NETAMS

СИСТЕМА КОРПОРАТИВНОЙ АВТОРИЗАЦИИ WNAM

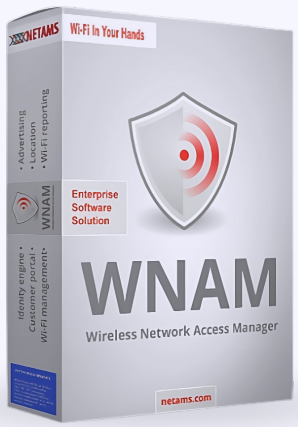
Российское программное обеспечение контроля сетевого доступа

Компьютерные сети предприятий обеспечивают подключение корпоративных компьютеров, принтеров, телевизоров, IP-телефонов, и иного оборудования. Беспроводные сети, помимо этого, используются для гостевого доступа, а также для личных устройств сотрудников. Удалённое подключения к сети через Internet обеспечивается средствами защищённого доступа.

Во всех этих сценариях администраторы сталкиваются с задачами обеспечения безопасных, контролируемых подключений на основе правил и политик, утверждённых на предприятии, противодействия атакам и угрозам, протоколирования всех попыток получения доступа.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ WNAM

Программное обеспечение Wireless Network Access Manager версии 1.6 с модулем «Корпоративная авторизация» позволяет внедрить в сети предприятия передовые механизмы контроля и управления сетевым доступом. Они функционируют для проводных, беспроводных и удалённых подключений с авторизацией корпоративных и гостевых пользователей или устройств.



АУТЕНТИФИКАЦИЯ И АВТОРИЗАЦИЯ

Аутентификация заключается в проверке подлинности предоставленных учётных данных того, кто запрашивает сетевой доступ, и различных параметров самого запроса. Авторизация проверенного пользователя назначает подключению некоторые ограничивающие атрибуты, например номер VLAN, правило ACL, лимит скорости загрузки.

