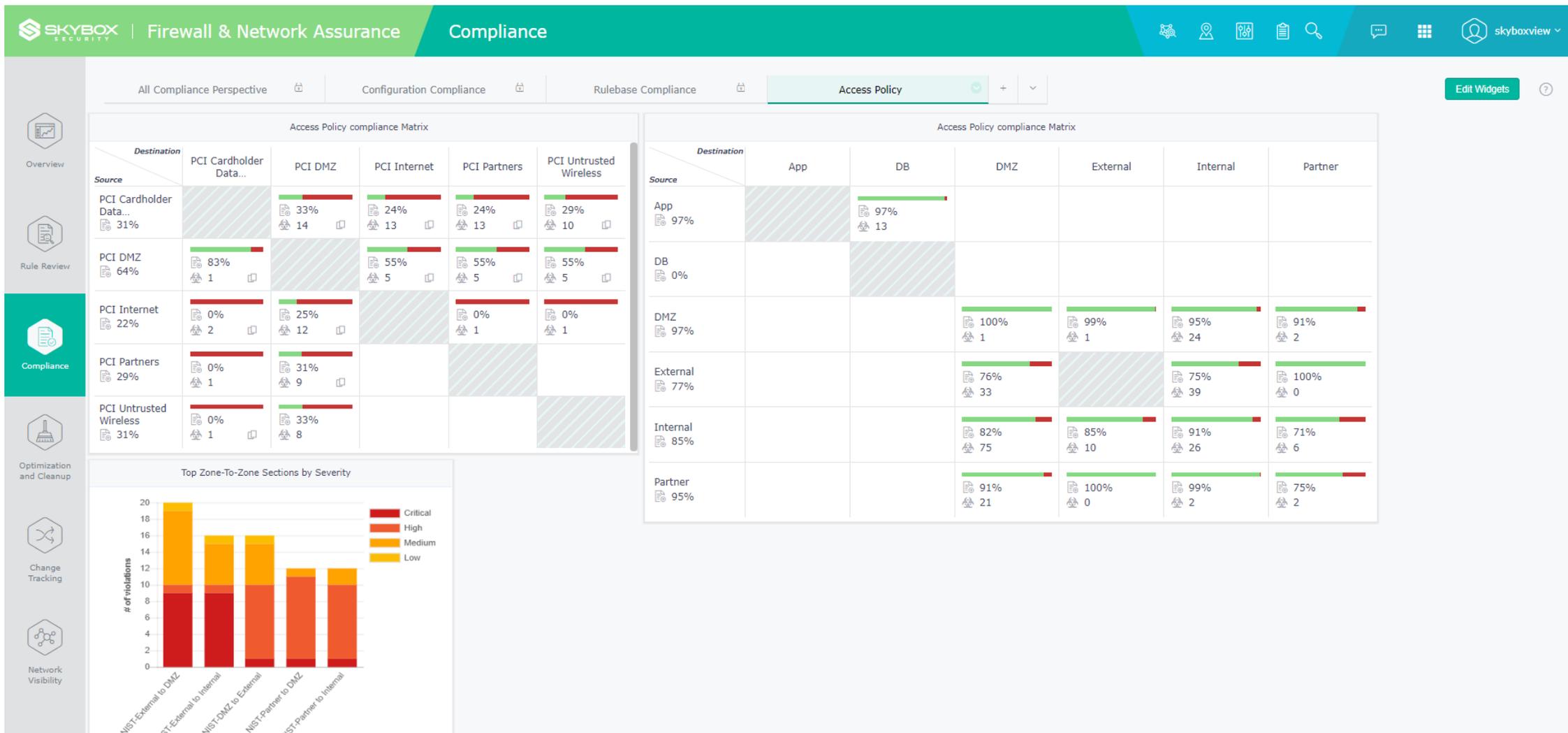
The diagram illustrates a network topology with several key components: Internet (cloud) at the source, a path through main_FW (16.0.0.1), Main Router (192.169.1.2), Internal Router (192.170.8.2), and dev FW (192.170.1.1) to the destination developmentWindowsWS (192.170.17.0/24). Other nodes include Partner1, Partner2, gatewayEastA, gatewayEastB, gatewayWestA, gatewayWestB, NSX-edge, NSX, developmentServers, and Core Router. Locations like US, Los Angeles, New York, and Paris are also indicated.

