



7.1

БОЛЬШОЕ ОБНОВЛЕНИЕ

Игорь Шефер

Ведущий инженер UserGate



UserGate
7.1

IPSecv3



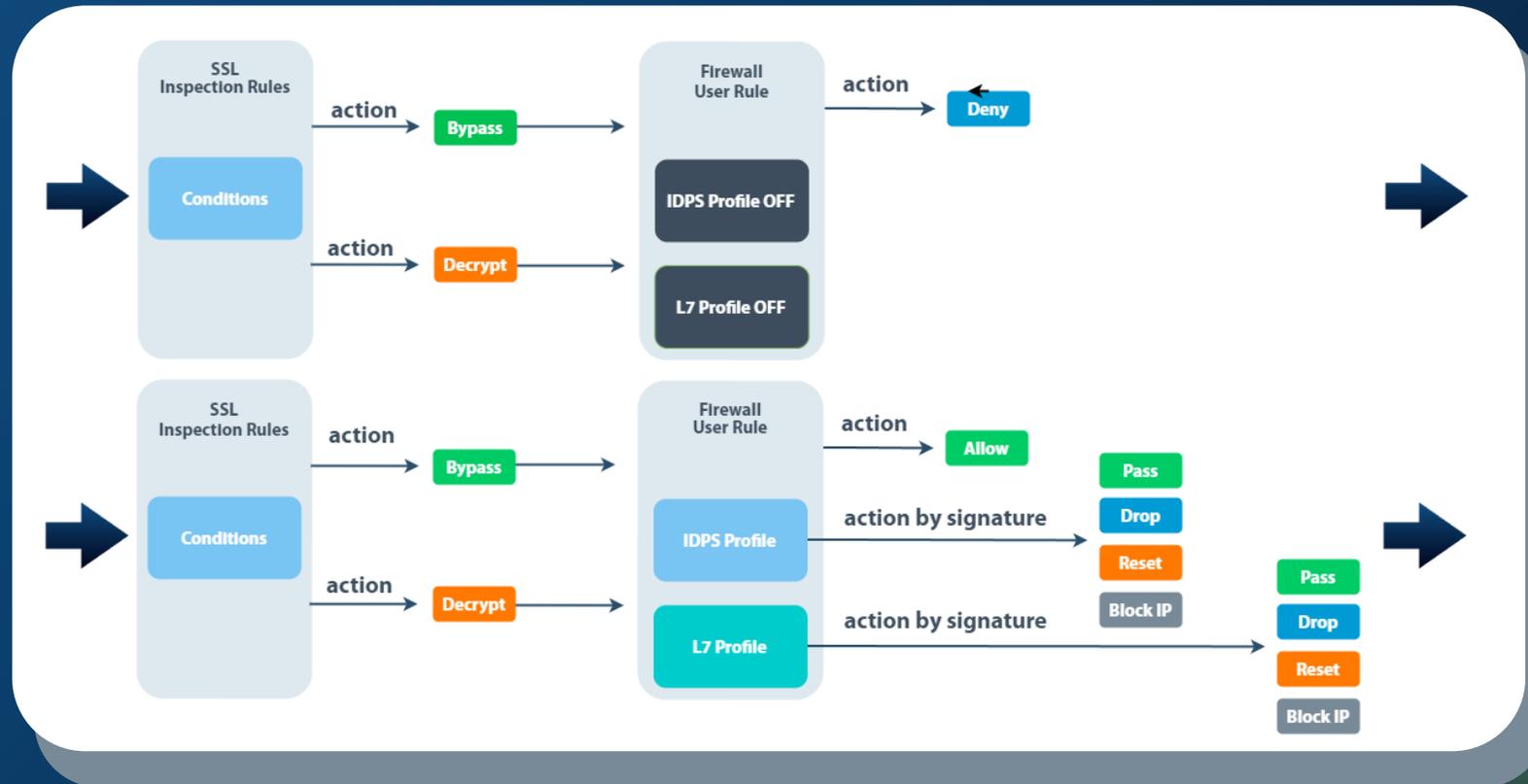
ДВИЖОК

UserGate
7.1

- 3 версия движка
- поддержка обработки расшифрованного SSL
- возможность описывать свои сигнатуры COB и L7-приложений (UASL)
- верификация
- интеграция в политики МЭ
- расширение списка действий (action) при срабатывании
- применение действия (action) по каждой сигнатуре
- возможность захвата пакетов при сработке COB и L7-приложений
- полноценное управление в CLI