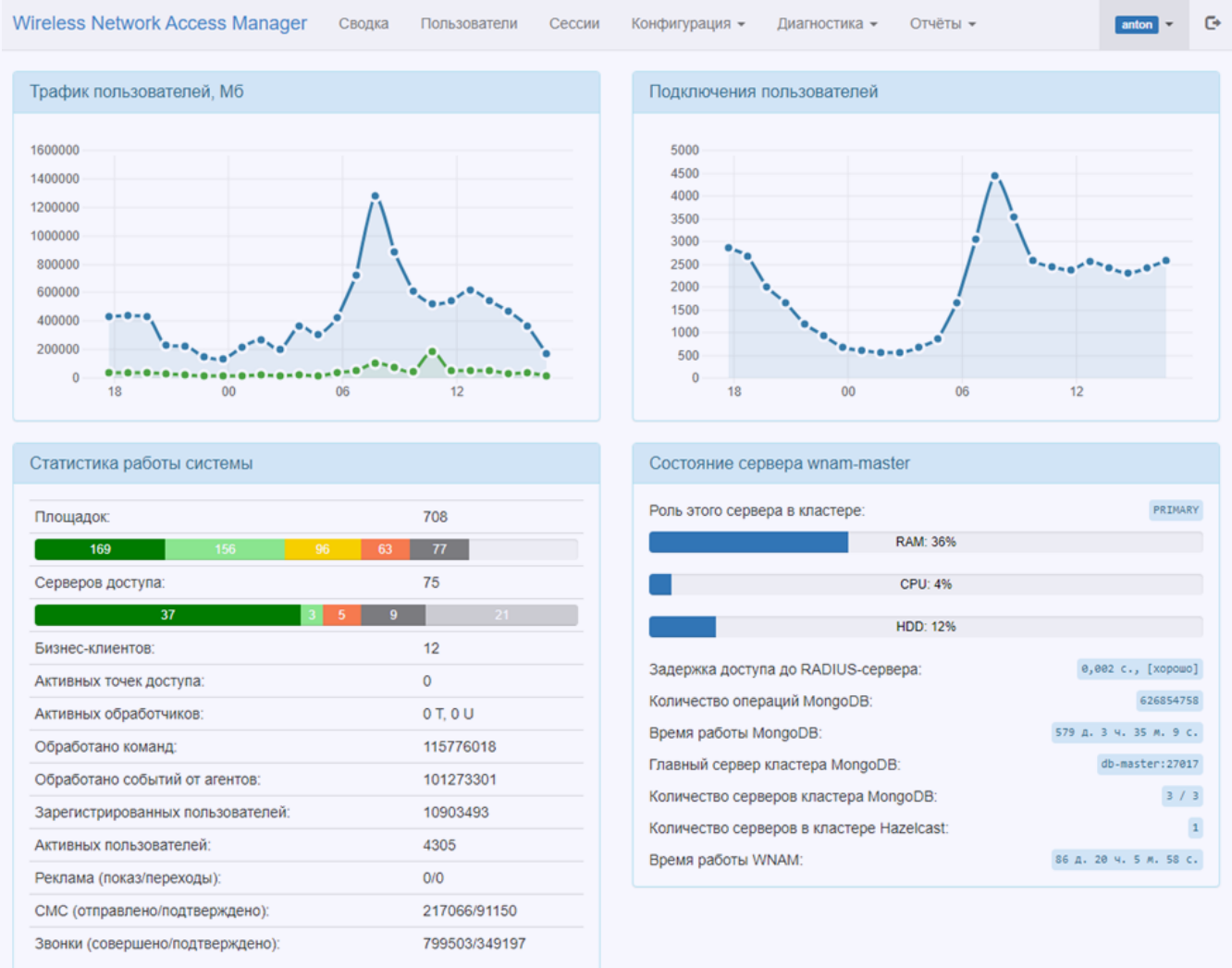
Каждая попытка подключения протоколируется, что используется как для целей расширенной диагностики конфигурационных и сетевых проблем, так и для уведомления ИБ-систем. Собранные аккаунтинг-данные позволяют строить различные отчёты об использовании ресурсов сети.

КОНТРОЛЬ СЕТЕВОГО ДОСТУПА

Для корпоративных подключений WNAM проверяет предоставленный TLS-сертификат, который может быть выписан пользователю удостоверяющим центром предприятия, или самой системой. Поддерживается защищённая проверка пар «логин-пароль» на основании встроенной базы данных, либо доменов Active Directory и других служб каталогов.

Доступ обезличенных устройств контролируется с автоматическим профилированием по MAC-адресу, производителю, функциональным параметрам, работе сенсоров, результатам сканирования, и иным критериям.

Авторизация гостевых беспроводных подключений проводится в соответствии с требованиями законодательства по СМС, звонку, ваучеру, гостиничной системе, или через Госуслуги.



КОНТРОЛЬ ДЕЙСТВИЙ АДМИНИСТРАТОРОВ

Для централизованного управления подключениями администраторов к сетевому оборудованию WNAM работает с ним по протоколу TACACS+ и позволяет настроить аутентификацию доступа, разрешения допустимых к исполнению команд,
и их протоколирование.

WNAM является полностью локальной, зарегистрированной в Реестре Минцифры разработкой, работающей под управлением ОС Linux, в том числе в кластерном, распределённом и отказоустойчивом исполнении. WNAM совместим со множеством проводного и беспроводного оборудования, реализующего протоколы RADIUS, 802.1x, Captive Portal, в частности и российского производства.

ВОЗМОЖНОСТИ СИСТЕМЫ WNAM

Поддерживаемые подключения

- Проводные: MAC Bypass, 802.1X
- Беспроводные: MAC Bypass, Captive Portal, 802.1X
- Удалённые VPN: 802.1X

Поддержка протоколов

- RADIUS
- 802.1X
- PAP
- EAP-TLS
- PEAP
- TACACS+
- LDAP
- SNMP
- Syslog
- SCEP

Взаимодействие с оборудованием

Согласно штатной документации производителя оборудования по настройке контроля доступа: RADIUS, TACACS+, SNMP.

