Процесс пилотного внедрения AxelNAC на проекте

В данном документе описаны процессы пилотного внедрения системы контроля доступа к сети AxelNAC на проектах.

Стартовая встреча по пилотному внедрению

В рамках стартовой встречи необходимо узнать:

1. Функциональные сценарии, для которых заказчику необходим AxelNAC;
2. Какое оборудование будет использоваться у заказчика (например, заказчик использует одинаковое количество устройств Cisco и HP: для такого пилотного внедрения будет необходимо использовать не только известный и понятный коммутатор Cisco, но и коммутатор производства HP);
3. Под управлением какой ОС используются АРМ пользователей заказчика;
4. Если заказчик использует Wi-Fi для доступа к сети, необходимо уточнить производителя WLC;
5. Если заказчик хочет обеспечить защищенное подключение пользователей по протоколу EAP-TLS, необходимо уточнить какой Удостоверяющий Центр (УЦ) использует заказчик. Согласен ли заказчик на интеграцию с продуктивным УЦ;
6. Если заказчик хочет обеспечить защищенное подключение пользователей по протоколу MS-CHAPv2, необходимо уточнить какой AD/LDAP-сервер использует заказчик. Согласен ли заказчик на интеграцию с продуктивным AD/LDAP-сервером.

По окончании стартовой встречи, у интегратора должны быть четкие ответы на следующие вопросы:

- Какие сценарии подключения пользователей предусмотрены заказчиком?
- Какое клиентское оборудование будет использоваться?
- Какой УЦ использует заказчик (MS, Alladin и т.д.)?
- Какой AD/LDAP-сервер использует заказчик (MS AD, Samba и т.д.)?

Запрос архитектуры

Для следующего этапа необходимо изучить и проанализировать инфраструктуру заказчика, после чего подготовить черновой вариант схемы интеграции AxelNAC с ней.

Схема интеграции должна включать в себя:

- Предоставление Virtual appliance AxelNAC;
- Процесс разворачивания узлов AxelNAC в нечетном количестве (от 3 до 9 узлов);
- Список портов взаимодействия между AxelNAC и коммутатором;
- Список портов взаимодействия между AxelNAC и пользователем;
- Список портов взаимодействия между узлами кластера AxelNAC;
- Список портов взаимодействия с AD;
- Список портов взаимодействия с УЦ (если используется SCEP);
- VLAN для продуктивной сети;
- VLAN для изоляционной сети;
- VLAN для голосовой сети (если в требованиях присутствует проверка голосовых устройств);
- VLAN для сети исправления;
- VLAN для сети конкретного оборудования (если обозначено в требованиях);
- В каждом из запрошенных VLAN необходимо настроить ip helper в сторону VIP-адреса AxelNAC;
- Ноутбук с возможностью подключения двух и более сетевых интерфейсов (например, проводное + беспроводное соединение или проводное + проводное соединение) с указанием на схеме, и доступом к приложениям **RDP, PS, SSH, Wireshark**;
- Рабочая станция для инженера с приложениями для доступа через **SSH, RDP, Telnet, веб-браузер, Wireshark**.

Для корректного перемещения пользователей между VLAN необходимо иметь работающий DHCP-сервер в каждом VLAN.

Запрос доступов

Для следующего шага необходимо убедиться, что все оборудование корректно сконфигурировано и имеет все необходимые доступы.

Тестируемый ноутбук под управлением ОС Windows:

1. Необходимо создать локальную учетную запись с правами локального администратора;
2. Созданный пользователь должен иметь права изменять настройки сетевых интерфейсов;
3. Созданный пользователь должен иметь права изменять настройки службы **winrm**;
4. Созданный пользователь должен иметь права на запуск и использование приложений **RDP, SSH, Wireshark, telnet**;
5. Необходимо разрешить обращение пользователя на DNS-имена описанные в таблице 3;
6. Необходимо разрешить взаимодействие на портах TCP 80, 443, 5985 до всех узлов AxelNAC.