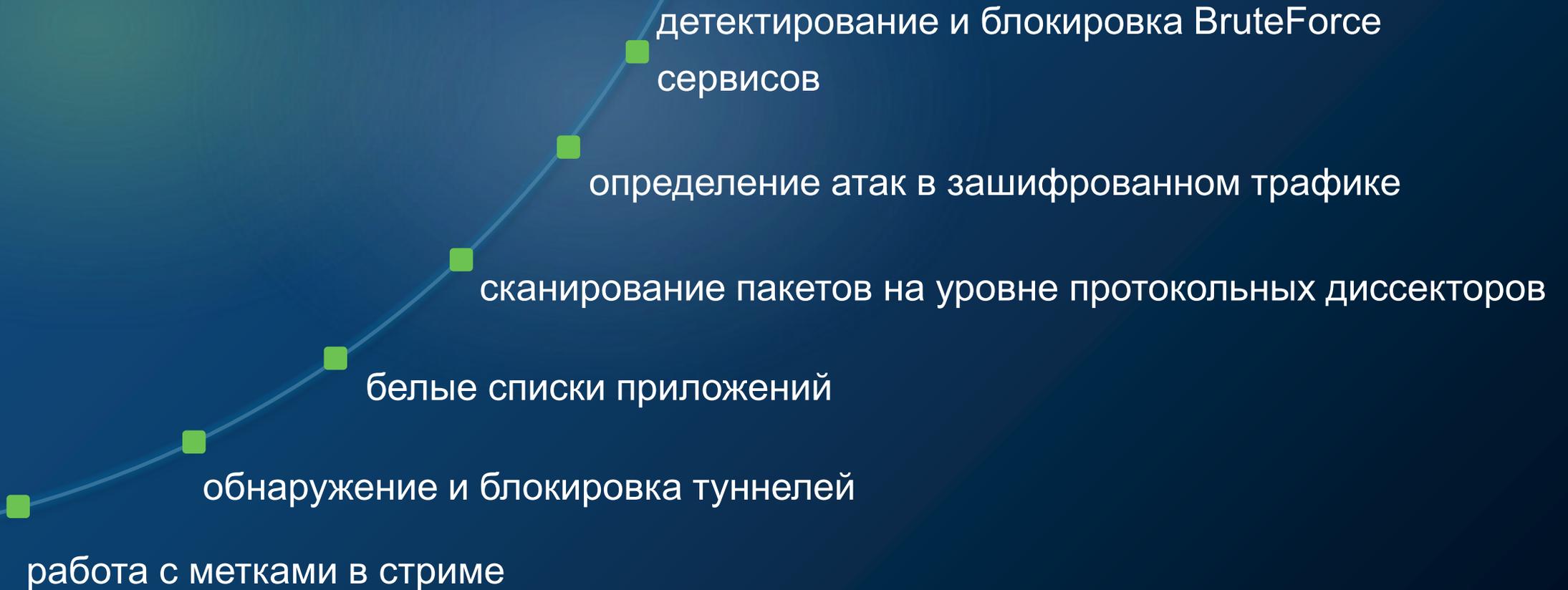
Action Flow





Новые кейсы

UserGate
7.1





GUI. IPS-профиль

UserGate
7.1

IPS profile properties

General Signatures matched

Override Enable Disable Restore default Select all View All

Enable: All All Action: All Owner: All More Reset Search Advanced

	Id		Signature name ↑	Action	Signature ope...	Protocol	Class type	References	Category	Enable PCAP	Owner
S	20020090		(MS00-021)Microsoft NT / Win...	Pass	Windows	tcp	denial-of-ser...	CVE: 2000-02...	misc	Disabled	© UserGate
S	20020052		(MS00-040)Microsoft					2000-03...	misc	Disabled	© UserGate
S	22000124		(MS00-092)Microsoft S					2000-10...	sql	Disabled	© UserGate
S	22000122		(MS00-092)Microsoft S					2000-10...	sql	Disabled	© UserGate
S	22000170		(MS02-038)Microsoft S					2008-01...	sql	Disabled	© UserGate

Signature settings

Enabled: Enable

Action: Block IP

Enable logging: Enable

PCAP file: Enable

Apply to: Both

Duration: 0 / days

Save Cancel

Действия: None, Pass, Drop, Reset, Block IP
Логирование: Enable, Disable
Запись PCAP: Enable, Disable
Применить к: Src, Dst, Both (активно при Reset и Block IP)
Продолжительность: days, hours, minutes



GUI. IPS-сигнатура Создание

UserGate
7.1

Шаг 1

Custom signatures properties

General UASL and settings

Enabled:

Id: Automatic

Name:

Description:

Signature threat: 1 very low

Class type: Select value

Category: Select value

Signature operating system:

Windows Linux Mac OS
 BSD Solaris X
 Android iOS Cisco
 Other

CVE: 2000-0001

BDU: 2020-01000

URL: https://example.com

Save Cancel

Шаг 2

Custom signatures properties

General UASL and settings

UASL

```
UASL(name="brute.force"; .protocol=tcp; .pattern="USER"; .flow=from_server; .rate=3,60; .track=src_ip)
```

Settings

Action: Block IP

Enable logging: Enable

PCAP file: Disable

Apply to: Both

Duration: 5 minutes

Verify signature Save Cancel



GUI. UASL

UserGate
7.1

Фильтр по IP-адресам:

— src/dst (IPaddr/IPsubnet)

Фильтр по TCP/UDP-портам:

— src/dst (equal, less than, greater than, in range)

Поиск паттернов (packet payload):

— pattern (string)

Модификаторы области поиска:

— icmp, tcp, udp etc

Частота срабатывания:

— rate (count, period); track (src/dst IP)

Направление анализа:

— from_client, from_server, bi_directional

Протокольные диссекторы:

— tcp dissector, udp dissector, icmp dissector etc

Матчинг бинарных данных

— byte_test, byte_jump

Пример:

```
UASL(.name='Scan';  
.flow=from_client;  
.tcp.flags = S;  
.dst_port=1:1024;  
.rate=100,10; .track=src_ip;)
```



GUI. SCADA

UserGate 7.1

The screenshot displays the UserGate GUI interface for managing IPS signatures. The main window shows a list of signatures with columns for ID, Status, Signature name, Action, Signature operating system, Protocol, Class type, References, Category, Enable PCAP, and Owner. A filter properties dialog is open, showing a list of signatures matched by the filter: category = scada and classtype = protocol-command. The dialog includes a search bar, a list of signatures with columns for ID, Signature name, Action, Signature operating system, Protocol, Class type, References, Category, Enable PCAP, and Owner, and a page navigation bar at the bottom.

Id	Status	Signature name	Action	Signature operating ...	Protocol	Class type	References	Category	Enable PCAP	Owner
1378	Default settin...	3S Smart Software Solutions CoDeSys Gat...	Pass	Windows	tcp	arbitrary-code-exec...	CVE: 2012-4704	scada	Disabled	UserGate
1379	Default settin...	3S Smart Software Solutions CoDeSys Gat...	Pass	Windows						
1396	Default settin...	3S Smart Software Solutions CoDeSys Gat...	Pass	Windows						
1412	Default settin...	3S Smart Software Solutions CoDeSys Gat...	Pass	Windows						
1323	Default settin...	7T Interactive Graphical SCADA System Fil...	Pass	Windows						
162	Default settin...	7T Interactive Graphical SCADA System M...	Pass	Windows						
163	Default settin...	7T Interactive Graphical SCADA System Re...	Pass	Windows						
1371	Default settin...	ABB MicroSCADA Wserver Command Exec...	Pass	Windows						
24060948	Default settin...	ABB MicroSCADA wserver.exe CreateProce...	Pass	BSD Linux MacOS Windows						
1438	Default settin...	Advantech Studio NTWebServer.exe Create...	Pass	Windows						
1333	Default settin...	Advantech WebAccess AspVCOby ActiveX ...	Pass	Windows						
1364	Default settin...	Advantech WebAccess BwRPwd.exe Stac...	Pass	Windows						
1425	Default settin...	Advantech WebAccess Client bwsfcfg St...	Pass	Windows						
1400	Default settin...	Advantech WebAccess Dashboard openWi...	Pass	Windows						
1401	Default settin...	Advantech WebAccess Dashboard remove...	Pass	Windows						
1399	Default settin...	Advantech WebAccess Dashboard remove...	Pass	Windows						
165	Default settin...	Advantech WebAccess Dashboard Viewer ...	Pass	Windows						
1403	Default settin...	Advantech WebAccess Datacore DCE/RPC...	Pass	Windows						
1402	Default settin...	Advantech WebAccess DCE/RPC webnrc...	Pass	Windows						
1417	Default settin...	Advantech WebAccess HMI and SCADA So...	Pass	Windows						

Filter's properties dialog: Enabled, category = scada and classtype = protocol-command. Signatures matched: 80000325, 80000304, 80000301, 80000324, 80000334, 80000319, 80000303, 80000317, 80000318, 80000335, 80000314, 80000302, 80000144, 80000151, 80000159, 80000154, 80000156, 80000139, 80000146, 80000153, 80000140, 80000147, 80000155, 80000158.



