ASA 8. x руководство по развертыванию политиков динамического доступа (DAP)

Содержание

Введение

Шлюзы VPN работают в динамических средах. Каждое VPN-подключение зависит от множества переменных, например, от часто меняющихся конфигураций интрасети, различных ролей каждого пользователя в организации и входа в систему с удаленных объектов с различными конфигурациями и уровнями безопасности. Задача наделения пользователей полномочиями в динамической среде VPN намного сложнее, чем в сети со статической конфигурацией.

Динамическая политика доступа (DAP) — новая функция, представленная в выпуске программного обеспечения для устройств адаптивной защиты (ASA) 8.0, позволяет настроить авторизацию в соответствии с динамическим характером VPN-окружений. Динамическая политика доступа создается путем задания набора атрибутов управления доступом, которые связываются с определенным пользовательским туннелем или сеансом. Эти атрибуты решают проблемы членства в нескольких группах и безопасности оконечных устройств.

Например, устройство защиты может предоставить конкретному пользователю доступ для конкретного сеанса исходя из определенной политики. Во время аутентификации пользователя оно формирует политику DAP, выбирая и/или объединяя атрибуты из одной или нескольких записей DAP. Выбор записей DAP производится на основе сведений о безопасности удаленного оконечного устройства и/или данных авторизации AAA для пользователя, прошедшего аутентификацию. Затем запись DAP начинает действовать для пользовательского туннеля или сеанса.

Примечание: *dap.xml* файл, который содержит атрибуты выбора политики DAP, хранится во флэш-памяти ASA. Несмотря на то, что файл dap.xml можно экспортировать из системы, редактировать (при условии знания синтаксиса XML) и импортировать обратно, в этом случае необходима предельная осторожность, поскольку при ошибках в настройке ASDM прекратит обрабатывать записи DAP. Эта часть настройки не может выполняться через

интерфейс командной строки.

Примечание: *При попытке настройки параметров dynamic-access-policy-record access в интерфейсе командной строки DAP может перестать работать, в то время как ASDM обработает такую ситуацию корректно.* Для управления политикой DAP следует во всех случаях избегать CLI в пользу ASDM.

Атрибуты DAP и AAA

Дополняя службы AAA, DAP предусматривает ограниченный набор атрибутов авторизации, которые могут действовать взамен атрибутов AAA. Устройство защиты может выбирать записи DAP на основе сведений авторизации AAA для конкретного пользователя. Руководствуясь этими сведениями, устройство защиты может выбрать сразу несколько записей DAP, в дальнейшем объединить их для назначения атрибутов авторизации DAP.

Можно определить атрибуты AAA из иерархии атрибутов AAA Cisco или из полного набора атрибутов ответа, которые устройство защиты получает от сервера RADIUS или LDAP, как показано на рис. 1.

Рис. 1. DAP графический интерфейс для атрибутов AAA в DAP

DAP и атрибуты безопасности оконечных устройств

В дополнение к атрибутам AAA устройство защиты может также получать атрибуты безопасности оконечных устройств путем настраиваемых методов оценки состояния. Как показано на рис. 2, к этим методам относятся: базовое сканирование хостов, защищенная настольная система, стандартная/расширенная оценка оконечных устройств и управление допуском к сети (NAC). Получение атрибутов оценки оконечных устройств и их отправка устройству защиты происходят до аутентификации пользователя. Тем не менее, во время аутентификации пользователя подтверждаются атрибуты AAA, включая полную запись DAP.

Рис. 2. Графический интерфейс атрибутов оконечного устройства

Динамическая политика доступа по умолчанию

До возникновения и реализации DAP определение пар «атрибут —значение» для политики доступа, связываемых с конкретным пользовательским туннелем или сеансом, происходило либо локально на устройстве ASA (т. е. посредством групп туннелей и групповых политик), либо с привязкой через внешние серверы AAA. В выпуске 8.0 появилась возможность настройки DAP в дополнение или взаимен политик локального и внешнего доступа.

По умолчанию DAP действует всегда. Однако для администраторов, предпочитающих старый способ реализации политики, например, путем управления доступом через группы туннелей, групповые политики и AAA без реализации DAP в явном виде, старые механизмы по-прежнему доступны. Как видно на рис. 3, для реализации старых механизмов не требуется изменять конфигурацию функции DAP, включая запись DAP по умолчанию, DfltAccessPolicy.

Рис. 3. Динамическая политика доступа по умолчанию

Тем не менее, при изменении любого из значений по умолчанию в записи DAP, например,

изменении параметра «Action:» (Действие): в DfltAccessPolicy с исходного значения на «Terminate» (Прерывание) в отсутствие иных настроенных записей DAP пользователи, прошедшие аутентификацию, будут по умолчанию подпадать под условия записи DAP DfltAccessPolicy и не получат доступа к VPN.

Следовательно, необходимо создать и настроить одну или несколько записей DAP, чтобы разрешить установление соединения VPN и определить состав сетевых ресурсов, к которым разрешен доступ прошедшему аутентификацию пользователю. При этом настроенная запись DAP будет иметь приоритет над старой реализацией политики.

Настройка динамической политики доступа

В случае использования DAP для определения состава сетевых ресурсов, доступных пользователю, требуется принимать во внимание множество параметров. Например, нужно определить, относится ли подключающееся оконечное устройство к управляемой, неуправляемой или недоверенной среде, установить критерии выбора для определения подключающегося оконечного устройства и, опираясь на оценку оконечного устройства и/или параметры доступа AAA, указать, к каким сетевым ресурсам будет разрешен доступ подключающемуся пользователю. Предварительно необходимо ознакомиться с возможностями и функциями DAP, показанными на рис. 4.

Рис. 4. Динамическая политика доступа

При настройке записи DAP следует обратить внимание на два основных компонента:

- Критерии отбора, включая дополнительные параметры
- Атрибуты политики доступа

В разделе критериев отбора администратор настраивает атрибуты AAA и оконечных устройств для выбора определенной записи DAP. Запись DAP используется в тех случаях, когда атрибуты авторизации пользователя соответствуют критериям атрибутов AAA и все атрибуты оконечных устройств удовлетворяют условиям.

Например, при выборе: LDAP (Active Directory) выбран, строка Названия атрибута является memberOf, и строка Значения является Подрядчиками, как показано на рисунке 5a, аутентифицирующийся пользователь должен быть участником Подрядчиков Группы Active Directory для соответствия с критериями атрибута AAA.