Тестируемый ноутбук под управлением Linux-систем:

1. Необходимо создать локальную учетную запись с правами на изменение настроек сетевого интерфейса;
2. Созданный пользователь должен иметь права изменять настройки сетевых интерфейсов;
3. Созданный пользователь должен иметь права на запуск и использование приложений SSH, tcpdump, telnet;
4. Созданный пользователь должен иметь возможность удаленного подключения по рекомендованному приложению

вендора Linux-системы.

Рабочая станция для инженера:

1. Необходимо запросить доступ по протоколу **HTTPS** до веб-интерфейса управления на все узлы AxelNAC через порт TCP 1443;
2. Необходимо запросить доступ по протоколу **SSH** до терминала управления на все узлы AxelNAC через порт TCP 22;
3. Необходимо запросить доступ по протоколу **RDP** во всех VLAN, используемых в пилотном внедрении, если тестируемое устройство — ноутбук под управлением ОС Windows;
4. Необходимо иметь возможность удаленного подключения по рекомендованному приложению вендора Linux-системы к тестируемому устройству под управлением Linux-системы;
5. Необходимо иметь возможность подключения по протоколу SSH к тестируемому устройству под управлением ОС Linux через порт TCP 22.

Коммутатор, WLC, AP, NGFW:

1. Необходимо создать пользователя на сетевом устройстве с наивысшим уровнем привилегий в системе. Если заказчик хочет настроить оборудование сам, необходимо запросить права на просмотр, чтобы найти ошибки в конфигурации при сбоях;
2. Необходимо настроить доступ по протоколу **SSH** до сетевого устройства от рабочей станции под управлением ОС Windows для инженера;
3. Сетевое устройство должно иметь сетевую связность между всеми узлами AxelNAC, тестируемыми устройствами, рабочей станцией под управлением ОС Windows для инженера;
4. Необходимо запросить сетевую связность VLAN, описанных в архитектуре между коммутатором и тестовой архитектурой;
5. Запросить DHCP во VLAN, описанных в архитектуре.

Проверка доступов

После того, как все доступы запрошены и первоначальная конфигурация выполнена, необходимо выполнить проверку доступов на всех устройствах, которые входят в архитектуру для пилотного внедрения.

Тестируемый ноутбук под управлением ОС Windows:

1. Необходимо проверить, что созданная заказчиком учетная запись имеет права локального администратора;
2. Необходимо проверить, что пользователь имеет право изменять настройки сетевого интерфейса и запускать сервис проводной автонастройки;
3. Необходимо проверить, что пользователь имеет право на изменение глобальных параметров службы **winrm**, изменение способов аутентификации, доверенных хостов, параметра защищенности подключения;
4. Необходимо проверить, что на АРМ установлено приложение telnet, позволяющее строить TCP-сессии на выбранный порт;
5. Необходимо проверить, что на АРМ разрешено удаленное подключение по протоколу **RDP** на порт TCP 3389 или другой порт, разрешенный заказчиком;
6. Необходимо проверить, что на АРМ установлено и запускается приложение **Wireshark**, при этом нет ограничений на захват трафика с сетевых интерфейсов;
7. Необходимо проверить, что пользователь разрешает DNS-имена командой nslookup;
8. Необходимо проверить, что у пользователя есть сетевая связность между AxelNAC, и проверка командойtelnet со стороны host → AxelNAC корректно отрабатывает на порты 80, 443. Проверка командой telnet со стороны AxelNAC → host 5985 (в случае настроенного прослушивателя WinRM) должна отрабатывать идентично.

Тестируемый ноутбук под управлением Linux-систем:

1. Необходимо проверить, что заказчиком создана учетная запись, вы имеете право зайти в сеть под этим пользователем;
2. Необходимо проверить, что пользователь может изменять настройки сетевого интерфейса;
3. Необходимо проверить, что пользователь должен имеет право запускать и использовать приложения **SSH, tcpdump, telnet**;
4. Необходимо убедиться, что вы можете удаленно подключиться к пользователю;
5. Необходимо проверить, что открыт доступ до пользователя по протоколу **SSH**.