GUI. Сигнатуры L7

UserGate
7.1

Applications

Add Edit Delete Refresh

All Owner: All More Reset Search Advanced

	Id	Type	Name ↑	Application categories	Application technology
1	8163	Application	0bin	<input type="checkbox"/> Web posting	Browser-based
2	731	Application	11st	<input type="checkbox"/> Web browsing	Browser-based
3	894	Application	123f.com	<input type="checkbox"/> Web browsing	Browser-based
4	5810	Application	123VPN	<input type="checkbox"/> Proxies and anonymizers	Client-server
5	9074	Application	1337x.to	<input type="checkbox"/> Web browsing	Browser-based
6	188	Application	1C	<input type="checkbox"/> Business	Client-server
7	7855	Application	1C-Connect	<input type="checkbox"/> Instant messaging <input type="checkbox"/> Conferencing	Client-server
8	7856	Application	1C-Connect audio	<input type="checkbox"/> Instant messaging <input type="checkbox"/> Conferencing	Client-server
9	7858	Application	1C-Connect chat	<input type="checkbox"/> Instant messaging <input type="checkbox"/> Conferencing	Client-server
10	7859	Application	1C-Connect file transfer	<input type="checkbox"/> Instant messaging <input type="checkbox"/> Conferencing	Client-server
11	7860	Application	1C-Connect proxy	<input type="checkbox"/> Instant messaging <input type="checkbox"/> Conferencing	Client-server
12	7857	Application	1C-Connect remote access	<input type="checkbox"/> Instant messaging <input type="checkbox"/> Conferencing	Client-server
13	9025	Application	1clickVPN	<input type="checkbox"/> Proxies and anonymizers	Browser-based
14	9845	Application	1F Mobile	<input type="checkbox"/> Instant messaging	Client-server
15	9041	Application	2ch.hk	<input type="checkbox"/> Social networking	Browser-based
16	7696	Application	2GIS	<input type="checkbox"/> Web browsing	Browser-based
17	532	Application	360.com	<input type="checkbox"/> Web browsing	Browser-based
18	9666	Application	3DNews	<input type="checkbox"/> Web posting	Browser-based
19	9040	Application	4chan	<input type="checkbox"/> Social networking	Browser-based
20	811	Application	4PDA	<input type="checkbox"/> Web browsing	Browser-based
21	254	Application	4Shared	<input type="checkbox"/> File storage and backup	Browser-based
22	34	Application	6indon	<input type="checkbox"/> Tunneling	Network protocol

Page 1 of 72 Total: 1781

Custom application properties

General UASL

Type: Application

Id: Automatic

Name:

Description:

Signature threat: very low

Technology: Select value

Categories:

- Media streaming
- Tunneling
- Conferencing
- Mobile
- VOIP
- File storage and backup
- Instant messaging
- Email
- Games
- Trojan Horses
- Proxies and anonymizers
- Web posting
- Web browsing
- Social networking
- Coin Miners
- Remote access
- Business
- Standard networks
- Software update
- File sharing P2P

Save Cancel



GUI. Правила МЭ

UserGate
7.1

Rule properties

General Source Users Destination Service Time HIP profiles Usage History

Enabled:

Name: Rule

Description:

Action: **Deny**

Application profile: *Do not use application profile*

IPS profile: *Do not use IPS profile*

Reject with: Not selected

Scenario: Do not use scenario

Logging: None

Enable logging limit:

Limit logging events to: 3 / hour

Maximum number of packets per event: 5

Apply rule to: Any packets

Place to: End of the list

Rule properties

General Source Users Destination Service Time HIP profiles Usage History

Enabled:

Name: Rule

Description:

Action: **Allow**

Application profile: Test app profile

IPS profile: Test IPS profile

Reject with: Not selected

Scenario: Do not use scenario

Logging: None

Enable logging limit:

Limit logging events to: 3 / hour

Maximum number of packets per event: 5

Apply rule to: Any packets

Place to: End of the list

Save Cancel



UserGate
7.1

UserID



UserID. Задачи

Прозрачная идентификация
пользователей



Синхронизация групп пользователей



Сегментация на базе принадлежности к группе LDAP или имени
пользователя (Identity Based Network Firewall)



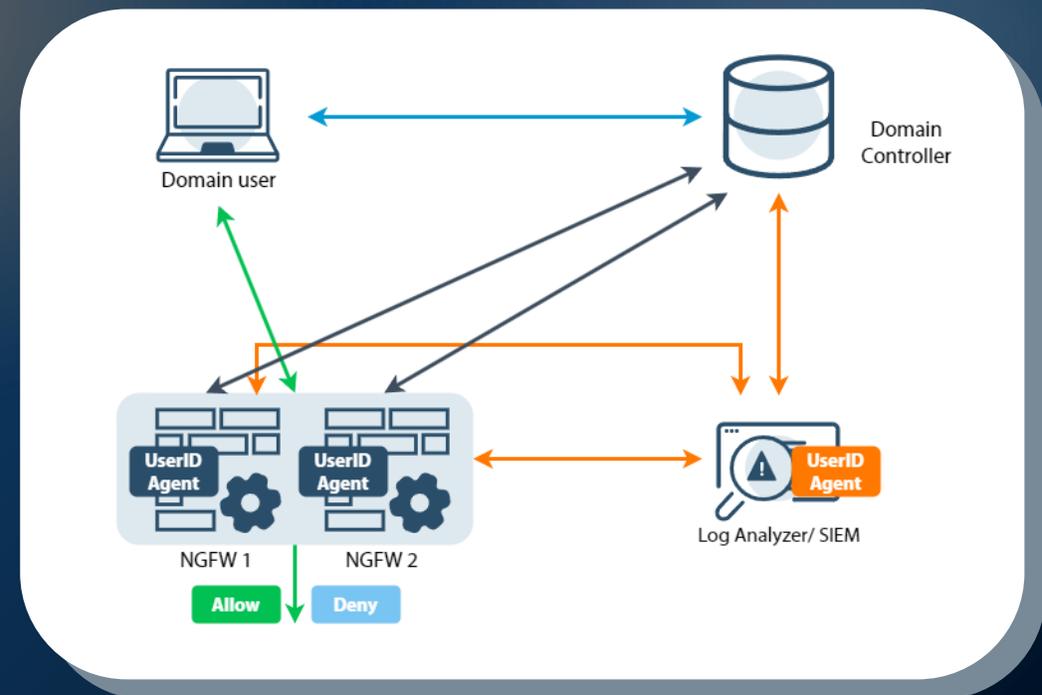
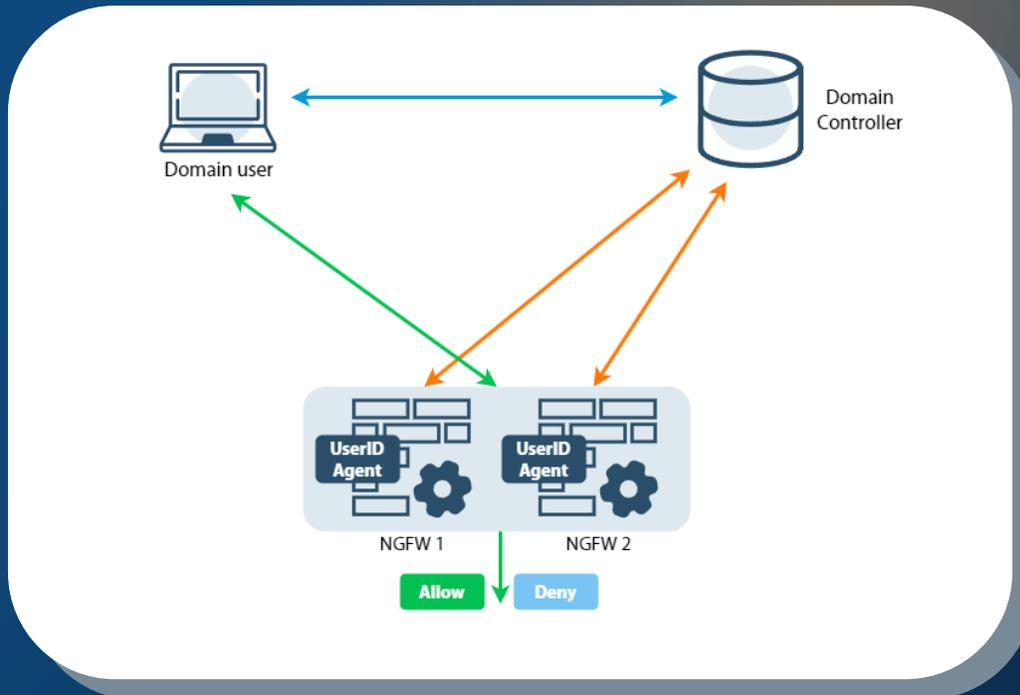