В дополнение к удовлетворению критериев атрибутов AAA проходящий аутентификацию пользователь должен также соответствовать критериям атрибутов оконечного устройства. Например, если администратор настроил Cisco Secure Desktop (CSD) для определения состояния подключаемого оконечного устройства и по результатам определения состояния оконечное устройство было отнесено к неуправляемым местоположениям CSD, то администратор может использовать эти сведения оценки в качестве критериев отбора для атрибута оконечного устройства, как показано на рис. 5б.

Рис. 5a. Критерии атрибутов AAA Рис. 5b. Критерии атрибутов оконечного устройства

Таким образом, для соответствия записи DAP, показанной на рис. 6, проходящий аутентификацию пользователь должен быть членом группы Active Directory «Contractors», а его оконечное устройство, используемое для подключения, для назначения записи DAP должно отвечать значению политики CSD «Unchanged» (Без изменения).

Рис. 6. Критерии AAA и критерии атрибутов оконечного устройства совпадают

Создавать атрибуты AAA и оконечного устройства можно при помощи таблиц, как показано на рис. 6, и/или через указание логического выражения в разворачивающемся разделе Advanced (Дополнительно), как показано на рис. 7. В настоящее время логическое выражение создается функциями EVAL, например EVAL (endpoint.av.McAfeeAV.exists,"EQ","true","string") и EVAL (endpoint.av.McAfeeAV.description,"EQ","McAfee VirusScan Enterprise","string"), которые представляют логические операции выбора AAA и/или оконечного устройства.

Логические выражения полезны для добавления критериев отбора, недоступных в расположенных сверху областях атрибутов AAA и оконечного устройства. Например, для устройств защиты можно задать использование атрибутов AAA, отвечающих всем, любым или никаким из указанных критериев, но атрибуты оконечных устройств в этом случае дополняют друг друга и должны выполняться все целиком. Чтобы разрешить устройству защиты использовать атрибуты оконечного устройства выборочно, нужно создать соответствующие логические выражения в разделе Advanced (Дополнительно) записи DAP.

Рис. 7. Графический интерфейс логического выражения для создания атрибута в режиме Advanced

Как показано на рис. 8, в разделе Access Policy Attributes (Атрибуты политики доступа) администратор настраивает атрибуты доступа через сеть VPN для определенной записи DAP. Когда атрибуты авторизации пользователя соответствуют критериям AAA, оконечного устройства и/или логического выражения, действуют настроенные в этом разделе значения атрибутов политики доступа. Определяемые здесь значения атрибутов заменяют собой значения, получаемые от системы AAA, включая значения из существующих записей пользователей, групп, групп туннеля и групп по умолчанию.

Запись DAP имеет ограниченный набор значений атрибутов, доступных для настройки. Как показано на рис. 8–14, эти значения распределены по вкладкам:

Рис. 8. Вкладка Action (Действие) определяет особый порядок обработки для определенного подключенного или сеанса.

- Continue (Продолжать — по умолчанию) — применять атрибуты политики к сеансу.
- Terminate (Прервать) — прервать сеанс.
- User Message (Пользовательское сообщение) —введите текстовое сообщение, которое будет отображаться на странице портала при выборе этой записи DAP. Длина — не более 128 знаков. Пользовательское сообщение отображается в круге желтого цвета. При входе пользователя сообщение мигает три раза для привлечения внимания и затем остается статическим. Если выбрано несколько записей DAP, каждая из которых имеет пользовательское сообщение, то отображаются все пользовательские сообщения. Дополнительно можно включить в такие сообщения URL-адрес или другую текстовую вставку, используя соответствующие тэги HTML.

Рис. 9. Вкладка Network ACL Filters (Фильтры сетевых списков ACL) позволяет выбирать и настраивать сетевые списки контроля доступа, действующие для данной записи DAP. Список контроля доступа для DAP может содержать разрешающие или запрещающие правила, но не оба вида правил. Если ACL одновременно содержит разрешающие и запрещающие правила, то устройство защиты отклоняет конфигурацию ACL.

- Network ACL (Сетевой список контроля доступа) — этот раскрывающийся список служит для выбора настроенных ранее сетевых списков контроля доступа, добавляемых к данной записи DAP. Здесь действительны и приводятся только те списки контроля доступа, которые целиком состоят из разрешающих или запрещающих правил.

- Manage (Управление) — служит для добавления, редактирования и удаления сетевых списков контроля доступа.
- Network ACL list (Перечень сетевых списков контроля доступа) — отображает сетевые списки контроля доступа для данной записи DAP.
- Add (Добавить) — нажмите эту кнопку для добавления выбранного сетевого списка контроля доступа из раскрывающегося списка в перечень справа.
- Delete (Удалить) — нажмите эту кнопку для удаления выделенного сетевого списка контроля доступа из перечня списков. Нельзя удалить ACL, если он назначен записи DAP или иной записи.

Рис. 10. Вкладка Web-Type ACL Filters (Фильтры списков ACL web-типа) позволяет выбирать и настраивать списки контроля доступа web-типа, действующие для данной записи DAP. Список контроля доступа для DAP может содержать только разрешающие или запрещающие правила. Если ACL одновременно содержит разрешающие и запрещающие правила, то устройство защиты отклоняет конфигурацию ACL.

- Web-Type ACL (Список контроля доступа web-типа) — этот раскрывающийся список служит для выбора настроенных ранее списков контроля доступа web-типа, добавляемых к данной записи DAP. Здесь действительны и приводятся только те списки контроля доступа, которые целиком состоят из разрешающих или запрещающих правил.
- Управляйте... — служит для добавления, редактирования и удаления списков контроля доступа web-типа.
- Web-Type ACL list (Перечень контроля доступа web-типа) — отображает списки контроля доступа web-типа для данной записи DAP.
- Add (Добавить) — нажмите эту кнопку для добавления выбранного списка контроля доступа web-типа из раскрывающегося списка в перечень справа.
- Delete (Удалить) — нажмите эту кнопку для удаления выделенного списка контроля доступа web-типа из перечня. Нельзя удалить ACL, если он назначен записи DAP или иной записи.

Рис. 11. Вкладка Functions (Функции) позволяет настраивать ввод и обзор файловых серверов, а также прокси-сервера HTTP и ввод URL-адреса для записи DAP.