Рабочая станция для инженера:

1. Необходимо проверить, что открыт доступ по протоколу **HTTPS** до веб-интерфейса управления на все узлы AxelNAC через порт TCP 1443;
2. Необходимо проверить, что открыт доступ по протоколу **SSH** до терминала управления на все узлы AxelNAC через порт TCP 22;
3. Необходимо проверить, что открыт доступ по протоколу **RDP** во всех VLAN, используемых в пилотном внедрении, если тестируемое устройство — ноутбук под управлением ОС Windows;
4. Необходимо проверить, что имеется возможность удаленного подключения по рекомендованному приложению Linux-вендора к тестируемому устройству под управлением Linux-системы;
5. Необходимо проверить, что имеется возможность подключения по протоколу **SSH** к тестируемому устройству под управлением Linux-системы через порт TCP 22.

Коммутатор, WLC, AP, NGFW:

1. Необходимо убедиться, что пользователь создан на сетевом устройстве с наивысшим уровнем привилегий в системе;
2. Необходимо убедиться, что имеется доступ по протоколу **SSH** до сетевого устройства от рабочей станции под управлением ОС Windows для инженера;
3. Необходимо убедиться, что сетевое устройство имеет сетевую связность между всеми узлами AxelNAC, тестируемыми

устройствами, рабочей станцией под управлением ОС Windows для инженера;
4. Необходимо убедиться, что есть сетевая связность VLAN, описанных в архитектуре между коммутатором и тестовой архитектурой;
5. Необходимо убедиться, что в запрошенных VLAN корректно работает DHCP. Адреса выдаются в соответствии с запрошенной подсетью.

Приложение 1. Таблицы взаимодействия AxelNAC

Взаимодействие AxelNAC ⟷ AxelNAC

В данном разделе приведены таблицы взаимодействия узлов AxelNAC.

Таблица 1.1 — Доступ к SSH

TCP	22

Таблица 1.2 — MariaDB

TCP	3306
TCP	3307

Таблица 1.3 — Высокая доступность

UDP	4253
TCP	4444
TCP	4567
TCP	4568
TCP	7890
TCP	7891
UDP	5405
UDP	5407
TCP	7788
UDP	694
TCP	2224
TCP	3121
TCP	21064

Таблица 1.4 — MANAGEMENT-IF

TCP	9090
TCP	7070
TCP	9999

TCP	1444
TCP	9292
UDP	2056
TCP	19999
TCP	23001-23256

Таблица 1.5 — HAproxy-stats

TCP	1025
TCP	1026

Таблица 1.6 — RADIUS

TCP	1812
UDP	1812
TCP	1813
UDP	1813
TCP	1815
UDP	1815
TCP	2083

Таблица 1.7 — FingerStorage

UDP	1192

Таблица 1.8 — Syslog

UDP	514

Взаимодействие AxelNAC ⟷ Сетевое устройство

В данном разделе приведены таблицы взаимодействия AxelNAC с сетевыми устройствами.

Таблица 2.1 — RADIUS

TCP	1812
UDP	1812
TCP	1813
UDP	1813

UDP	3799 (данный порт обычно используется, как CoA-порт. Настройки можно изменить на коммутаторе.)
UDP	1700

Таблица 2.2 — SNMP

UDP	162
UDP	161

Таблица 2.3 — SSH/Telnet

TCP	22
TCP	23

Таблица 2.4 — HTTP/HTTPS

TCP	80
TCP	443
TCP	8443

Взаимодействие AxelNAC ⟷ Пользователь

В данном разделе приведены таблицы взаимодействия AxelNAC с пользователем.

Таблица 3.1 — HTTP/HTTPS

TCP	80
TCP	443
TCP	1443 (Данный порт является управляющим интерфейсом AxelNAC и необходим для открытия при использовании спонсорского портала.)

Таблица 3.2 — WinRM

TCP	5985
TCP	5986

Взаимодействие AxelNAC ⟷ Active Directory

В данном разделе приведены таблицы взаимодействия AxelNAC с каталогом Active Directory.