UserID. Возможности

- Идентификация посредством использования журналов DC по WMI (коды событий 4624, 4634, 4768, 4769, 4770) и/или по Syslog (RFC 3164, RFC 5424, RFC 6587).
 - Использование фильтров и таймеров в настройках агента.
- Режимы работы:
 - а. Агент на борту NGFW;
 - б. Агент на борту LogAn;
 - в. Агенты на NGFW и LogAn.
- Дистрибуция данных пользователей на NGFW.

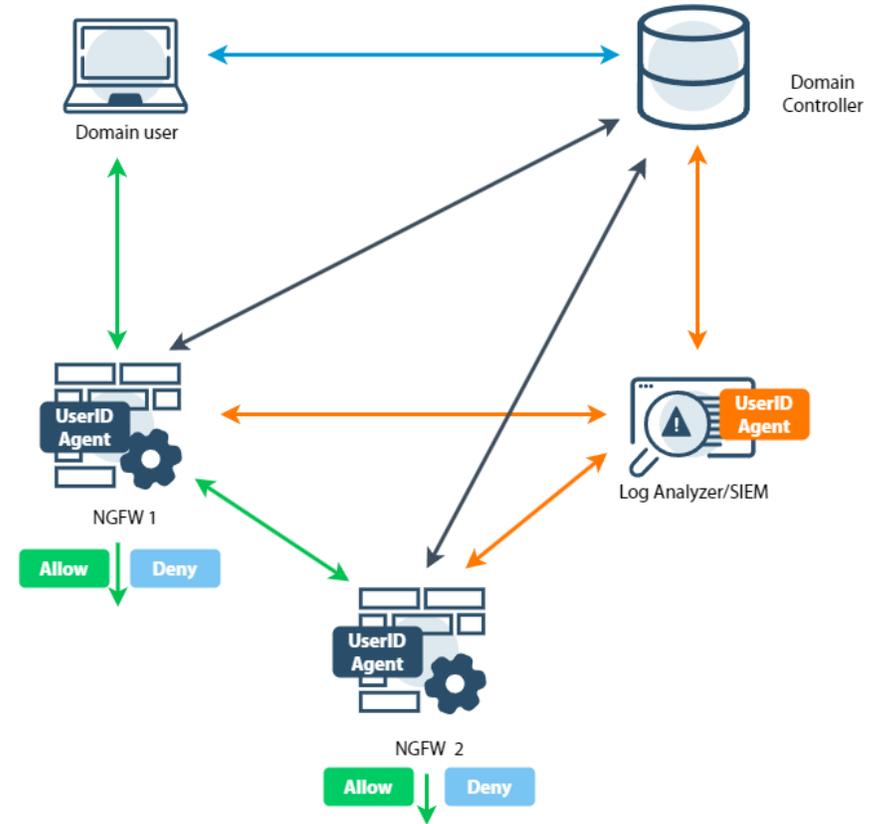


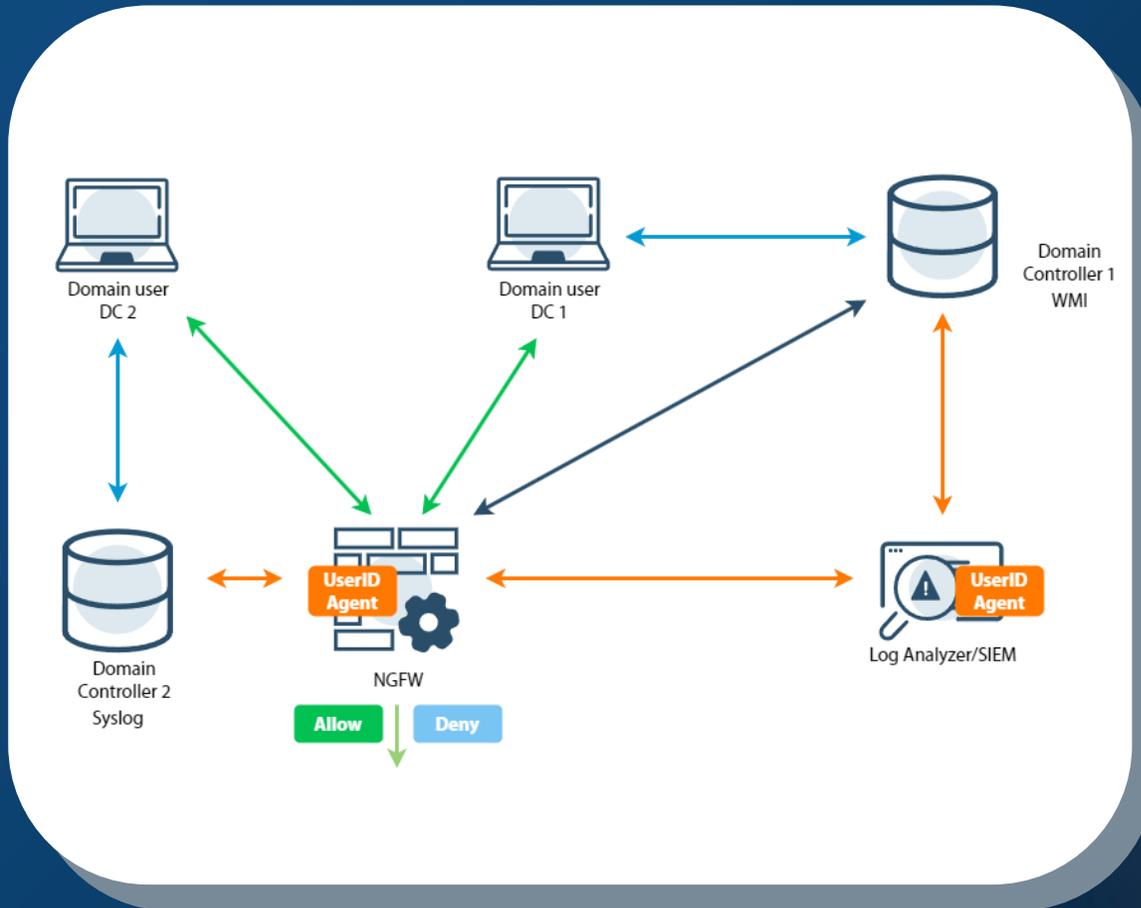
Вариант исполнения: Cluster NGFW





Вариант исполнения: NGFW + LogAn/ SIEM Дистрибуция

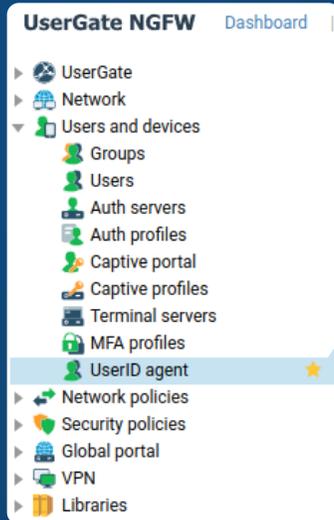




Вариант исполнения:
NGFW + LogAn/SIEM
с активными агентами



GUI. Добавление агента



Microsoft Active Directory server properties

Enabled:

Name: DC

Description:

Address: 192.168.0.100

Protocol: WMI

Name: user

Password:

Auth profile: Example user auth profile

Save Cancel

Syslog sender properties

General Filters

Enabled:

Name: DC2

Description:

Address: 192.168.0.200

Default domain: domain.local

Timezone: UTC

Auth profile: Example user auth profile

Save Cancel



GUI. Конфигурирование агента

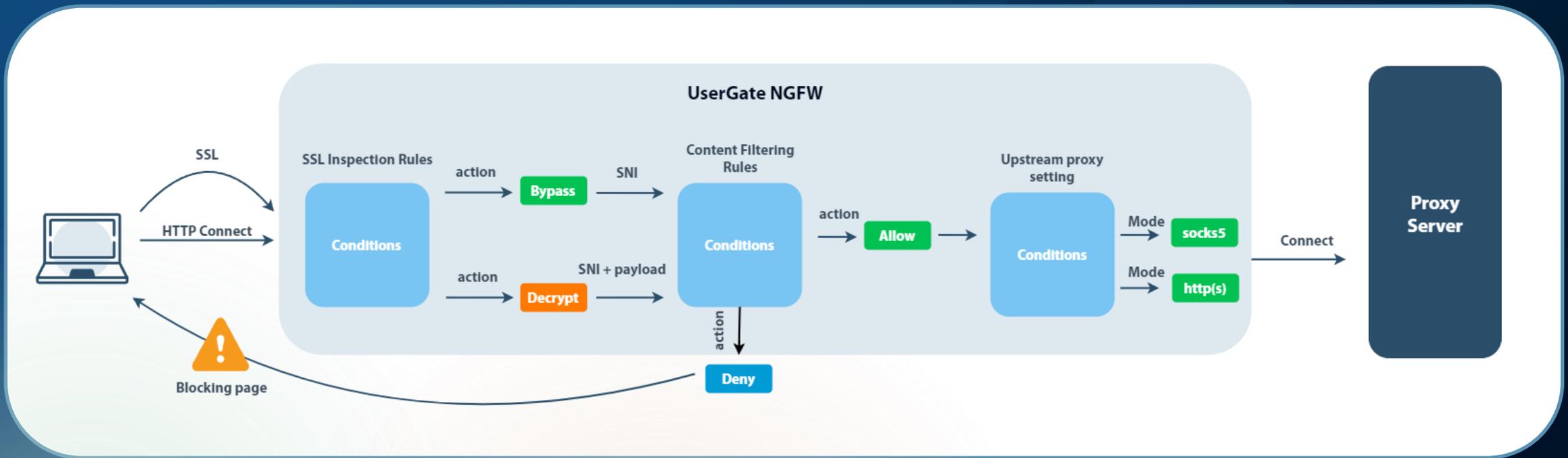


UserGate
7.1

Upstream Proxy



Upstream Proxy flow





GUI. Настройка. Пользовательский трафик

UserGate
7.1

- UserGate
 - General settings
 - Device management
 - Administrators
 - Certificates
 - User certificate profiles
 - Network
 - Users and devices
 - Network policies
 - Security policies
 - Global portal
 - VPN
 - Libraries

Upstream proxy

Upstream proxy settings socks5://0.0.0.0:1080 Disabled

Upstream proxy settings

Enabled:

Mode: socks5 http(s)

IP address: 192.168.0.100

Port: 1080

Authentication:

Name: user

Password:

Save Cancel



GUI. Настройка. Лицензия и обновления

UserGate
7.1

Product activation

Welcome to UserGate activation wizard! Please enter your pin code.

Pin code:

Use upstream proxy
[Configure](#)

Back Next Cancel

Upstream proxy settings for licensing and updates

Enabled:

IP address:

Port:

Authentication:

Name:

Password:

Save Cancel



GUI. Реконфигурация Лицензия и обновления

UserGate
7.1

- ▼ UserGate
 - ⚙️ General settings
 - 📱 Device management ★
 - 👤 Administrators
 - 📜 Certificates
 - 📄 User certificate profiles
 - ▶️ 🌐 Network
 - ▶️ 👤 Users and devices
 - ▶️ ↔️ Network policies
 - ▶️ 🛡️ Security policies
 - ▶️ 🌐 Global portal
 - ▶️ 🖥️ VPN
 - ▶️ 📚 Libraries

Server operations

Maintenance actions: [Reboot](#) | [Shutdown](#)

Updates channel: [Stable](#)

Server updates: **Updates are available!**
[Install now](#)
[View changelog](#)

Offline update: [Upload file](#)

Upstream proxy settings for licensing and updates: [Configure](#)



UserGate
7.1

Endpoint Client



Client – агент SUMMA

Режимы работы UserGate Client

VPN

НIP, проверка состояния

Управление

Мониторинг событий

Аналитика и реагирование



Режим NGFW

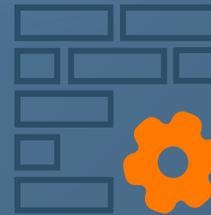
Внешние пользователи



VPN
телеметрия



UserGate NGFW



Идентификация
Политика доступа
(Правила)