- File Server Browsing (Обзор файловых серверов) — разрешает или запрещает обзор CIFS для файловых серверов или ресурсов совместного доступа.
- File Server Entry (Ввод файлового сервера) — разрешает или запрещает пользователю вводить пути и имена файловых серверов на странице портала. В разрешенном состоянии на странице портала размещается секция записи файлового сервера. Пользователи могут ввести непосредственные имена путей к файлам Windows. Они могут загружать, редактировать, удалять, переименовывать и перемещать файлы. Они также могут добавлять файлы и папки. Ресурсы совместного доступа также требуется настраивать для доступа пользователей к соответствующим серверам Microsoft Windows. В зависимости от требований сети, перед доступом к файлам может потребоваться аутентификация пользователей.
- HTTP Proxy (Прокси-сервер HTTP) — влияет на пересылку апплета прокси-сервера HTTP клиенту. Прокси-сервер полезен для технологий, конфликтующих с надлежащим преобразованием содержимого, например, Java, ActiveX и Flash. Эта функция обходит процесс преобразования/перезаписи, обеспечивая постоянное использование устройства защиты. Пересылаемый прокси-сервер автоматически изменяет старую

конфигурацию прокси-сервера в браузере и переадресовывает все запросы HTTP и HTTPS прокси-серверу в новой конфигурации. Он поддерживает практически все технологии на стороне клиента, включая HTML, CSS, JavaScript, VBScript, ActiveX и Java. Единственный поддерживаемый браузер — Microsoft Internet Explorer.
- URL Entry (Ввод URL-адреса) — разрешает или запрещает пользователю вводить URL-адреса HTTP/HTTPS на странице портала. Когда эта функция включена, пользователи могут вводить web-адреса в поле URL-адреса и обращаться к соответствующим web-сайтам по бесклиентской сети VPN на основе SSL.
- Unchanged (Без изменений — по умолчанию). Выберите этот параметр, чтобы использовать значения из групповой политики, действующей для этого сеанса.
- Enable/Disable (Включение/отключение) — выберите этот параметр для включения или отключения функции.
- Auto-start (Автозапуск) — выберите этот параметр, чтобы разрешить прокси-сервер HTTP и задать для записи DAP автоматический запуск апплетов, связанных с этими функциями.

Рис. 12. Вкладка Port Forwarding Lists (Списки переадресации портов) позволяет выбирать и настраивать списки переадресации портов для пользовательских сеансов.

- Port Forwarding (Переадресация портов) — выберите режим, который будет действовать для списков переадресации портов в этой записи DAP. Другие атрибуты в этом поле допускаются только при установке параметра Port Forwarding (Переадресация портов) в значение Enable (Включено) или Auto-start (Автозапуск).
- Unchanged. Выберите этот параметр, чтобы использовать значения из групповой политики, действующей для этого сеанса.
- Enable/Disable (Включение/Отключение) — выберите этот параметр для включения или отключения переадресации портов.
- Auto-start (Автозапуск) — выберите этот параметр, чтобы разрешить переадресацию портов и задать для записи DAP автоматический запуск апплетов, связанных с ее списками переадресации портов.
- Port Forwarding List (Список переадресации портов) — в этом раскрывающемся списке выберите один из настроенных списков переадресации портов для добавления в запись DAP.
- New (Создать) — для настройки новых списков переадресации портов нажмите эту кнопку.
- Port Forwarding Lists (Списки переадресации портов) — отображает список переадресации портов для записи DAP.
- Add (Добавить) — нажмите эту кнопку для добавления выбранного списка переадресации портов из раскрывающегося списка в перечень списков переадресации портов справа.
- Delete (Удалить) — нажмите эту кнопку, чтобы удалить выбранный список переадресации портов из перечня. Нельзя удалить ACL, если он назначен записи DAP или иной записи.

Рис. 13. Вкладка Bookmarks (Закладки) позволяет выбирать и настраивать списки закладок/URL-адресов для пользовательских сеансов.

- Enable bookmarks (Включить закладки) — отметьте этот флажок для разрешения закладок. Когда флажок снят, список закладок на странице портала для подключения не приводится

- Manage (Управление) — служит для добавления, импорта, экспорта и удаления списков закладок.
- Bookmarks Litss (Списки Закладок) — раскрывающийся список с перечнем закладок для записи DAP.
- Add (Добавить) — нажмите эту кнопку для добавления выбранного списка закладок из раскрывающегося списка в перечень списков закладок справа.
- Delete (Удалить) — нажмите эту кнопку, чтобы удалить выбранный список закладок из перечня. Нельзя удалить перечень закладок из устройства защиты, не удалив его предварительно это из записей DAP.

Рис. 14. Вкладка Method (Метод) позволяет настроить разрешенный тип удаленного доступа.

- Unchanged (Без изменений) — продолжает использоваться текущий метод удаленного доступа, заданный в групповой политике для сеанса.
- AnyConnect Client (Клиент AnyConnect) — подключение выполняется с использованием VPN-клиента Cisco AnyConnect.
- Web-Portal (Web-портал) — подключение выполняется посредством бесклиентской сети VPN.
- Both-default-Web-Portal — подключение выполняется через бесклиентскую сеть или клиент AnyConnect; по умолчанию используется бесклиентская сеть.
- Both-default-AnyConnect Client — подключение выполняется через бесклиентскую сеть или клиент AnyConnect; по умолчанию используется клиент AnyConnect.

Как упоминалось ранее, запись DAP имеет ограниченный набор значений атрибутов по умолчанию, и только в случае их изменения они приобретают приоритет над существующими записями AAA, пользователей, групп, групп туннелей и групп по умолчанию. Если требуются значения атрибутов, выходящие за рамки DAP, например, списки раздельного туннелирования, баннеры, интеллектуальные туннели, настройки портала и т. п., то их необходимо реализовывать посредством записей AAA, пользователей, групп, групп туннелей и группы по умолчанию. В этом случае данные конкретные значения атрибутов будут дополнять, но не заменять DAP. Таким образом, пользователь получит дополняющий набор значений атрибутов во всех записях.

Объединение нескольких динамических политик доступа

Администратор может настроить несколько записей DAP для охвата нескольких переменных. В результате при выполнении аутентификации пользователя становится возможным обеспечить соответствие критериям атрибутов AAA и оконечных устройств из нескольких записей DAP. Как следствие, атрибуты политики доступа в разных политиках могут быть либо согласованными, либо конфликтовать. В этом случае зарегистрированный пользователь получает суммарный результат по всем совпавшим записям DAP.

Сюда также входят уникальные значения атрибутов, реализуемые записями аутентификации, авторизации, пользователей, групп, групп туннелей и групп по умолчанию. Суммарный результат атрибутов политики доступа образует динамическую политику доступа. Примеры объединенных атрибутов политики доступа перечислены ниже в таблицах. Эти примеры отражают результаты 3 объединенных записей DAP.