Проверяем
отсутствие
доступа в 2 клика

Контроль политик сетевого доступа



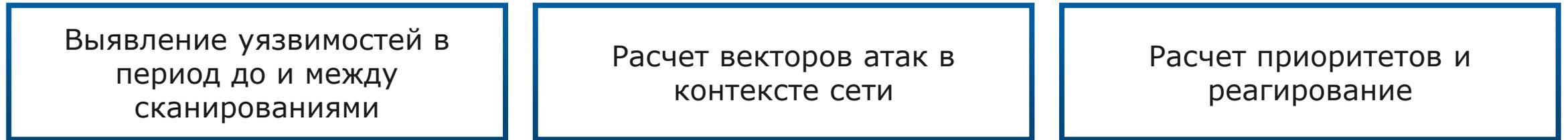
Соответствие политикам сетевого доступа



Работа с уязвимостями

Возможные сценарии

Принцип работы

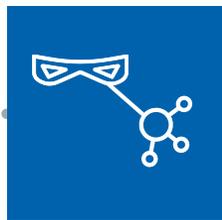


Как Это Работает



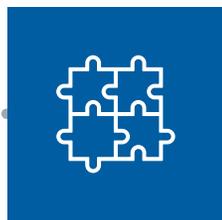
1

Выявление



2

Анализ



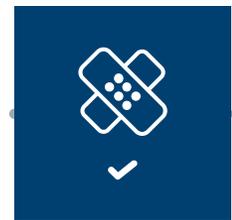
3

Приоритезация



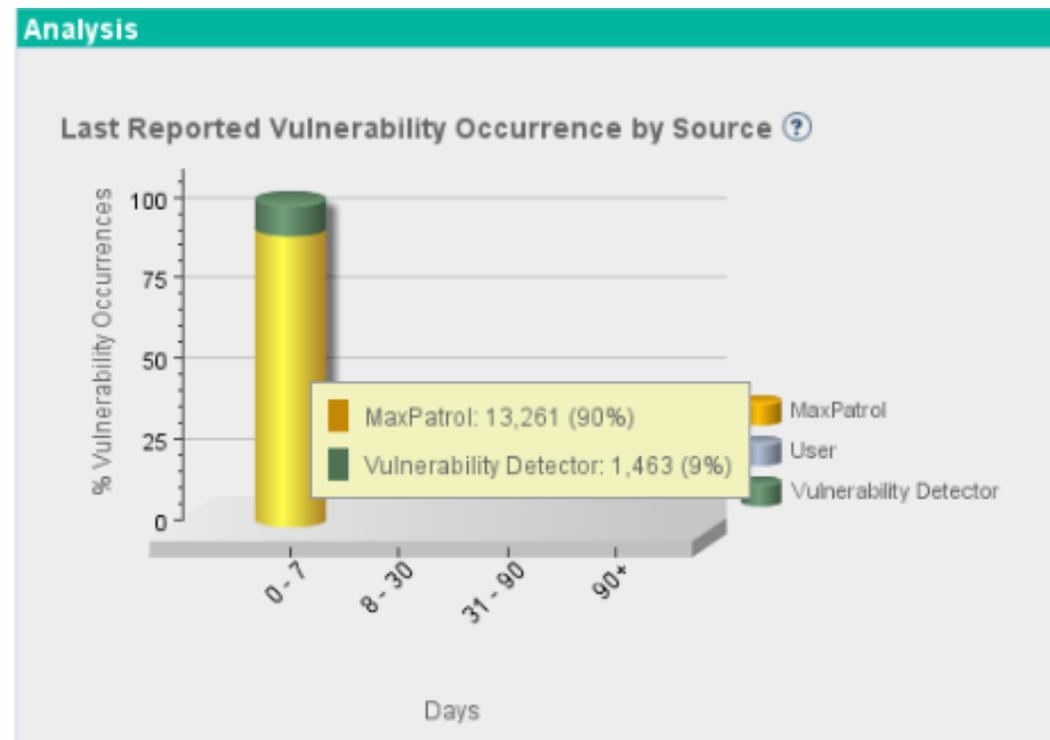
4

Реагирование

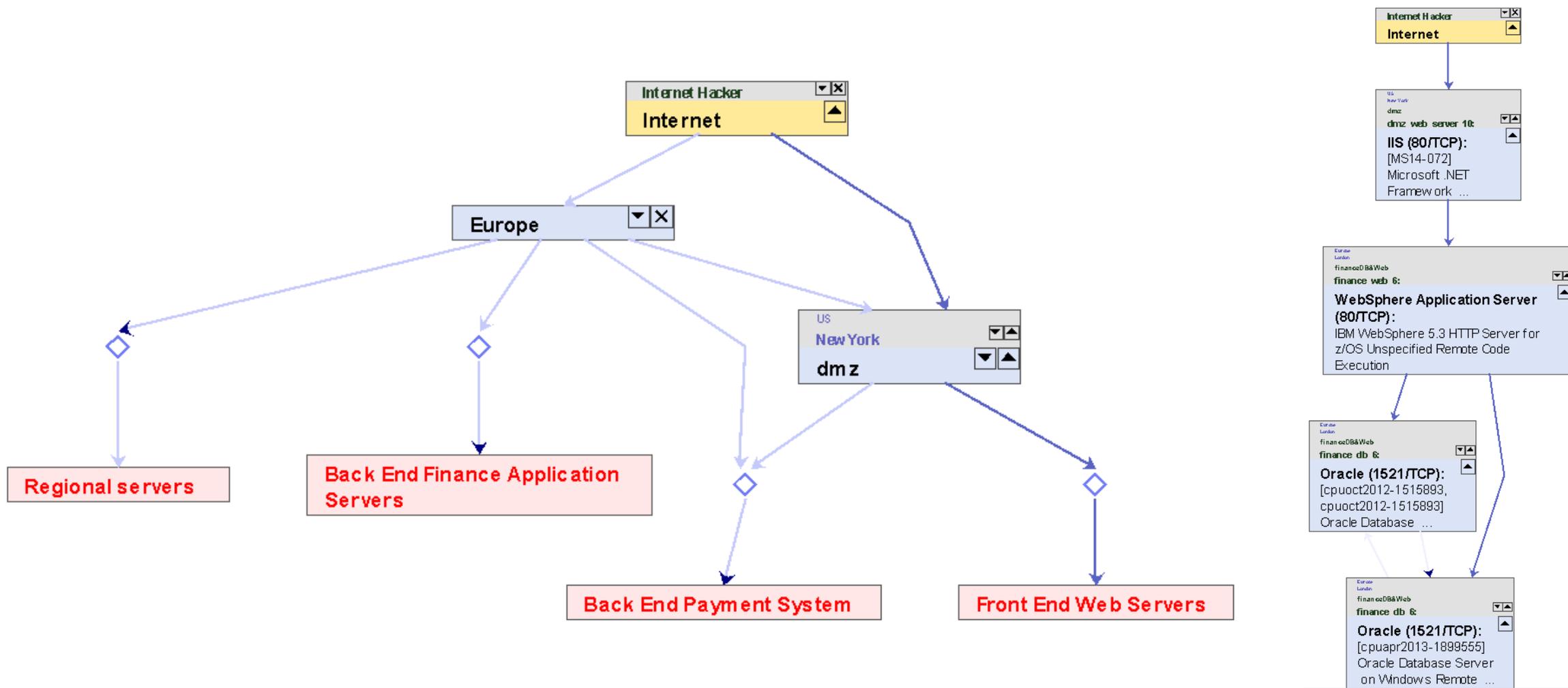


Выявление уязвимостей

- Как это работает:
 - » Загрузка отчетов сканеров
 - » Загрузка отчетов систем инвентаризации SCCM, WSUS и др.
 - » Ежедневное «пассивное» сканирование
- Результат:
 - » Актуальный список всех известных уязвимостей (обновляемая база Skybox из 25+ источников)
 - » актуальный список уязвимостей для ИТ-активов



Визуализация вектора атаки



Индикаторы угроз и приоритезация уязвимостей

■ Учитываются:

- » Критичность