Таблица 4.1 — NTP

UDP	123

Таблица 4.2 — LDAP

UDP	389

TCP	389

Взаимодействие AxelNAC ⟷ Центр сертификации (CA)

В данном разделе приведены таблицы взаимодействия AxelNAC с центром сертификации (CA)

Таблица 5.1 — SCEP

TCP	443
TCP	80

Взаимодействие Пользователь ⟷ Active Directory

В данном разделе приведены таблицы взаимодействия пользователей с каталогом Active Directory.

Таблица 6.1 — DNS

UDP	53
TCP	53

Таблица 6.2 — NTLM/LDAP

UDP	389
TCP	389

Таблица 6.3 — DHCP

UDP	67
UDP	68

Взаимодействие AxelNAC ⟷ Интерфейс управления

В данном разделе приведены таблицы взаимодействия AxelNAC с интерфейсом управления.

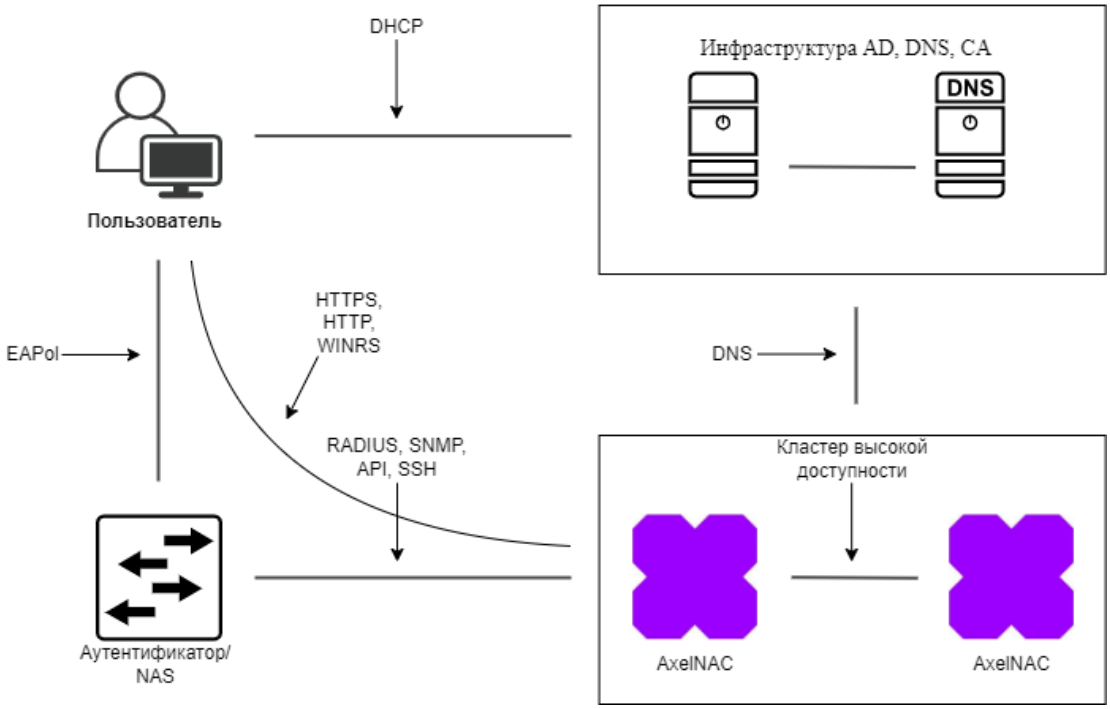
Таблица 7.1 — HTTPS

TCP	1443
TCP	8080

Таблица 7.2 — Portal HTTP

TCP	80
TCP	443

Приложение 2. Пример схемы интеграции AxelNAC с инфраструктурой заказчика



ID статьи: 16
Последнее обновление: 14 июн., 2024
Обновлено от: Егоров В.
Ревизия: 10
База знаний AxelNAC -> Документация -> Процесс пилотного внедрения AxelNAC на проекте
https://docs.axel.pro/entry/16/