Атрибут действия, показанный в Таблице 1, имеет одно из двух значений: Terminate (Прервать) или Continue (Продолжить). Объединенным значением атрибута будет Terminate

(Прервать) если хотя бы в одной из выбранных записей DAP настроено значение Terminate, и Continue (Продолжить), во всех выбранных записях DAP настроено значение Continue.

Таблица 1. Атрибут Action (Действие)

Наименование атрибута	DAP 1	DAP#2	DAP#3	DAP
Действие (пример № 1)	continue	continue	continue	continue
Действие (Пример 2)	Оконечный	continue	continue	оконечный

Атрибут пользовательского сообщения, показанный в таблице 2, содержит значение строки. Объединенное значение атрибута будет представлять собой строку, составленную путем объединения значений атрибутов из отобранных записей DAP, разделенных символом перевода строки (шестнадцатеричное значение 0 x 0A). Порядок значений атрибутов в объединенной строке не представляет значимости.

Таблица 2. Атрибут User-Message (пользовательское сообщение)

Наименование атрибута	DAP 1	DAP#2	DAP#3	DAP
user-message	the quick	brown fox	Jumps over	the quick<LF>brown fox<LF>jumps over

Атрибуты разрешения бесклиентских функций (Functions), приведенные в Таблице 3, содержат одно из значений: Auto-start (Автозапуск), Enable (Включено) или Disable (Отключено). Если в любой из выбранных записей DAP настроено значение Auto-Start (Автозапуск), то объединенным значением атрибута будет Auto-start.

В отсутствие значений Auto-start в отобранных записях DAP объединенным значением атрибута будет Enable (Включено), если значение Enable настроено как минимум в одной из отобранных записей DAP.

В отсутствие значений Auto-start или Enable в отобранных записях DAP объединенным значением атрибута будет Disable (Отключено), если значение Disable настроено как минимум в одной из отобранных записей DAP.

Таблица 3. Атрибуты разрешения бесклиентских функций (Functions)

Наименование атрибута	DAP 1	DAP#2	DAP#3	DAP
port-forward	enable	отключить		enable
file-browsing	отключить	enable	отключить	enable
file-entry			отключить	отключить
http-proxy	отключить	автоматический запуск	отключить	автоматический запуск

url-entry	отключить		enable	enable

Атрибуты url-list и port-forward, показанные в таблице 4, содержат значение, представляющее собой либо строку, либо строковый список через запятую. Объединенное значение атрибута будет представлять собой строку с перечислением значений атрибутов из отобранных записей DAP через запятую. Все дублирующиеся значения атрибутов в объединенной строке удаляются. Порядок значений атрибутов в объединенной строке не представляет значимости.

Таблица 4. Атрибут списка URL-адресов и списка портов для переадресации

Наименование атрибута	DAP 1	DAP#3	DAP#3	DAP
url-list	o	b, c	o	a B C
port-forward		d, e	e, f	d, e, f

Атрибуты метода доступа указывают метод доступа клиента, разрешенный для VPN-подключений на основе SSL. Возможны следующие методы доступа: доступ только посредством клиента AnyConnect, доступ только через web-портал и доступ через клиент AnyConnect или web-портал с выбором AnyConnect или web-портала в качестве механизма доступа по умолчанию. Получаемые объединенные значения атрибутов перечислены в таблице 5.

Таблица 5. Атрибуты метода доступа

Выбранные значения атрибута				Результат объединения
AnyConnect Client	Web-Portal	Both-default-Web-Portal	Both-default-AnyConnect Client	
			X	Both-default-AnyConnect Client
		X		Both-default-Web- Portal
		X	X	Both-default-Web- Portal
	X			Web- Portal
	X		X	Both-default-AnyConnect Client
	X	X		Both-default-Web- Portal
	X	X	X	Both-default-Web- Portal
X				AnyConnect Client
X			X	Both-default-AnyConnect

				Client
X		X		Both-default-Web- Portal
X		X	X	Both-default-Web- Portal
X	X			Both-default-Web- Portal
X	X		X	Both-default-AnyConnect Client
X	X	X		Both-default-Web- Portal
X	X	X	X	Both-default-Web- Portal

При объединении атрибутов фильтра ACL сетевого типа (межсетевой экран) и web-типа (бесклиентский доступ) двумя основными компонентами, требующими внимания, являются атрибуты фильтра ACL: DAP Priority (Приоритет DAP) и DAP ACL (Список контроля доступа DAP).

Атрибут приоритета, как показано на рис. 15, не участвует в объединении. Устройство защиты использует это значение для логического упорядочения списков контроля доступа при объединении списков контроля доступа сетевого и web-типа из нескольких записей DAP. Устройство защиты приводит выстраивает записи в порядке от максимального (вверху таблицы) до минимального численного значения приоритета. Например, запись DAP со значением 4 имеет более высокий приоритет, чем запись со значением 2. Вручную отсортировать записи нельзя.

Рис. 15. Атрибут Priority показывает приоритет записи DAP.

- Policy Name (Наименование политики) — показывает имя записи DAP.
- Description (Описание) — показывает предназначение записи DAP.

Атрибут списка контроля доступа DAP поддерживает списки контроля доступа, которые соответствуют либо строгой модели ACL «белого списка», либо строгой модели «черного списка». В модели ACL «белого списка» записи списка контроля доступа определяют правила, разрешающие доступ к указанным сетям или хостам. В модели ACL «черного списка» записи списка контроля доступа определяют правила, запрещающие доступ к указанным сетям или хостам. Список контроля доступа, сочетающий разрешающие и запрещающие записи, называется несоответствующим. В случае настройки несоответствующего списка контроля доступа для записи DAP такой список будет отклонен как ошибка конфигурации, когда администратор попытается добавить запись. Если соответствовавший список контроля доступа назначен записи DAP, то любое изменение списка контроля доступа, изменяющее характеристику соответствия, будет отклонено как ошибка конфигурации.

Рис. 16. Выбор и настройка сетевых списков контроля доступа, действующих для данной записи DAP.

При выборе нескольких записей DAP атрибуты «access-lists», заданные в сетевом списке контроля доступа (для межсетевого экрана), объединяются в динамический список контроля доступа (Dynamic Access-List) для списка контроля доступа межсетевого экрана DAP. Аналогичным образом атрибуты «access-lists», заданные в списке контроля доступа web-типа (для бесклиентских подключений), объединяются в список Dynamic Access-List для

списка контроля доступа межсетевого экрана DAP. В нижеследующем примере рассматривается конкретный случай создания списка контроля доступа для межсетевого экрана DAP. В случае динамического списка контроля доступа для бесклиентского режима DAP процесс будет таким же.