Политики аутентификации на основе

- Источника запроса
- Типа подключения (проводной, беспроводной, VPN)
- Параметров беспроводной сети (SSID)
- Протокола подключения
- RADIUS-атрибута
- Профилирования по MAC адресу, таблицам MAC, вендору, DHCP, CDP, LLDP, SNMP, NMAP проберам и сенсорам
- Совпадения в полях Serial, DN, SAN, Issuer полей TLS-сертификата
- Членства пользователя в домене Windows или FreeIPA, доменной группе, атрибута

Политики авторизации

- Назначение VLAN, ACL, загружаемых ACL (с их редактором), лимитов объёма и скорости трафика, произвольных RADIUS-атрибутов
- Контроль числа эндпоинтов на учётную запись
- Редирект на гостевой портал
- Помещение эндпоинтов в карантин для утверждения по результатам профилирования
- Интеграция с системой пост-авторизационных проверок состояния эндпоинта через сервер и агента «Сакура»

Удостоверяющий центр

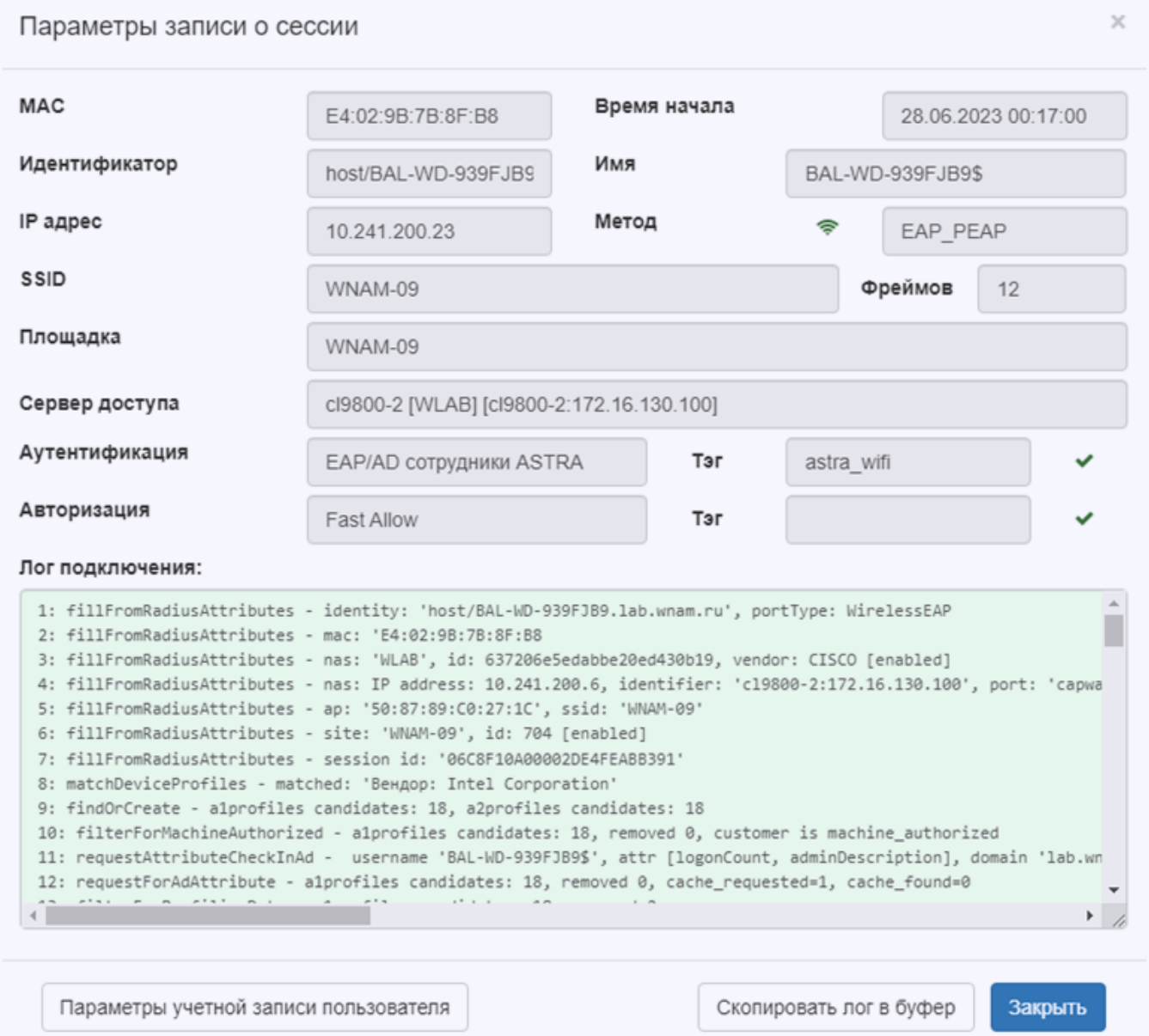
- Встроенный УЦ с созданием корневого, подчинённого УЦ и сертификата для EAP-подключений
- Подключение любого числа доверенных корневых или подчинённых УЦ
- Создание запроса на подпись сертификата, и его последующий импорт
- Выписывание пользовательских сертификатов администратором, или через веб-портал самообслуживания
- Выписывание пользовательских сертификатов в УЦ предприятия через SCEP