- » Достижимость (наличие доступа)
- » Уровень злоумышленника
- » Ценность актива
- » Наличие готового эксплойта
- » Статистика атак с использованием конкретной уязвимости

The screenshot displays a vulnerability management interface. The top section shows a list of 141 vulnerability occurrences. Below this, a detailed view for a specific vulnerability is shown, including a 'Solutions' tab. The solutions table lists several upgrade options and one mitigation option.

ID	Solution Name	Solution Type	Description
SBV-36637	Upgrade:10.2.0.4.14	Upgrade	Upgrade Oracle, Oracle Database to version 10.2.0.4.14:For Oracle Database ...
SBV-36637	Upgrade:11.1.0.7.17	Upgrade	Upgrade Oracle, Oracle Database to version 11.1.0.7.17:For Oracle Database ...
SBV-36637	Upgrade:11.2.0.2.8	Upgrade	Upgrade Oracle, Oracle Database to version 11.2.0.2.8:For Oracle Database 1...
SBV-36637	Upgrade:14275629	Upgrade	Upgrade Oracle, Oracle Database to version 14275629:For Oracle Database 1...
SBV-36637	Upgrade:14275630	Upgrade	Upgrade Oracle, Oracle Database to version 14275630:For Oracle Database 1...
SBV-36637	Mitigate by IPS:0245123	Mitigate by IPS	The vulnerability can be mitigated by activating FortiGate IPS signature 33432: ...

Рекомендации по устранению

Важность приоритезации

ОПРЕДЕЛЕНИЕ ВСЕХ ИЗВЕСТНЫХ УЯЗВИМОСТЕЙ

ВСЕГО: 70К
Skybox Vulnerability Database

Потенциальная угроза

ОПРЕДЕЛЕНИЕ СУЩЕСТВУЮЩИХ УЯЗВИМОСТЕЙ

ВСЕГО НАЙДЕНО: 7122
Сканеры защищенности,
Skybox Vulnerability Detector

Потенциальная угроза

НАЛИЧИЕ ЭКСПЛОЙТОВ

ВСЕГО ОПРЕДЕЛЕНО: 1105
Skybox Research Lab real-time threat intelligence

Потенциальная угроза



КОРРЕЛЯЦИЯ С CVSS

ВСЕГО КРИТИЧНЫХ: 3578
CVSS scoring

Потенциальная угроза

ДОСТУПНЫЕ В СЕТИ УЯЗВИМОСТИ

ДОСТУПНО В СЕТИ: 141
Анализ векторов атак

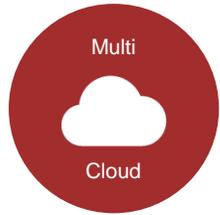
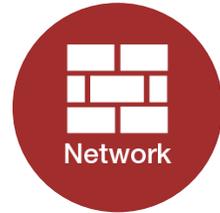
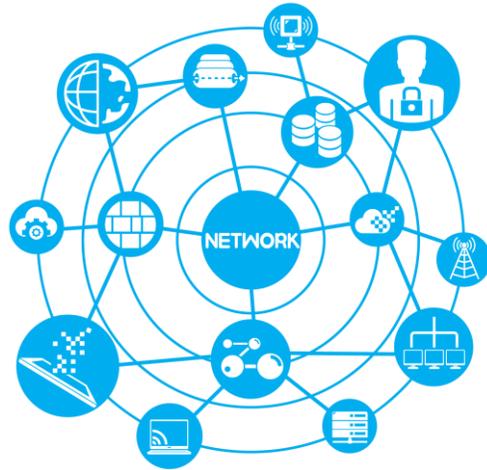
Вероятная угроза