Вначале ASA динамически создает уникальное имя для сетевого списка контроля доступа DAP, как показано в таблице 6.

Таблица 6. Наименование динамического списка Network-ACL для DAP

Наименование списка Network-ACL для DAP
DAP-Network-ACL-X (где X — целое число, которое увеличивается для обеспечения уникальности)

Далее ASA извлекает атрибут Network-ACL из отобранных записей DAP, как показано в Таблице 7.

Таблица 7. Сетевые списки контроля доступа

Отобранные записи DAP	Приоритет	Списки контроля доступа Network-ACL	Записи Network-ACL
DAP 1	1	101 и 102	ACL 101 содержит 4 запрещающих правила, а ACL 102 — 4 разрешающих правила
DAP 2	2	201 и 202	Список контроля доступа 201 содержит 3 разрешающих правила, а список контроля доступа 202 — 3 запрещающих правила
DAP 3	2	101 и 102	ACL 101 содержит 4 запрещающих правила, а ACL 102 — 4 разрешающих правила

После этого ASA переупорядочивает сетевые списки контроля доступа: вначале — по численному приоритету записей DAP, а затем — делая первым «черный список», если значение приоритета у двух или более отобранных записей DAP будет совпадать. Следующим шагом ASA извлекает записи Network-ACL из каждого списка Network-ACL, как показано в таблице 8.

Таблица 8. Приоритет записи DAP

Списки контроля доступа Network-ACL	Приоритет	Модель «черного» или «белого» списка контроля доступа	Записи Network-ACL
101	2	Черный список	4 запрещаю

			щих правила (DDDD)
202	2	Черный список	3 запрещающих правила (DDD)
102	2	Белый список	4 разрешающих правила (PPPP)
202	2	Белый список	3 разрешающих правила (PPP)
101	1	Черный список	4 запрещающих правила (DDDD)
102	1	Белый список	4 разрешающих правила (PPPP)

Наконец, ASA объединяет записи Network-ACL в динамически формируемый сетевой список контроля доступа и возвращает имя динамического сетевого списка контроля доступа в качестве нового сетевого списка контроля доступа, который применяется, как показано в таблице 9.

Таблица 9. Динамический список Network-ACL для DAP

Наименование списка Network-ACL для DAP	Запись Network-ACL
DAP-Network-ACL-1	DDDD DDD PPPP PPP DDDD PPPP

Реализация DAP

С точки зрения администратора, реализация DAP может быть целесообразна сразу по нескольким причинам. Предпосылками могут быть необходимость применения оценки состояния на оконечных устройствах или потребность в более детальных атрибутах AAA или политик при разрешении доступа пользователей к сетевым ресурсам. В приведенном ниже примере показана настройка DAP и соответствующих компонентов для идентификации подключаемого оконечного устройства и разрешения доступа пользователя к различным сетевым ресурсам.

Практическая демонстрация. Заказчику требовалось решение для обоснования концепции со следующими требованиями доступа через VPN:

- Способность обнаруживать и определять оконечные устройства штатных сотрудников в качестве управляемых и неуправляемых. Если оконечное устройство идентифицируется как управляемое (рабочий ПК), но не проходит требования к состоянию, то ему должно быть отказано в доступе. С другой стороны, если оконечное устройство сотрудника идентифицируется как неуправляемое (домашний ПК), то ему должен быть предоставлен бесклиентский доступ.
- Способность вызывать очистку сеансовых cookie-файлов и кэша при разрыве бесклиентского соединения.
- Способность обнаруживать приложения на управляемых оконечных устройствах сотрудников, например, McAfee AntiVirus, и контролировать их выполнение. Если приложения не существует, то оконечному устройству должно быть отказано в доступе.
- Способность использовать аутентификацию AAA для определения состава сетевых ресурсов, к которым разрешается доступ авторизованных пользователей. Устройство защиты должно поддержать аутентификацию MS LDAP, реализованную штатными средствами, и роли с членством в нескольких группах LDAP.
- Способность разрешать доступ из локальной сети к таким сетевым ресурсам, как сетевые факсы и принтеры, при «клиентском» или «сетевом» подключении.
- Способность предоставлять авторизованный гостевой доступ внештатным сотрудникам. Внештатные сотрудники и их оконечные устройства должны получать бесклиентский доступ, а их доступ к приложениям с портала должен быть ограниченным по сравнению с доступом штатных сотрудников.

В этом примере мы выполняем серию шагов настройки для выполнения требований заказчика к доступу посредством VPN. Некоторые необходимые шаги конфигурации не будут непосредственно связаны с DAP, в то время как другие этапы конфигурации относиться к DAP непосредственным образом. Устройство ASA характеризуется высокой динамичностью и адаптируется к разным сетевым средам. Как следствие, VPN-решения могут быть реализованы разными способами с одинаковым конечным результатом. В то же время избранный подход диктуется потребностями заказчиков и спецификой их окружений.

В свете ограниченного объема настоящей заметки и поставленных заказчиком требований мы будем использовать Менеджер устройств адаптивной защиты (ASDM) версии 6.0(x), а основная часть выполняемых настроек базируется на DAP. Вместе с тем мы также настроим политику локальной группы, чтобы продемонстрировать, каким образом DAP может дополнять или заменять атрибуты локальной политики. В рамках данной практической демонстрации мы предположим, что предварительно были настроены: группа серверов LDAP, список сетей раздельного туннелирования и базовые сетевые средства IP, включая пулы IP и группу серверов DefaultDNS.

Определение групповой политики. Эта настройка необходима для задания атрибутов локальной политики. Некоторые из определяемых здесь атрибутов не допускают настройки в DAP (например, локальный доступ к сети LAN). (Эта политика будет также использоваться для определения атрибутов бесклиентского и клиентского режимов).

Последовательно выберите Configuration > Remote Access VPN > Network (Client) Access > Group Policies (Конфигурация > VPN для удаленного доступа > Сетевой (клиентский) доступ > Групповые политики) и добавьте внутреннюю групповую политику следующим образом:

Рис. 17. Групповая политика определяет локальные специфические атрибуты VPN.