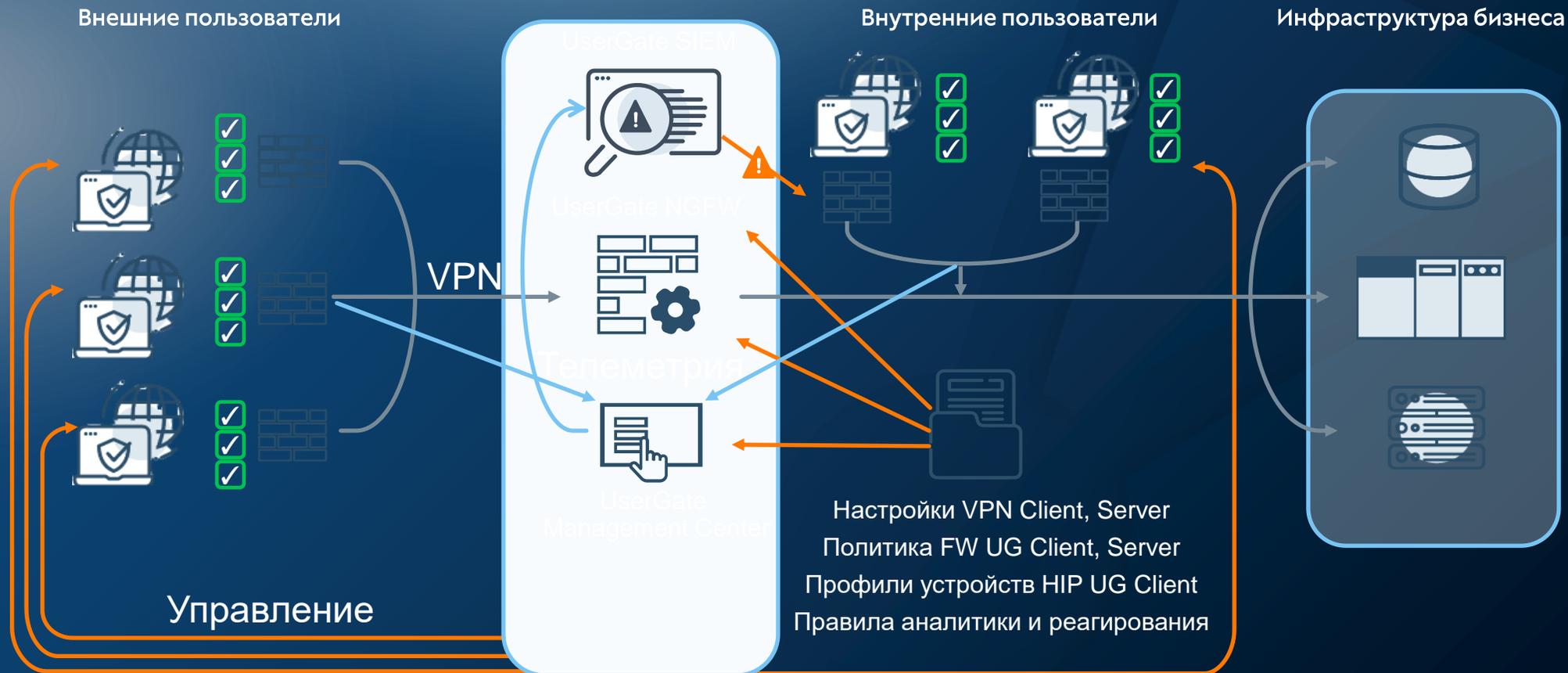
Профили устройств HIP

Инфраструктура бизнеса





Режим МС



UserGate Client –



UserGate
7.1

Функции		UG client (MC режим)	UG client (NGFW режим)	Сторонние VPN клиенты (Win, Android, etc.)
VPN		Endpoint лицензия MC Лицензия пользователя в NGFW	Лицензия пользователя NGFW	Лицензия пользователя NGFW
IKEv1	Аутентификация L2TP	✓	✓	✓
IKEv2	Аутентификация по сертификатам	✓	✓	✓
	Аутентификация EAP MS-CHAPv2	✓	✓	✓
	MFA	✓	✓	
	Split-tunneling	✓	✓	
NIP		Endpoint лицензия MC NAC подписка MC	Лицензия пользователя NGFW NAC подписка NGFW	
	Блокировка на клиенте	✓		
	Блокировка на NGFW		✓	
	Поддержка работы из-за NAT	✓		
Локальный FW на клиенте		Endpoint лицензия MC		
Мониторинг логов клиента		Sensor лицензия Logan		
Аналитика и реагирование		SIEM лицензия Logan		
Пред-настроенные правила аналитики		Подписка на экспертизу SIEM		



НІР - сбор информации с устройства

- Состояние, производительность
- Безопасность
- USB-устройства
- Элементы автозагрузки
- Процессы
- Службы
- Ключи реестра
- Программное обеспечение
- Установленные обновления

Информация о конечном устройстве

Общие Производительность Безопасность USB устройства Элементы автозагрузки Процессы Службы Ключи реестра

Пользователи

Фотография	Пользоват...	Статус	Аккаунт	Имя поль...	Фамилия	Электрон...	Телефон
	user2@ug...	Локальный	Доменный	user2	ug.local	user2@ug...	111111

Информация о хосте

Netbios имя:	PC10
Версия ОС:	Майкрософт Windows 10 Корпоративная LTSC сборка 17763
Тип системы:	x64-based PC
Версия UserGate Client:	7.1.0.333
IP-адрес:	10.10.5.33
Время загрузки системы:	24 октября 2023 г., 08:45 GMT+07:00
Время:	10 ноября 2023 г., 12:53 GMT+07:00
Статус:	Онлайн
Последние данные получены:	10 ноября 2023 г., 08:53

Имя службы	Описание	Статус
AssignedAccessManagerSvc	Служба AssignedAccessManager	Остановлен
AudioEndpointBuilder	Средство построения конечных точек Windows Audio	Запущен
AudioSrv	Windows Audio	Запущен
AxinstSV	Установщик ActiveX (AxinstSV)	Остановлен
BFE	Служба базовой фильтрации	Запущен
BITS	Фоновая интеллектуальная служба передачи (BITS)	Остановлен
BrokerInfrastructure	Служба инфраструктуры фоновых задач	Запущен
BTAGService	Служба звукового шлюза Bluetooth	Остановлен
BthAvctpSvc	Служба AVCTP	Запущен
bthserv	Служба поддержки Bluetooth	Остановлен
camsvc	Служба диспетчера доступа к возможностям	Остановлен
CDPSvc	Служба платформы подключенных устройств	Запущен
DevProSvc	Распространение сертификата	Запущен

Безопасность

Компонент	Статус
Межсетевой экран	Выключен
Автоматическое обновление	Включен
Антивирус	Выключен
Центр обеспечения безопасности Windows	Выключен

Имя компонента	Имя разработчика	Версия
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.28.29...	Microsoft Corporat...	14.28.29913.0
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.28.29...	Microsoft Corporat...	14.28.29913.0
Mozilla Firefox (x64 ru)	Mozilla	118.0.2
Mozilla Maintenance Service	Mozilla	117.0
UserGate Client	UserGate	7.1.0.333
VMware Tools	VMware, Inc.	11.3.5.18557794
WinRAR 6.11 (64-разрядная)	win.rar GmbH	6.11.0
Пакет драйверов Windows - UserGate kgdrv ActivityMonitor (0...	UserGate	06/08/2022 1.0.0.552



HIP - нотификация

The screenshot displays the UserGate management console interface. On the left is a navigation sidebar with categories like 'Устройства' (Devices) and 'HIP объекты' (HIP objects). The main area shows a table of devices with columns for name, OS, version, last connection, and compliance status. A device named 'Autogenerated endpoi...' is highlighted with a green status icon.

Название ↑	Версия ОС	Версия	Последнее подключение	Телеметрия	Мониторинг	Группы шаблонов	HIP профили	Устройство
✓ Autogenerated endpoi...	Майкрософт...	7.1.0.333	10 ноября 2023 г., 09:31	IP Address: 10.10.5.33 Netbios имя: PC10	Синхронизация конечного устройства завершилась успешно Информация о конечном у...	eps1	Не соответствует комплаенсу Посмотреть отчет	Log

Below the table, two 'Отчет несоответствия требованиям' (Compliance Report) windows are shown. The first report is dated 10 ноября 2023 г., 09:34 and lists 'HIP1' and 'CMD' as non-compliant elements. The second report is dated 10 ноября 2023 г., 09:35 and lists 'CMD' as a prohibited object.