Взаимодействие со службой каталогов

- Получение списка доменных групп (с фильтром) для обработки правил аутентификации
- Запрос принадлежности пользователя к доменной группе
- Защищённая проверка пароля пользователя при EAP-PEAP/MSCHAPv2 подключении
- Поддержка взаимодействия с несколькими доменами одновременно

Гостевая авторизация

- Перенаправление неавторизованных устройств на портал для проведения их идентификации
- Авторизация по СМС, звонку, ваучерам, порталу Госуслуги и т.п.
- Конструктор демонстрируемых абоненту сети страниц
- Возможности проведения рекламных кампаний, опросов
- Множественные отчёты
- Интеграция с COPM



Контроль доступ к оборудованию

- Проверка источника подключения
- Проверка пароля и прав администратора в локальной базе данных, или в домене
- Назначение списка запрещенных и разрешенных к выполнению команд

Логирование и отчетность

- Протоколирование всех сессий корпоративных подключений с детальным логированием всех шагов проверки правил аутентификации и авторизации
- Уведомление внешней системы (например SIEM) о событиях авторизации, конфигурирования по протоколам SNMP и Syslog
- Хранение сессий подключения со статистикой по трафику
- Отчёты по источнику, политикам подключений, списки эндпоинтов
- Поиск сессий подключения к оборудованию, в том числе по отправленным ему конфигурационным командам

ЛИЦЕНЗИРОВАНИЕ

Программное обеспечение WNAM лицензируется по общему числу подключающихся устройств (эндпоинтов), кроме гостевых, поставляется с бессрочной лицензией, не требующих подписок и использования облачных технологий. Производитель WNAM, совместно с компаниями-партнёрами, оказывает услуги по проектированию, внедрению, кастомизации последующей и технической поддержке системы корпоративной сетевой авторизации.