1. Открыв раздел по ссылке General (Общее) укажите имя групповой политики в поле Name: SSLVPN_GP.
2. В этом же разделе щелкните More Options (Дополнительные параметры) и в поле Tunneling Protocols в качестве протокола туннелирования задайте: Clientless SSLVPN (Бесклиентская сеть VPN на основе SSL). (Для замены метода доступа и управления им мы настроим DAP.).)
3. По ссылке Advanced > Split Tunneling (Дополнительно > Раздельное туннелирование) выполните следующие настройки:Рис. 18. Раздельное туннелирование позволяет указанному виду трафика (локальной сети) обходить нешифруемый туннель при подключении через клиент. Политика: Снимите флажок Inherit (Наследовать) и выберите Exclude Network List Below (Исключить указанный ниже сетевой список).Network List (Сетевой список): Снимите флажок Inherit (Наследовать) и выберите наименование списка: Local_Lan_Access. (Предполагается, что предварительно выполнялась настройка.).)
4. По ссылке Advanced > SSL VPN Client (Дополнительно > Клиент VPN на основе SSL) выполните следующие настройки:Рис. 19. Средство установки клиента VPN на основе SSL. После завершения работы VPN клиент SSL может оставаться на оконечном устройстве или может быть удален.
5. Сохранение средства установки на клиентской системе: Снимите флажок Inherit (Наследовать), затем выберите Yes (Да).
6. Нажмите кнопку OK, затем нажмите кнопку Apply (Применить).
7. Приведите в действие изменения конфигурации.

Определение профиля подключения. Эта настройка необходима для определения применяемого нами метода аутентификации AAA, например, LDAP, и применения предварительно настроенной групповой политики (SSLVPN_GP) к данному профилю подключения. Для пользователей, подключающихся посредством этого профиля, будут действовать определенные здесь атрибуты наряду с атрибутами, определенными в групповой политике SSLVPN_GP. (Этот профиль будет также использоваться одновременно для определения атрибутов бесклиентского и клиентского режимов).

Последовательно выберите Configuration > Remote Access VPN > Network (Client) Access >SSL VPN Connection Profiles (Конфигурация > VPN для удаленного доступа > Сетевой (клиентский) доступ > Профили подключений VPN на основе SSL) и выполните следующие настройки:

Рис. 20. Профиль подключения определяет атрибуты, специфические для локальной части VPN.

1. В разделе Connection Profiles (Профили подключения) отредактируйте запись DefaultWEBVPNGroup, затем по ссылке Basic (Базовая настройка) настройте следующие параметры:Authentication method: AAAAuthentication (Аутентификация) — AAA Server Group (Группа серверов AAA): LDAP (предполагается, что настройка предварительно выполнена)Client Address Assignment (Назначение адресов клиентам) — Client Address Pools (Пулы адресов клиентов): IP_Pool (предполагается, что настройка предварительно выполнена)Default Group Policy (Группа политик по умолчанию) — Group Policy (Группа политик): Выберите SSLVPN_GP
2. Приведите в действие изменения конфигурации.

Определение интерфейса IP для подключений по сети VPN на основе SSL. Эта настройка необходима для оконечной обработки клиентских и бесклиентских подключений SSL на

указанном интерфейсе.

Перед активацией клиентского/сетевого доступа на интерфейсе необходимо определить клиентский образ VPN на основе SSL.

1. Последовательно выберите Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings > Add (Конфигурация > VPN для удаленного доступа > Сетевой (клиентский) доступ > Дополнительно > VPN на основе SSL > Настройки клиента > Добавить) и добавьте следующий образ VPN-клиента на основе SSL из файловой системы флеш-памяти ASA: (Этот образ можно загрузить в разделе CCO на сайте www.cisco.com)Рис. 21. Установка клиентского образа сети VPN на основе SSL. Задается клиентский образ SSLVPN (AnyConnect), отправляемый подключающимся оконечным устройствам. anyconnect-win-2. x. xxx-k9.pkgНажмите OK, затем снова OK и Apply (Применить).
2. Последовательно выберите Configuration > Remote Access VPN > Network (Client) Access >SSL VPN Connection Profiles (Конфигурация > VPN для удаленного доступа > Сетевой (клиентский) доступ > Профили подключений VPN на основе SSL) и включите следующие параметры:Рис. 22. Интерфейс доступа к VPN на основе SSL. Задание интерфейсов для оконечной обработки подключений SSL VPN. В разделе Access Interface (Интерфейс доступа) включите параметр: «Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below» (Разрешить VPN-клиенту Cisco AnyConnect или старым VPN-клиентам на основе SSL доступ по интерфейсам, выбранным в приведенной ниже таблице).”Также в разделе Access Interfaces (Интерфейсы доступа) выберите Allow Access (Разрешить доступ) для внешнего интерфейса. (Эта конфигурация также разрешает бесклиентский доступ на внешнем интерфейсе.).)Щелкните "Применить".

Определение перечней закладок (URL-адресов) для бесклиентского доступа. Эта настройка необходима для определения web-приложения, публикуемого на портале. Мы определим 2 списка URL-адресов: один — для штатных, второй — для внештатных сотрудников.

1. Выберите Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks (Конфигурация > VPN для удаленного доступа > Бесклиентский доступ по VPN на основе SSL > Портал > Закладки), нажмите кнопку + Add (Добавить) и настройте следующие параметры:Рис. 23. Перечень закладок определяет публикуемые URL-адреса, к которым осуществляется доступ с web-портала. (Пользовательская настройка для доступа штатных сотрудников). Bookmark List Name (Наименование списка закладок): Employees (Штатные сотрудники) и нажмите кнопку Add (Добавить).Bookmark Title (Заголовок закладки): Company Intranet (Интрасеть компании)URL Value (Значение URL-адреса): http://company.resource.comНажмите кнопку OK, затем снова нажмите OK.
2. Нажмите кнопку + Add и настройте второй список закладок (список URL-адресов) следующим образом:Рис. 24. Перечень закладок. Требует пользовательской настройки для гостевого доступа. Bookmark List Name (Наименование списка закладок): Contractors (Внештатные сотрудники) и нажмите кнопку Add (Добавить).Bookmark Title (Заголовок закладки): Guest Access (Гостевой доступ)URL Value (Значение URL-адреса): http://company.contractors.comНажмите кнопку OK, затем снова нажмите OK.Щелкните "Применить".

Cisco Secure Desktop — эта конфигурация необходима для определения атрибутов оценки

оконечного устройства. В зависимости от выполнения критериев подключаемые оконечные устройства классифицируются как управляемые и неуправляемые. Оценки Cisco Secure Desktop выполняются до процесса аутентификации.