Overlaid on the console is a 'UserGate Endpoint Client' notification window with a yellow warning icon: 'UserGate Endpoint Agent Device added to quarantine'. At the bottom left, a settings menu is open, showing options like 'Настройка VPN', 'Политики сети', and 'Механизм экрана'.



Мониторинг событий

Журнал событий:

В журнале событий конечных устройств отражены события, получаемые от конечных устройств, контролируемых с использованием программного обеспечения UserGate Client.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например, диапазон дат, важности, типу события и т.п.

Узел	Время	Статус	Конец...	Уровень лога	Данные
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:31:57	🟢	PC10	🟢 Аудит успеха	Перечислено участие в защищенных локальных группах. Субъект: ИД безопасности: S-1-5-18 Имя у...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:31:57	🟢	PC10	🟢 Аудит успеха	Перечислено участие в защищенных локальных группах. Субъект: ИД безопасности: S-1-5-18 Имя у...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:35	🟢	PC10	🟢 Аудит успеха	Попытка запроса существования пустого пароля для учетной записи. Тема: ИД безопасности: S-1-5...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:35	🟢	PC10	🟢 Аудит успеха	Попытка запроса существования пустого пароля для учетной записи. Тема: ИД безопасности: S-1-5...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:35	🟢	PC10	🟢 Аудит успеха	Попытка запроса существования пустого пароля для учетной записи. Тема: ИД безопасности: S-1-5...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:35	🟢	PC10	🟢 Аудит успеха	Попытка запроса существования пустого пароля для учетной записи. Тема: ИД безопасности: S-1-5...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:28	🟢	PC10	🟢 Аудит успеха	Выполнен выход учетной записи из системы. Субъект: ИД безопасности: S-1-5-21-144772055-15890...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:28	🟢	PC10	🟢 Сведения	Окончание транзакции установщика Windows: C:\Users\user2\Downloads\utmauthclient_6.2.0.17.msi...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:28	🟢	PC10	🟢 Сведения	Product: UserGate Domain Authorization Agent – Installation completed successfully.
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:28	🟢	PC10	🟢 Сведения	Установщик Windows выполнил установку продукта. Продукт: UserGate Domain Authorization Agent...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:28	🟢	PC10	🟢 Сведения	Завершение сеанса 0, запущенного 2023-10-03T06:27:27.083644900Z.
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:27	🟢	PC10	🟢 Сведения	Запуск сеанса 0 - 2023-10-03T06:27:27.083644900Z.
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:27	🟢	PC10	🟢 Аудит успеха	Новому сеансу входа назначены специальные привилегии. Субъект: ИД безопасности: S-1-5-21-144...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:27	🟢	PC10	🟢 Аудит успеха	Вход в учетную запись выполнен успешно. Субъект: ИД безопасности: S-1-5-18 Имя учетной записи...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:27	🟢	PC10	🟢 Аудит успеха	Выполнена попытка входа в систему с явным указанием учетных данных. Субъект: ИД безопаснос...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:16	🟢	PC10	🟢 Аудит успеха	Перечислено участие в защищенных локальных группах. Субъект: ИД безопасности: S-1-5-18 Имя у...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:16	🟢	PC10	🟢 Аудит успеха	Перечислено участие в защищенных локальных группах. Субъект: ИД безопасности: S-1-5-18 Имя у...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:27:15	🟢	PC10	🟢 Сведения	Начало транзакции установщика Windows: C:\Users\user2\Downloads\utmauthclient_6.2.0.17.msi. ИД...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:26:47	🟢	PC10	🟢 Сведения	Окончание транзакции установщика Windows: {38BA81AB-5A22-4BC5-84C9-9DDCABB2E13}. ИД кли...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:26:47	🟢	PC10	🟢 Сведения	Завершение сеанса 0, запущенного 2023-10-03T06:26:30.029325000Z.
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:26:47	🟢	PC10	🟢 Сведения	Product: UserGate Domain Authorization Agent – Removal completed successfully.
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:26:47	🟢	PC10	🟢 Сведения	Установщик Windows выполнил удаление продукта. Продукт: UserGate Domain Authorization Agent. B...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:26:46	🟢	PC10	🟢 Аудит успеха	Новому сеансу входа назначены специальные привилегии. Субъект: ИД безопасности: S-1-5-21-144...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:26:46	🟢	PC10	🟢 Аудит успеха	Вход в учетную запись выполнен успешно. Субъект: ИД безопасности: S-1-5-18 Имя учетной записи...
be63e2c2-0f95-4573-989c-ad09b626f463	03 октября, 09:26:46	🟢	PC10	🟢 Аудит успеха	Выполнена попытка входа в систему с явным указанием учетных данных. Субъект: ИД безопаснос...



Мониторинг событий

Приложения конечных устройств:

Отображает приложения, которые запускались на конечных устройствах

The screenshot shows the 'UserGate SIEM' interface with a sidebar on the left containing various logs and reports. The main area displays a table of applications running on endpoints. The table has columns for Node, Time, Device, Hash, Application, Version, Subject, and Signature.

Узел	Время	Конечное устройство	Хэш	Приложение	Версия	Субъект подписи	Подписано
be63e2c2...	03 октябр...	PC10	B8F00586870C42957EC5408B2C39CEEF9026F56A	consent.exe	6.2.17763.1697	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	DCE2AF90E45FB9FC05ECBC9BEDDEE53FB66F3C6D	DllHost.exe	6.2.17763.1	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	DCE2AF90E45FB9FC05ECBC9BEDDEE53FB66F3C6D	DllHost.exe	6.2.17763.1	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	DCE2AF90E45FB9FC05ECBC9BEDDEE53FB66F3C6D	DllHost.exe	6.2.17763.1	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	DCE2AF90E45FB9FC05ECBC9BEDDEE53FB66F3C6D	DllHost.exe	6.2.17763.1	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	DCE2AF90E45FB9FC05ECBC9BEDDEE53FB66F3C6D	DllHost.exe	6.2.17763.1	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	DCE2AF90E45FB9FC05ECBC9BEDDEE53FB66F3C6D	DllHost.exe	6.2.17763.1	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	5BE67DAD56E33CDBD1C327948EE70D43E69ED106	NOTEPAD.EXE	6.2.17763.1697		
be63e2c2...	03 октябр...	PC10	5BE67DAD56E33CDBD1C327948EE70D43E69ED106	NOTEPAD.EXE	6.2.17763.1697		
be63e2c2...	03 октябр...	PC10	4B8BF0359C6208468C9A55D9483E417729DB092C	utmclient.exe	6.2.0.17		
be63e2c2...	03 октябр...	PC10	DCE2AF90E45FB9FC05ECBC9BEDDEE53FB66F3C6D	DllHost.exe	6.2.17763.1	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	2FA92AF18B877319E660F8A152FAF386C33E2F3C	taskmgr.exe	6.2.17763.1697	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10					
be63e2c2...	03 октябр...	PC10					
be63e2c2...	03 октябр...	PC10					
be63e2c2...	03 октябр...	PC10					
be63e2c2...	03 октябр...	PC10					
be63e2c2...	03 октябр...	PC10	DCE2AF90E45FB9FC05ECBC9BEDDEE53FB66F3C6D	DllHost.exe	6.2.17763.1	Microsoft Windows	Microsoft Wind
be63e2c2...	03 октябр...	PC10	B54CE57731B58A49800EFA31894DDF6AB66A4F4	MsiExec.exe	5.0.17763.404		