ВЫДЕЛЕНИЕ УЯЗВИМОСТЕЙ С МАКСИМАЛЬНЫМ РИСКОМ

ВСЕГО: 13
Skybox Vulnerability Control Prioritization Center

Вероятная угроза

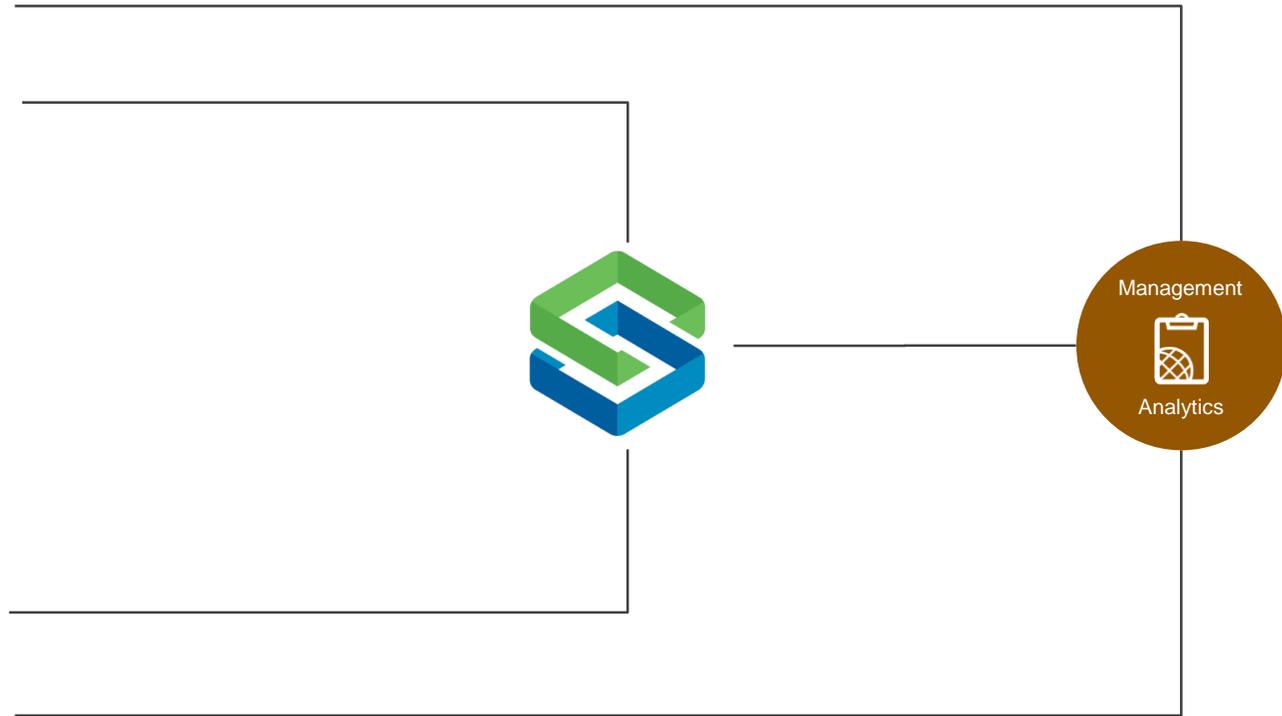
Fortinet Security Fabric + Skybox Security



Системы
инвентаризации и
патч-менеджмента



Сканеры
защищенности



FERTINET®



+7 (800) 511 08 28



Sales.Russia@skyboxsecurity.com