Настройка Cisco Secure Desktop и дерево принятия решений до входа в систему для местоположений Windows:

1. Последовательно выберите Configuration > Remote Access VPN > Secure Desktop Manager > Setup (Конфигурация > VPN для удаленного доступа > Secure Desktop Manager > Настройка) и выполните следующие настройки:Рис. 25. Установка образа Cisco Secure Desktop. Задается образ Cisco Secure Desktop, отправляемый подключающимся оконечным устройствам. Установите образ disk0:/securedesktop-asa-3.3.-xxx-k9.pkg с файловой системы флеш-памяти ASA.Отметьте флажок Enable Secure Desktop (Включить Secure Desktop).Щелкните "Применить".
2. Последовательно выберите Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy (Конфигурация > VPN для удаленного доступа > Secure Desktop Manager > Политика перед входом в систему) и выполните следующие настройки:Рис. 26. Дерево принятия решений перед входом в систему. Пользовательская настройка состоит в проверке файлов для различения управляемых и неуправляемых оконечных устройств. Щелкните узел Default (По умолчанию) и переименуйте метку Managed (Client Access) (Управляемое [Клиентский доступ]), затем нажмите Update (Обновить).Щелкните значок «+» в начале узла Managed (Управляемые).Для выполнения проверки выберите проверку файла (File Check) и вставьте ее кнопкой Add.В поле File Path (Путь к файлу) для условия «exists» (существует) введите C:\managed.txt, затем нажмите кнопку Update (Обновить).Выберите узел Login Denied (Отказ во входе), затем выберите Subsequence (Последующее состояние).В качестве метки введите Unmanaged (Неуправляемое) и нажмите кнопку Update (Обновить).Выберите узел Login Denied (Отказ во входе), затем выберите Location (Местоположение).В качестве метки введите Unmanaged (Clientless Access) (Неуправляемое [бесклиентский доступ]) и нажмите кнопку Update (Обновить).Выберите Apply All (Применить все).
3. Последовательно выберите Configuration > Remote Access VPN > Secure Desktop Manager > Managed (Client Access) (Конфигурация > VPN для удаленного доступа > Secure Desktop Manager > Управляемое устройство [клиентский доступ]) и выполните следующие настройки в разделе Location Settings (Настройки местоположения):Рис. 27. Настройки местоположения/конфиденциальности. Для клиентского/сетевого доступа позиции Secure Desktop (защищенное хранилище) и Cache Cleaner (очистка браузера) необязательны. Location Module (Модуль местоположения): Снимите флажки Secure Desktop и Cache Cleaner, если они установлены.При необходимости выберите Apply All (Применить все).
4. Последовательно выберите Configuration > Remote Access VPN > Secure Desktop Manager > Unmanaged (Clientless Access) (Конфигурация > VPN для удаленного доступа > Secure Desktop Manager > Неуправляемое устройство [бесклиентский доступ]) и выполните следующие настройки в разделе Location Settings (Настройки местоположения):Рис. 28. Настройки местоположения. Для бесклиентского доступа позиция Cache Cleaner (очистка браузера) обязательна, а Secure Desktop (защищенное хранилище) — нет. Location Module (Модуль местоположения): Снимите флажок Secure Desktop и отметьте флажок Cache Cleaner.Выберите Apply All (Применить все).

Углубленная оценка оконечных устройств. Эта настройка требуется в случае обязательного применения антивируса, антишпионского ПО и персонального межсетевого экрана на оконечном устройстве. Например, эта оценка позволяет проверить, выполняется ли на подключающемся оконечном устройстве антивирус McAfee. (Углубленная оценка оконечных устройств — лицензируемая функция, которая не допускает настройки при отключенной функции Cisco Secure Desktop).

Последовательно выберите Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan (Конфигурация > VPN для удаленного доступа > Secure Desktop Manager > Сканирование хостов) и выполните следующие настройки в разделе Host Scan Extensions (Расширения для сканирования хостов):

Рис. 29. Пользовательская настройка контроля за применением антивируса для клиентского/сетевого доступа.

В разделе Host Scan Extensions (Расширения для опроса хостов) настройте следующие параметры:

1. Выберите Advanced Endpoint Assessment ver 2.3.3.1, затем выберите Configure (Настроить).
2. Выберите Enforce AntiVirus (Требовать применения антивируса).
3. В раскрывающемся списке Enforce AntiVirus (Требовать применения антивируса) выберите McAfee, Inc.
4. В раскрывающемся списке AntiVirus Version (Версия антивируса) выберите McAfee VirusScan Enterprise 8.0.0.x.
5. Выберите Force File System Protection (Сделать защиту файловой системы обязательной), затем нажмите кнопку Apply All (Применить все).

Динамическая политика доступа. Эта настройка необходима для контроля подключающихся пользователей и их оконечных устройств на основании определенных критериев AAA и/или критериев оценки оконечных устройств. При выполнении заданных критериев для записи DAP подключающиеся пользователи получат доступ к сетевым ресурсам, связанным с соответствующей записью или записями DAP. Авторизация DAP выполняется в ходе процесса аутентификации.

Чтобы по умолчанию VPN-подключение на основе SSL прерывалось, например, когда оконечное устройство не соответствует ни одной из настроенных динамических политик доступа), мы настраиваем следующие параметры:

Примечание: При настройке политики динамического доступа впервые, сообщение об ошибках DAP.xml отображено, указав, что не существует файл конфигурации DAP (DAP.XML). После изменения начальной конфигурации DAP и ее последующего сохранения это сообщение более не появляется.

1. Последовательно выберите Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies (Конфигурация > VPN для удаленного доступа > Бесклиентский доступ по SSL VPN > Динамические политики доступа) и выполните следующие настройки:Рис. 30. Динамическая политика доступа по умолчанию. В отсутствие совпадающих предопределенных записей DAP будет действовать эта запись DAP. Таким образом, в доступе через SSL VPN будет отказано. Отредактируйте параметр DfltAccessPolicy и в качестве действия (Action) задайте Terminate (Прервать).Нажмите кнопку OK.
2. Добавьте новую динамическую политику доступа Managed_Endpoints следующим