Мониторинг событий

Аппаратура конечных устройств:

Данный журнал содержит информацию об устройствах, подключаемых к конечным устройствам с установленным UserGate Client

Узел	Время	□	Конечное устройство	Устройство	Идентификатор уст
be63e2c2-0f95-4573-989c-ad09b626f463	15 сентября, 05:07:13	+	PC10	USB Root Hub	USB\ROOT_HUB\48
be63e2c2-0f95-4573-989c-ad09b626f463	15 сентября, 05:07:13	+	PC10	USB Input Device	USB\VID_0627&PID
be63e2c2-0f95-4573-989c-ad09b626f463	15 сентября, 05:07:13	+	PC10	HID-compliant mouse	HID\VID_0627&PID
0ff6e78b-3b22-4ffe-a350-6ec569071e2e	13 сентября, 08:20:22	+	PC11	USB Root Hub	USB\ROOT_HUB\48
0ff6e78b-3b22-4ffe-a350-6ec569071e2e	13 сентября, 08:20:22	+	PC11	USB Input Device	USB\VID_0627&PID
0ff6e78b-3b22-4ffe-a350-6ec569071e2e	13 сентября, 08:20:22	+	PC11	HID-compliant mouse	HID\VID_0627&PID
be63e2c2-0f95-4573-989c-ad09b626f463	13 сентября, 01:14:21	+	HOME-PC	USB Root Hub	USB\ROOT_HUB\48
be63e2c2-0f95-4573-989c-ad09b626f463	13 сентября, 01:14:21	+	HOME-PC	USB Input Device	USB\VID_0627&PID
be63e2c2-0f95-4573-989c-ad09b626f463	13 сентября, 01:14:21	+	HOME-PC	HID-compliant mouse	HID\VID_0627&PID



Аналитика

Группы аналитики	Правила аналитики												
<ul style="list-style-type: none">НазваниеВоздействиеВыполнениеЗакреплениеИсследованиеПервоначальный доступПеремещение внутри периметраПовышение привилегийПолучение учётных данныхПредотвращение обнаруженияРазведкаСбор данныхУправление и контрольЭксофильтрация данных	<table border="1"><thead><tr><th>Название</th><th>Описание</th></tr></thead><tbody><tr><td>SMB admin share accessed</td><td>Detects scenarios where an attacker attempts to connect to the administrative SMB share. References: https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0008-Lateral%20Movement/T1021.002%20-SMB%20Windows%20Admin%20Shares Tags:...</td></tr><tr><td>RDP hijacking via tscon</td><td>An attempt to hijack RDP session with the Microsoft Windows "tscon" utility is detected Tags: attack.lateral_movement</td></tr><tr><td>Logon process then pass the hash</td><td>Detects logon process then pass the hash References: https://blog.netrix.com/2021/11/30/how-to-detect-pass-the-hash-attacks/#~:text=In%20particular%2C%20one%20common%20technique,move%20laterally%20within%20the Tags:...</td></tr><tr><td>Impacket DCOMexec privilege abuse via MMC</td><td>Detects scenarios where an attacker execute the Impacket DCOMexec tool in order to abuse DCOM services. References: https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0008-Lateral%20Movement/T1021.003-Distributed%20Component%20Object%20Model%20(DCOM) https://enigma0x3.net/2017/01/23/lateral-movement-via-dcom-round-2/</td></tr><tr><td>Enabling RDP via Registry</td><td>Identifies registry write modifications to enable Remote Desktop Protocol (RDP) access. This could be indicative of</td></tr></tbody></table>	Название	Описание	SMB admin share accessed	Detects scenarios where an attacker attempts to connect to the administrative SMB share. References: https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0008-Lateral%20Movement/T1021.002%20-SMB%20Windows%20Admin%20Shares Tags:...	RDP hijacking via tscon	An attempt to hijack RDP session with the Microsoft Windows "tscon" utility is detected Tags: attack.lateral_movement	Logon process then pass the hash	Detects logon process then pass the hash References: https://blog.netrix.com/2021/11/30/how-to-detect-pass-the-hash-attacks/#~:text=In%20particular%2C%20one%20common%20technique,move%20laterally%20within%20the Tags:...	Impacket DCOMexec privilege abuse via MMC	Detects scenarios where an attacker execute the Impacket DCOMexec tool in order to abuse DCOM services. References: https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0008-Lateral%20Movement/T1021.003-Distributed%20Component%20Object%20Model%20(DCOM) https://enigma0x3.net/2017/01/23/lateral-movement-via-dcom-round-2/	Enabling RDP via Registry	Identifies registry write modifications to enable Remote Desktop Protocol (RDP) access. This could be indicative of
Название	Описание												
SMB admin share accessed	Detects scenarios where an attacker attempts to connect to the administrative SMB share. References: https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0008-Lateral%20Movement/T1021.002%20-SMB%20Windows%20Admin%20Shares Tags:...												
RDP hijacking via tscon	An attempt to hijack RDP session with the Microsoft Windows "tscon" utility is detected Tags: attack.lateral_movement												
Logon process then pass the hash	Detects logon process then pass the hash References: https://blog.netrix.com/2021/11/30/how-to-detect-pass-the-hash-attacks/#~:text=In%20particular%2C%20one%20common%20technique,move%20laterally%20within%20the Tags:...												
Impacket DCOMexec privilege abuse via MMC	Detects scenarios where an attacker execute the Impacket DCOMexec tool in order to abuse DCOM services. References: https://github.com/mdecrevoisier/EVTX-to-MITRE-Attack/tree/master/TA0008-Lateral%20Movement/T1021.003-Distributed%20Component%20Object%20Model%20(DCOM) https://enigma0x3.net/2017/01/23/lateral-movement-via-dcom-round-2/												
Enabling RDP via Registry	Identifies registry write modifications to enable Remote Desktop Protocol (RDP) access. This could be indicative of												



Реагирование

Свойства действия реагирования

Общие Действие Шаблон

Включено:

Название:

Описание:

Действие:

- Послать команду на эндпоинт
- Отправить email
- Отправить сообщение
- Webhook
- Создать инцидент
- Послать команду на коннектор
- Послать команду на эндпоинт

Записывать в журнал правил:

Группировать похожие срабатывания:

Период группировки (мин.):

Количество срабатываний:

Конечные устройства

Показать Все 10 секунд Послать команду

Название ↑	Версия	Последнее подключение
✓ Autogenerated end...	7.1.0.333	10 ноября 2023 г., 10:24

Команда к конечному устройству

Команда:

Служба:

ИД процесса:

- Завершить процесс
- Запустить службу
- Остановить службу

Свойства действия реагирования

Общие Действие Шаблон

Команда:

- Отключить от сети
- Завершить процесс



7.1

Q&A?!

Игорь Шефер
Ведущий инженер UserGate