СПИСОК ПАРТНОМЕРОВ

№	Партномер	Наименование
1	WNAM-1.6-BASE	Базовая лицензия программного обеспечения WNAM версии 1.6 для установки на одном сервере, брендирование включено
2	WNAM-1.6-CA	Дополнительная лицензия на поддержку корпоративных методов авторизации 802.1x
3	WNAM-1.6-X100	Дополнительная лицензия на пакет 100 эндпоинтов корпоративной авторизации
4	WNAM-1.6-X1K	Дополнительная лицензия на пакет 1000 эндпоинтов корпоративной авторизации
5	WNAM-1.6-XS1K	Дополнительная лицензия на пакет 1000 одновременно работающих эндпоинтов корпоративной авторизации
6	WNAM-1.6-X10K	Дополнительная лицензия на пакет 10 тысяч эндпоинтов корпоративной авторизации
7	WNAM-1.6-X100K	Дополнительная лицензия на пакет 100 тысяч эндпоинтов корпоративной авторизации
8	WNAM-1.6-TACPLUS-10	Дополнительная лицензия на поддержку авторизации доступа к оборудованию по протоколу TACACS+, 10 устройств
9	WNAM-1.6-TACPLUS-100	Дополнительная лицензия на поддержку авторизации доступа к оборудованию по протоколу TACACS+, 100 устройств
10	WNAM-1.6-TACPLUS-1K	Дополнительная лицензия на поддержку авторизации доступа к оборудованию по протоколу TACACS+, 1000 устройств
11	WNAM-1.6-TACPLUS-10K	Дополнительная лицензия на поддержку авторизации доступа к оборудованию по протоколу TACACS+, 10 тысяч устройств
12	WNAM-1.6-LOC1	Дополнительная лицензия на 1 площадку предоставления услуги Wi-Fi
13	WNAM-1.6-LOC10	Дополнительная лицензия на 10 площадок предоставления услуги Wi-Fi
14	WNAM-1.6-LOC100	Дополнительная лицензия на 100 площадок предоставления услуги Wi-Fi
15	WNAM-1.6-AP1	Дополнительная лицензия на 1 точку доступа Wi-Fi
16	WNAM-1.6-AP10	Дополнительная лицензия на 10 точек доступа Wi-Fi
17	WNAM-1.6-AP100	Дополнительная лицензия на 100 точек доступа Wi-Fi
18	WNAM-1.6-CLUSTER	Дополнительная лицензия на функционал организации отказоустойчивого кластера Системы типа «active-active». Требуется вторая базовая лицензия
19	WNAM-SUPP1Y-BASE	Сертификат на удаленную базовую постгарантийную техническую поддержку Системы в течение одного года с правом обновления до текущей актуальной версии Системы **

СПИСОК ПАРТНОМЕРОВ

№	Партномер	Наименование
20	WNAM-SUPP1Y-ADV	Сертификат на удалённую расширенную постгарантийную техническую поддержку Системы в течение одного года с администрированием Системы и правом обновления до текущей актуальной версии Системы **
21	WNAM-1.6-CA-SUPP1Y	Техническая поддержка ядра системы WNAM с модулем корпоративной авторизации, на 1 год
22	WNAM-1.6-X-SUPP1Y	Техническая поддержка лицензии на пакет ... эндпоинтов корпоративной авторизации, на 1 год
23	WNAM-1.6-TACPLUS-SUPP1Y	Техническая поддержка лицензии на авторизацию доступа к оборудованию по протоколу TACACS+, ... устройств, на 1 год

РАЗВИТИЕ

В 2023 году запланированы следующие работы по совершенствованию возможностей системы корпоративной авторизации WNAM, а именно:

- Усиление поддержки временной изолированной работы узла авторизации на удаленном объекте кластера
- Возможность гибкого редактирования политик аутентификации с использованием логических выражений
- Возможность гибкой настройки внешнего вида таблиц пользователей, сессий и ряда отчетов
- Настройка выбора сертификата RADIUS-сервера в зависимости от источника запроса
- Контроль привязки эндпоинта к порту ЛВС, к которому он подключается
- Профилирование эндпоинта на основе NMAP-сканирования открытых портов
- Настраиваемые Пороги событий и уведомления

NETAMS
www.netams.com
info@netams.com
+7 (499) 346-76-60