образом:Описание: Employee Client Access (Клиентский доступ штатного сотрудника)Добавьте (расположенный направо от Типа атрибута Оконечной точки) Тип атрибута Оконечной точки (Политика) как показано на рисунке 31. По завершении настройки нажмите ОК.Рис. 31. Атрибут оконечного устройства DAP. Местоположение Cisco Secure Desktop будет играть роль критерия DAP для клиентского/сетевого доступа.Добавьте второй тип атрибута оконечного устройства (антивирус), как показано на рис. 32. По завершении нажмите кнопку ОК.Рис. 32. Атрибут оконечного устройства DAP. Углубленная оценка антивируса на оконечном устройстве будет играть роль критерия DAP для клиентского/сетевого доступа.В раскрывающемся списке над разделом«атрибутов AAA выберите User has ALL of the following AAA Attributes Values (Пользователь имеет ВСЕ из следующих атрибутов AAA)…Добавьте (при помощи кнопки справа от поля AAA Attribute) тип атрибута AAA (LDAP), как показано на рис. 33 и 34. Затем нажмите кнопку ОК.Рис. 33. Атрибут DAP AAA. Членство в группе AAA используется как критерий DAP для определения штатного сотрудника. Рис. 34. Атрибут DAP AAA. Членство в группе AAA используется как критерий DAP для разрешения средств удаленного доступа.На вкладке Action (Действие) убедитесь, что установлено действие Continue (Продолжать), как показано на рис. 35.Рис. 35. Вкладка Action (Действие). Эта настройка необходима для определения специальной обработки для конкретного подключения или сеанса. При совпадении с записью DAP и установке параметра Action (Действие) в значение Terminate (Прервать) в доступе будет отказано.На вкладке Access Method (Метод доступа) выберите метод доступа AnyConnect Client, как показано на рис. 36.Рис. 36. Вкладка Access Method (Метод доступа). Эта настройка необходима для определения типов клиентских подключений SSL VPN.Нажмите кнопку ОК, а затем Apply.
3. Добавьте новую динамическую политику доступа Unmanaged_Endpoints следующим образом:Описание: Employee Clientless Access (Бесклиентский доступ штатных сотрудников).Добавьте (расположенный направо от коробки Атрибута Оконечной точки) Тип атрибута Оконечной точки (Политика) как показано на рисунке 37. По завершении настройки нажмите ОК.Рис. 37. Атрибут оконечного устройства DAP. Местоположение Cisco Secure Desktop будет играть роль критерия DAP для бесклиентского доступа.В раскрывающемся списке над разделом«атрибутов AAA выберите User has ALL of the following AAA Attributes Values (Пользователь имеет ВСЕ из следующих атрибутов AAA)…Добавьте (расположенный направо от Типа Атрибута AAA) Тип Атрибута AAA (LDAP) как показано на рисунке 38 и 39. По завершении настройки нажмите ОК.Рис. 38. Атрибут DAP AAA. Членство в группе AAA используется как критерий DAP для определения штатного сотрудника. Рисунок 39. Атрибут AAA DAP — Состав группы AAA будет использоваться в качестве критерия DAP для разрешения возможностей Удаленного доступа.На вкладке Action проверьте, выбрано ли в поле Action (Действие) значение Continue. (См. рис. 35.).)Под вкладкой Bookmarks выберите Сотрудников имени списка от выпадающего и затем нажмите Add. Кроме того, проверьте, что Разрешать закладки проверены как показано на рисунке 40.Рисунок 40. Отмечает Вкладку — Позволяет вам выбрать и настроить Списки URL - адресов для пользовательских сеансов.На вкладке Access Method (Метод доступа) выберите метод доступа Web-Portal. (Ссылочный рисунок 36.)Нажмите кнопку ОК, а затем Apply.Внештатные сотрудники будут идентифицироваться только по атрибутам DAP AAA. В результате тип атрибутов оконечного устройства: Policy (Политика) на шаге 4 не настраивается. Этот подход только иллюстрирует универсальность DAP.
4. Добавьте третью динамическую политику доступа: Guest_Access со значением

атрибута:Описание: **Guest Clientless Access (Бесклиентский гостевой доступ).**Добавьте (при помощи кнопки справа от поля Endpoint Attribute) тип атрибута оконечного устройства (Policy — политика), как показано выше на рис. 37. **По завершении настройки нажмите OK.В раскрывающемся списке над разделом«атрибутов AAA выберите User has ALL of the following AAA Attributes Values (Пользователь имеет ВСЕ из следующих атрибутов AAA)…**Добавьте (расположенный направо от коробки Атрибута AAA) Тип Атрибута AAA (LDAP) как показано на рисунке 41 и 42. **По завершении настройки нажмите OK.Рис. 41. Атрибут DAP AAA. Членство в группе AAA используется как критерий DAP для определения внештатного сотрудника. Рис. 42. Атрибут DAP AAA. Членство в группе AAA используется как критерий DAP для разрешения средств удаленного доступа.На вкладке Action проверьте, выбрано ли в поле Action (Действие) значение Continue.** (См. рис. 35.).)Под вкладкой Bookmarks выберите **Подрядчиков** имени списка от выпадающего и затем нажмите Add. Кроме того, проверьте, что проверены **Разрешать закладки**. (Ссылочный рисунок 40.)**На вкладке Access Method (Метод доступа) выберите метод доступа Web-Portal.** (Ссылочный рисунок 36.)**Нажмите кнопку OK, а затем Apply.**

Критерии отбора DAP. На основе произведенных выше процедур настройки DAP критерии отбора для 4 заданных политик DAP должны согласовываться с рис. 43, 44, 45 и 46.

Рис. 43. Управляемые оконечные устройства. При выполнении критериев этой записи DAP штатные сотрудники будут иметь доступ к корпоративным ресурсам через клиентское/сетевое (клиент AnyConnect) подключение. Рис. 44. Неуправляемые оконечные устройства. При выполнении критериев этой записи DAP штатные сотрудники будут иметь доступ к корпоративным ресурсам через бесклиентское подключение (портал). В этой политике также применяется список URL-адресов для штатных сотрудников. Рис. 45. Гостевой доступ. При выполнении критериев этой записи DAP внештатные сотрудники будут иметь доступ к корпоративным ресурсам через бесклиентское подключение (портал). В этой политике также применяется список URL-адресов для внештатных сотрудников. Рис. 46. Политика DAP по умолчанию. В случае невыполнения критериев для всех вышеприведенных записей DAP штатные и внештатные сотрудники по умолчанию не получат доступа.

Заключение

Опираясь на отмеченные в этом примере требования заказчика к сети SSL VPN для удаленного доступа, данное решение отвечает потребностям заказчика в организации такой сети VPN.

В условиях развития и объединения динамических сред VPN динамические политики доступа можно адаптировать и наращивать с учетом частых изменений конфигурации доступа к Интернету, многообразия ролей каждого пользователя в организации и практики входа в систему с управляемых и неуправляемых объектов удаленного доступа с различными конфигурациями и уровнями безопасности.

Динамические политики доступа дополняются новыми и апробированными существующими технологиями, включая углубленную оценку оконечных устройств, сканирование хостов, защищенные настольные рабочие места, AAA и локальные политики доступа. В результате организации могут уверенно обеспечивать защищенный доступ посредством VPN к любому сетевому ресурсу из любого местоположения.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация