Нов български университет

Проектиране на корпоративни мрежи

Част VI

Система за контрол на достъпа в мрежата

Доц. Д-р Емил Стоилов

Департамент по Информатика на НБУ

София, март 2017

Съдържание

При решаването на проблема за защита на информацията в корпоративните мрежи обикновено различаваме три отделни системи, които трябва да бъдат проектирани:

1. Системата за контрол на достъпа

2. Системата от защитни стени и

3. Системата от виртуални частни мрежи (с използване на технологиите IPsec и SSL).

В този технически доклад е представена само системата за контрол на достъпа в мрежата. Останалите две системи ще бъдат предмет на отделни доклади.

За контрол на достъпа в мрежата Cisco използва терминологията **Network Admission Control (NAC)**. По-нататък навсякъде в текста ще използваме NAC поради следните съображения: текстът става по-кратък, избягват се всякакви двусмислици, както и проектантът по-лесно ще се ориентира в номенклатурата на устройствата и софтуера на Cisco.

NAC ограничава достъпа до мрежата въз основа на самоличност и становище за сигурност. Когато едно мрежово устройство (комутатор, маршрутизатор, безжична точка за достъп, DHCP сървър и др.) е конфигурирано за NAC, то може да принуди потребителя да удостовери своята самоличност преди да му бъде предоставен достъп до мрежата. Освен това, на гостите се осигурява достъп само до определена карантинна зона, в която могат да бъдат отстранени всички проблеми водещи до грешка в удостоверяването. Това се извършва чрез вградени специализирани мрежови устройства, промени в съществуващите комутатори и маршрутизатори или ограничени DHCP класове. Например една типична ограничена Wi-Fi връзка е форма на NAC. Потребителят трябва да представи някакви пълномощия (идентификационни данни), преди да му бъде предоставен достъп до мрежата.

Всъщност NAC представлява набор от технологии и решения изградени върху една инициатива водена от Cisco. NAC използва мрежовата инфраструктура за да осигури спазването на определена политика за сигурност от страна на всички устройства които изискват достъп до ресурсите на мрежата. По този начин се ограничават щетите от възникнали заплахи за сигурността като вируси, червеи и шпионски софтуер. На потребителите, които използват NAC, се позволява достъп само до съвместими и надеждни крайни устройства (като например персонални компютри, сървъри, персонални цифрови помощници [Personal Digital Assistants - PDA] и др.). Достъпът до останалите устройстйства е ограничен.

1. Мрежова сигурност с контрол на достъпа

Контролирането на достъпа до мрежовите ресурси е съществена част от защитата на мрежата. Това е една от функциите, които са част от архитектурната рамка SAFE на Cisco. Контролът на достъпа се състои от няколко елемента, които са ключови за архитектурата SAFE и включват следното:

- **Идентифициране (identify):** Като част от процедурите за контрол на достъпа, трябва да се установи самоличността на потребителя и да се проверят неговите права за достъп до мрежата.

- **Привеждане в действие (Enforce):** Политиките за сигурност често налагат използването на софтуер свързан със сигурността, като например скенери за вируси и защитни стени. Част от стратегията за контрол на достъпа е да се наложи използването на такъв софтуер за сигурност преди да се позволи достъп до мрежата.

- **Изолиране (Isolate):** Крайните точки, които не отговарят на изискванията на политиката за сигурност на фирмата, могат да бъдат изолирани и принудени да се възстановят до положението от преди получаването на достъп в мрежата.

Базовите мрежови услуги на Cisco за определяне на самоличността (Identity Based Networking Services - IBNS) представляват всъщност едно интегрирано решение, съчетаващо няколко продукта и предлагащо удостоверяване, контрол на достъпа и реализация на потребителските политики за защита на мрежовите връзки и ресурси. Решението IBNS дава възможност за по-голяма сигурност, като едновременно с това предлага по-ефективно управление на средствата при промени в организацията. IBNS рамката на Cisco позволява предприятията да управляват потребителската мобилност и да намалят разходите свързани с предоставянето и управлението на достъпа до мрежовите ресурси. IEEE 802.1X удостоверява автентичността на клиентите искащи достъп до каналния слой на мрежата. Все пак, с използване на Cisco разширенията на IEEE 802.1X, удостоверяването на потребителите и устройствата и допускането им до мрежата се извършва въз основа на това кой или какво са те, а не на тяхното състояние.

NAC помага да се гарантира, че само надеждни клиентски устройства (като например работни станции и крайни персонални компютри) ще получат пълен достъп до мрежата. Зареденият в клиентското устройство агент (NAC Appliance Agent - NAA), инспектира антивирусната програма, програмата за управление на кръпките и персоналната клиентска защитна стена за да направи оценка на състоянието на клиентското устройство преди да му позволи достъп до мрежата. NAC може да помогне в гарантирането, че даденият клиент притежава актуален комплект от вирусни сигнатури и най-новите кръпки на операционната система, както и че не е заразен. Ако клиентът се нуждае от актуализиране на антивирусната си програма или операционната система, NAC го насочва да направи необходимите промени преди да му се позволи достъпа до защитените мрежови ресурси. Ако клиентът е бил компрометиран или в мрежата съществува огнище на вируси, то NAC поставя клиента в карантинен сегмент на мрежата. След като клиентът е завършил своя процес на актуализация или дезинфекция, неговото състояние се проверява отново. На клиентите в здравословно състояние се разрешава нормален достъп до мрежата.

802.1X/IBNS и NAC предоставят взаимно допълващи се функции: разпознаване на потребителя и проверка на неговото състояние. Заедно те осигуряват контрол на достъпа и включване към VLAN.

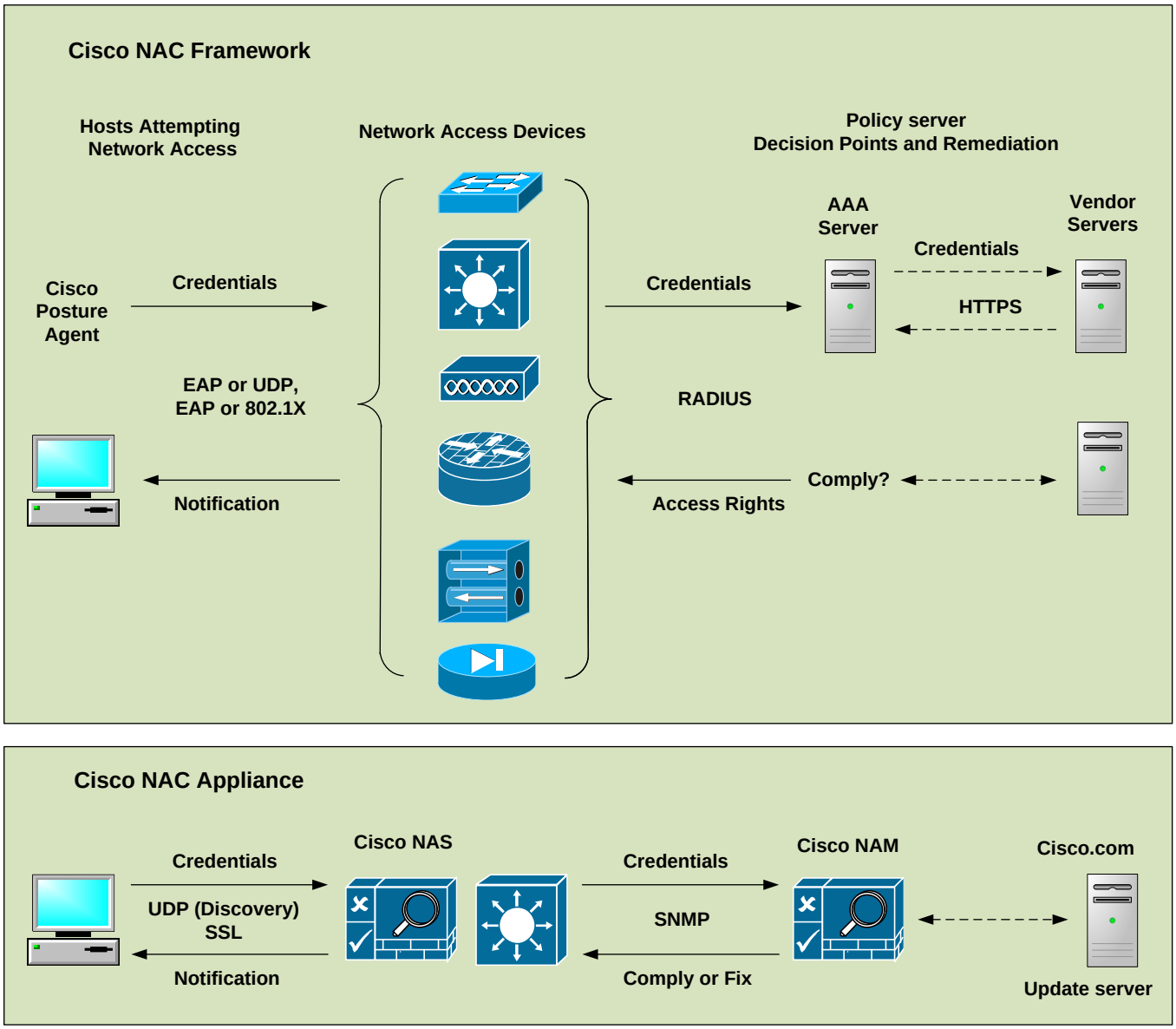
2. Видове NAC

Cisco поддържа два вида NAC, както е показано на Фиг. 1.

- **Cisco NAC Framework** е стандартна технология, която интегрира интелигентната мрежова инфраструктура със създадените от повече от 60 водещи производители антивирусни и други решения за сигурност и софтуер за управление. Тази технология налага спазването на определена политика за сигурност от всички устройства искащи достъп до мрежата. NAC Framework е вграден софтуер в NAC активираните продукти който осигурява повсеместен контрол валиден за всички методи за достъп до мрежата. Информацията за състоянието може да бъде събрана и да бъде наложена определена политика за достъп на всички хостове, които се опитват да достигнат ресурсите на мрежата през маршрутизатори, комутатори, безжични точки за достъп и VPN концентратори. Тази система се възползва от предимствата на множество продукти на Cisco, както и на други производители, които падкрепят NAC.

- **Cisco NAC Appliance** е цялостно решение за контрол и защита на мрежите. То концентрира всички NAC способности в едно устройство. Продуктите клиент, сървър и мениджър на Cisco NAC Appliance позволяват на мрежовите администратори да удостоверяват, оценяват и възстановяват отдалечени потребители и техните машини

преди да бъде даден достъп до мрежата. Тази система определя дали мрежови устройства като лаптопи, IP телефони, PDA устройства и принтери са в съответствие с правилата за сигурност на организацията и поправя всякакви уязвимости преди да позволи достъп до мрежата.



Фиг. 1 Сравнение на видовете NAC

3. Основни положения на Cisco NAC Appliance

В този раздел ще разгледаме основите на NAC Appliance, включително отделните компоненти и използваната терминология.

3.1 Компоненти

Cisco NAC Appliance осигурява контрол на достъпа до мрежата и налага спазването на определени политики в тази област. Системата е изградена от следните компоненти:

- **Мениджър (NAC Appliance Manager - NAM):** Това е сървърът за администриране на системата, където са дефинирани отделните политики. Със сигурната уеб конзола на NAM се управляват до 20 броя NAC сървъри (NAS). NAM действа като пълномощник (authentication proxy) на сървърите за удостоверяване от задния слой (Backend authentication servers). Когато системата е изградена с отделна мрежа за управление (out-of-band), NAM конзолата позволява управление на комутаторите и

присъединяване на потребителски портове към VLAN, като се използва протокола SNMP.

- **Сървър (NAC Appliance Server - NAS):** Това е правоприлагащият, изпълнителен сървър, който се намира между ненадеждната (untrusted), управлявана мрежа и доверената (trusted) мрежа. NAS налага политиките определени от уеб конзолата на NAM, включително привилегиите за достъп до мрежата, изискванията за проверка на автентичността, ограниченията на трафика, както и други изисквания на NAC Appliance системата. Възможни са две архитектурни решения. При първото от тях трафикът от сървъра се предава заедно с потребителския трафик (in-band). При второто решение този трафик е отделен от потребителския трафик (out-of-band), като заедно с потребителския трафик преминават само пакетите по време на проверката на самоличността и оценката на състоянието на клиента. Различаваме и два режима на използване на сървъра. Когато потребителите са съседи от слой 2 на NAS се използва режим на слой 2. Когато те са отдалечени и трафика преминава през маршрутизатори, в NAS се използва режим на слой 3.

- **Агент (NAC Appliance Agent - NAA):** За клиентите с операционна система Microsoft Windows се предлага като опция и агент само за четене. Агентът проверява приложенията, файловете, услугите или регистрационните ключове, за да гарантира, че клиентите отговарят на определените мрежови изисквания преди да получат достъп до мрежата.

- **Профайлер (NAC Profiler):** Профайлерът позволява на мрежовите администратори да поддържат в реално време инвентарен опис на всички устройства в мрежата. Това значително улеснява разполагането и управлението на NAC системите чрез откриване и проследяване на положението, както и типа на всички свързани към локалната мрежа клиенти, включително тези, които не могат да преминат процеса на удостоверяване. Профайлерът също използва събраната информация за устройствата, за да определи правилната политика на NAC, която да бъде приложена.

- **Акуализиране на политиките (NAC Appliance policy updates):** За да се определи точно текущото състояние на операционните системи, на антивирусните и антишпионски програми на клиентите, е необходима да се извършва редовно актуализиране на предварително подготвените политики и правила. В момента Cisco NAC Appliance осигурява вградена поддръжка на 24 антивирусни и 17 антишпионски програми на различни производители.

- **Сървър за гости (NAC Guest Server):** Сървърът за гости е основен компонент на системата Cisco TrustSec, която може да бъде добавена към кабелни и безжични NAC внедрявания, с цел получаване на интегриран и защитен достъп на гостите до мрежата. Сървърът за гости улеснява създаването на акаунти за временен достъп до мрежата чрез разрешаване на вътрешен потребител да спонсорира гост и да създаде акаунт за него по прост и сигурен начин. Освен това, целият този процес се записва само на едно място, и се съхранява за по-късно докладване, включително детайлите по получаването на мрежовия достъп

3.2 Актуализиране на политиките

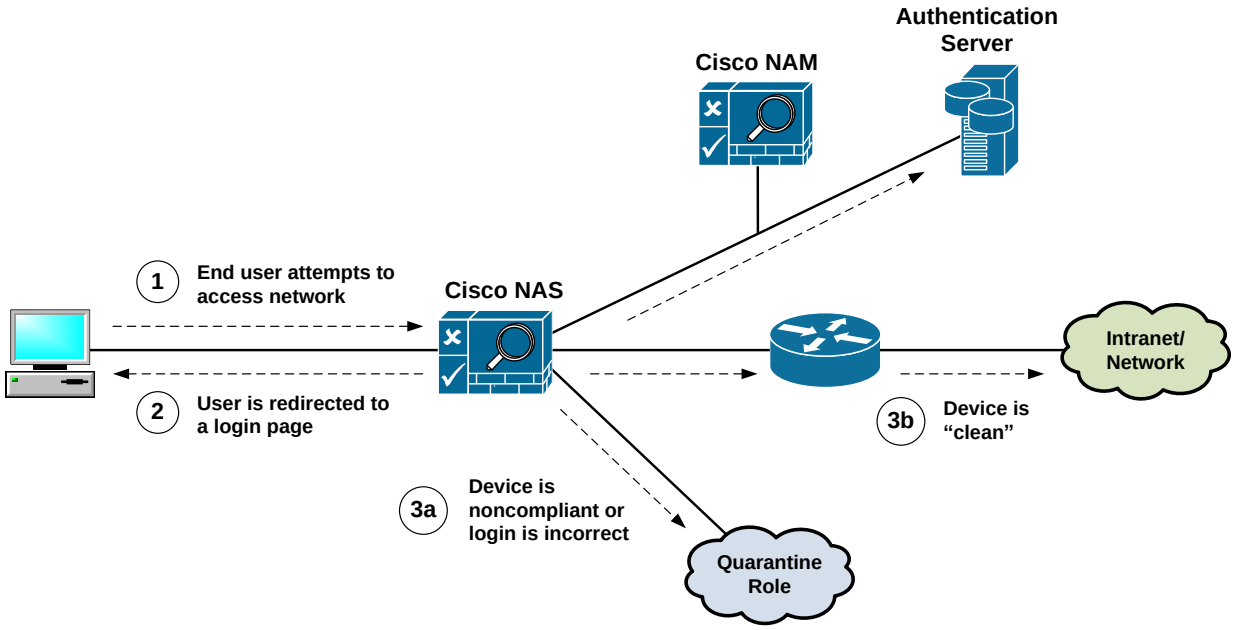
Cisco осигурява автоматични актуализации на политиките за сигурност като част от стандартния пакет за поддръжка на софтуера. При тези актуализации се доставят предварително дефинирани политики засягащи повечето общи критерии за достъп до мрежата, включително политики проверяващи за критични промени в операционните системи, за дефиниции на нови вируси, както и за промени в антишпионския софтуер.

Системата Cisco NAC Appliance е предварително конфигурирана да предлага проверки на политиката за повече от 200 приложения от над 50 доставчици.

В допълнение към предварително конфигурираните проверки, клиентът има пълен достъп до правилата на NAC и може да създаде своя персонализирана проверка или правило за всяко едно приложение от трета страна.

3.3 Последователност на процесите

На Фиг. 2 е показана последователността от протичащи процеси в Cisco NAC Appliance.



Фиг. 2 Последователност на процесите

Различаваме следните процеси в тяхната последователност:

1. Крайният потребител се опитва да получи достъп до уеб страница или да използва интранет.

2. Потребителят се пренасочва към страницата за вход. Cisco NAC Appliance проверява потребителското име и паролата, след което сканира устройството и мрежата за да оцени уязвимостта на устройството.

3. Ако устройството не отговаря на корпоративните политики, или опитът за вход в мрежата е неправилен, на потребителя се отказва достъпа до мрежата. На него се определя карантинна роля, с достъп само до ресурси за възстановяване. След възстановяването, потребителят се насочва към стъпка 2 за нова проверка и сканиране.

4. Ако потребителското име и парола са правилни и устройството е в съответствие с корпоративните политики, устройството се поставя в списъка на сертифицираните устройства и му се предоставя достъп до мрежата.

3.4 Мащабиране на NAS

Има три нива на NAM поддържащи различните приложения на Cisco NAC Appliance:

- Cisco NAC Appliance Lite Manager управлява до 3 Cisco NAS устройства, като всеки сървър може да поддържа до 100, 250, или 500 потребителя.

- Cisco NAC Appliance Standard Manager управлява до 20 Cisco NAS устройства. В тази конфигурация всеки сървър поддържа от 1500 до 5000 потребителя в зависимост от това кой модел е избран.

- Cisco NAC Appliance Super Manager управлява до 40 Cisco NAS устройства. Всеки сървър поддържа от 1500 до 5000 потребителя в зависимост от модела.

Броят на потребителите поддържани от сървъра отговаря на различните потребители, които са били сканирани за съответствие, а не на мрежовите устройства като принтери или IP телефони.

Броят на потребителите, които поддържа един сървър, зависи от много фактори консумиращи процесорното време и другите ресурси на сървъра, като например:

- Броят на новите удостоверявания на потребители за секунда

- Броят на оценките на състоянията в секунда

- Колко проверки се извършват във всяка оценка

- Броят на сканиранията на мрежата без използването на агенти в секунда

- Броят на електронните приставки (plug-ins) за всяко сканиране

- Интервалите за повторно сканиране

- Интервалите на общите таймери, както и на таймерите за всяка роля

- Контролирането на пропускателната способност

- Използването на различни филтри при контрола на достъпа.

Да отбележим, че всъщност пропускателната способност на интерфейсите оказва най-малко влияние върху изчисленията когато определяме колко потребителя NAS може да поддържа.

4. Възможности за разполагане на NAS

Има четири фактора, които трябва да вземем под внимание, когато решаваме къде да разположим сървърите. Това са различните възможни режими на работа на NAS, както и особеностите на топологията.

- **Режими на шлюз:** Избираме дали NAS ще действа като мрежово устройство от слой 2 или като мрежово устройство от слой 3.

- **Работни режими на NAS:** Избираме кога трафика да преминава през NAS.

- **Режими за достъп на клиента до NAS:** Определяме дали устройствата на клиента са директно свързани (съседни от слой 2) с NAS или отдалечени от него.

- **Физически модели за разполагане:** Определяме дали NAS е вграден в пътя на трафика.

4.1 Режими на шлюз

Имаме три режима, когато NAS работи като шлюз. Те са показани на Фиг.3.

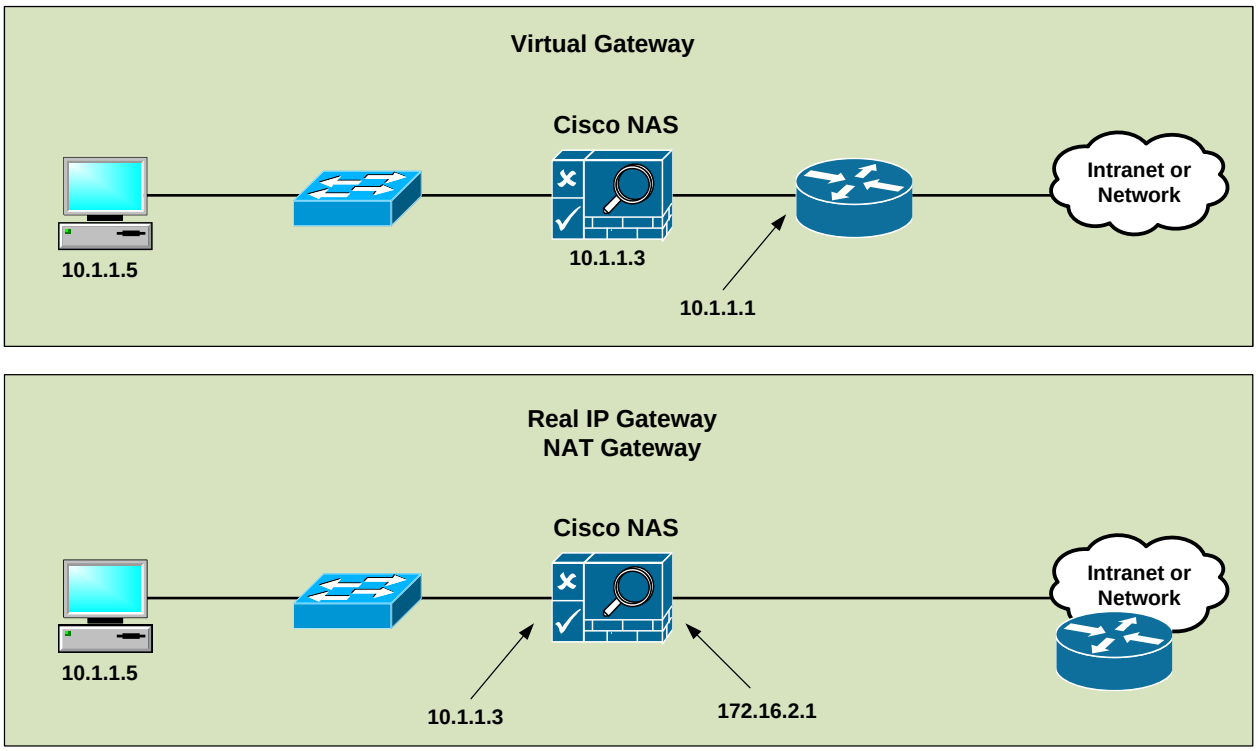


Figure 3 Cisco NAS Gateway Modes

NAS може да работи като мрежово устройство от слой 2 или като мрежово устройство от слой 3 в зависимост от конфигурирания режим на шлюз:

- **Режим на виртуален на шлюз (Virtual gateway mode):** В този режим NAS работи като стандартен Ethernet мост (в слой 2), но с добавена функционалност за IP филтър и IPsec модул. Тази конфигурация обикновено се използва, когато ненадеждната мрежа вече има шлюз от слой 3. Това е най-често срещаният вариант на разполагане. Неговото реализиране всъщност е и най-лесно. Все пак, може да се наложи използване на допълнително оборудване (шлюз от слой 3) и веднага се забелязва, че NAS възпрепятства в известна степен производителността.

- **Режим на реален IP шлюз (Real IP gateway mode):** В този режим NAS работи като шлюз по подразбиране от слой 3 за управляваните потребители от ненадеждната мрежа. Целият трафик между ненадеждната и надеждната мрежа преминава през NAS, където се прилагат правилата за IP филтриране, политиките за достъп, както и всякакви други механизми на обработка на трафика, които са конфигурирани. NAC е определен за шлюз по подразбиране на управляваната подмрежа и следователно може да изпълнява DHCP услуги, т.е да действа като DHCP сървър.

- **Режим на NAT шлюз (NAT gateway mode):** В този режим NAS функционира по същия начин както в режима на реален IP шлюз от слой 3. Добавени са само NAT услуги. Когато се използва NAT на клиентите динамично се присвояват IP частни адреси. NAS извършва преобразуването на частните IP адреси в публични и обратно когато трафика се маршрутизира между ненадеждната (управлявана) мрежа и външната мрежа. NAS поддържа NAT с различни конфигурации (стандартна, динамична, едно към едно).

Да отбележим, че режимът на NAT шлюз е предназначен предимно за улесняване на тестването, защото за установяването му се изисква минимално количество

конфигурационна информация. Поради ограничението на броя на връзките обаче, този режим (независимо in-band или out-of-band) не се препоръчва и не се поддържа за промишлени приложения.

Типът на инсталирането и работния режим определят услугите, които NAS ще предостави. Например NAS може да функционира като мост между ненадеждната и надеждната мрежа или да функционира като шлюз за ненадеждната мрежа.

4.2 Работни режими на NAS

При NAS се прилагат два модела за трафика: **in-band** или **out-of-band**.

Всеки NAS може да бъде конфигуриран по единия или другия метод, но само един метод може да се използва в даден момент. Изборът на режим се базира на това, дали клиентът иска да премахне NAS от пътя на данните след оценката на състоянието.

Режимът in-band е най-лесният за внедряване. NAS остава на пътя на трафика както преди, така и след оценяването. In-band режимът на работа осигурява текущо ACL филтриране, намаляване на скоростта на трафика и контролиране на достъпа въз основа на определена роля.

При режим out-of-band, NAS остава на пътя на трафика само по време на оценяване на състоянието. Този режим осигурява контролиране на достъпа въз основа на VLAN портове или на определена роля. ACL филтрирането и намаляването на скоростта на трафика се постига само по време на оценяването на състоянието.

Да отбележим, че работен режим in-band се поддържа от NAS свързан с всяка безжична точка за достъп, комутатор или концентратор. Работният режим out-of-band се поддържа от NAS свързан с повечето комутатори на Cisco с последни версии на софтуера.

4.3 Режими за достъп на клиента до NAS

Изборът на режим тук зависи от това по какъв начин клиентът е свързан с NAS. Възможни са два режима:

- **Режим на слой 2 (Layer 2 mode):** При него MAC адреса на устройството на клиента се използва за уникална идентификация на устройството. Този режим поддържа виртуалните и реални режими на шлюзове, както и двата работни режима на NAS (in-band и out-of-band). Това е най-разпространения модел, който се използва в локалните мрежи.

- **Режим на слой 3 (Layer 3 mode):** При него устройството на клиента не е в съседство от слой 2 с NAS. Тогава IP адресът на клиента (и неговия MAC адрес, започвайки от Cisco NAA версия 4.0 в Layer 3 out-of-band приложения) се използва за уникална идентификация на устройството. Този режим поддържа виртуалните и реални режими на шлюзове, както и работните режими in-band и out-of-band.

Всеки NAS може да бъде конфигуриран по единия или другия метод, но само един метод може да се използва в даден момент. Режимът за достъп на клиента се конфигурира независимо от работния режим на NAS.

4.4 Физически модели за разполагане

Моделът за разполагане на границата (edge deployment model) е най-лесният за разбиране физически модел на разполагане. При него NAS е физически и логически вграден в пътя на трафика. VLAN ID преминават направо, без промяна, през сървъра когато той е в

режим на виртуален шлюз. Определени трудности можем да срещнем и ситуацията да се усложни, когато потребителите са свързани към много комуникационни шкафове.

Моделът за централно разполагане (central deployment model) е най-често срещания вариант и всъщност най-лесния. При него NAS е логически вграден (inline), но не и физически.

Да обясним малко по-подробно как може да се реализира идеята на втория модел. Когато NAC appliance е конфигуриран като виртуален шлюз, той действа като мост между крайните потребители и шлюза по подразбиране (в маршрутизатора) за управляваната клиентска подмрежа. За даден клиентски VLAN, NAC appliance прехвърля трафика от своя ненадежден интерфейс в своя надежден интерфейс. Когато той действа като мост използваме две VLAN. Например клиентска VLAN 110 е дефинирана между безжичния LAN контролер (Wireless LAN Controller – WLC) и ненадеждния интерфейс на NAC appliance. Тук нямаме маршрутизируем интерфейс или пък комутируем виртуален интерфейс (Switched Virtual Interface - SVI) свързан с VLAN 110 на комутатора в разпределителния слой. Конфигурирана е VLAN 10 между надеждния (доверения) интерфейс на NAC appliance и интерфейса на следващия маршрутизатор / SVI за клиентската подмрежа. NAC appliance прехвърля пакетите които получава по VLAN 110 към VLAN 10, като естествено променя съответните VLAN етикети (tags). Същият процес протича в обратна посока за пакетите, които се връщат на клиента. Да отбележим, че в този режим протоколните пакети (Bridge Protocol Data Units - BPDU) не се пропускат от ненадеждната мрежа към надеждната мрежа. Тази опция за преобразуване на една VLAN в друга VLAN се нарича VLAN mapping и обикновено се използва когато NAC appliance се намира логически вграден (inline) между клиентите и защитената мрежа. Тъй като NAC сървърът е наясно с протоколите от по-горните слоеве, по подразбиране той изрично позволява протоколи които са необходими за връзка с мрежата в процеса на удостоверяване (например DNS и DHCP).

5. Проектантски решения за използване на Cisco NAC Appliance

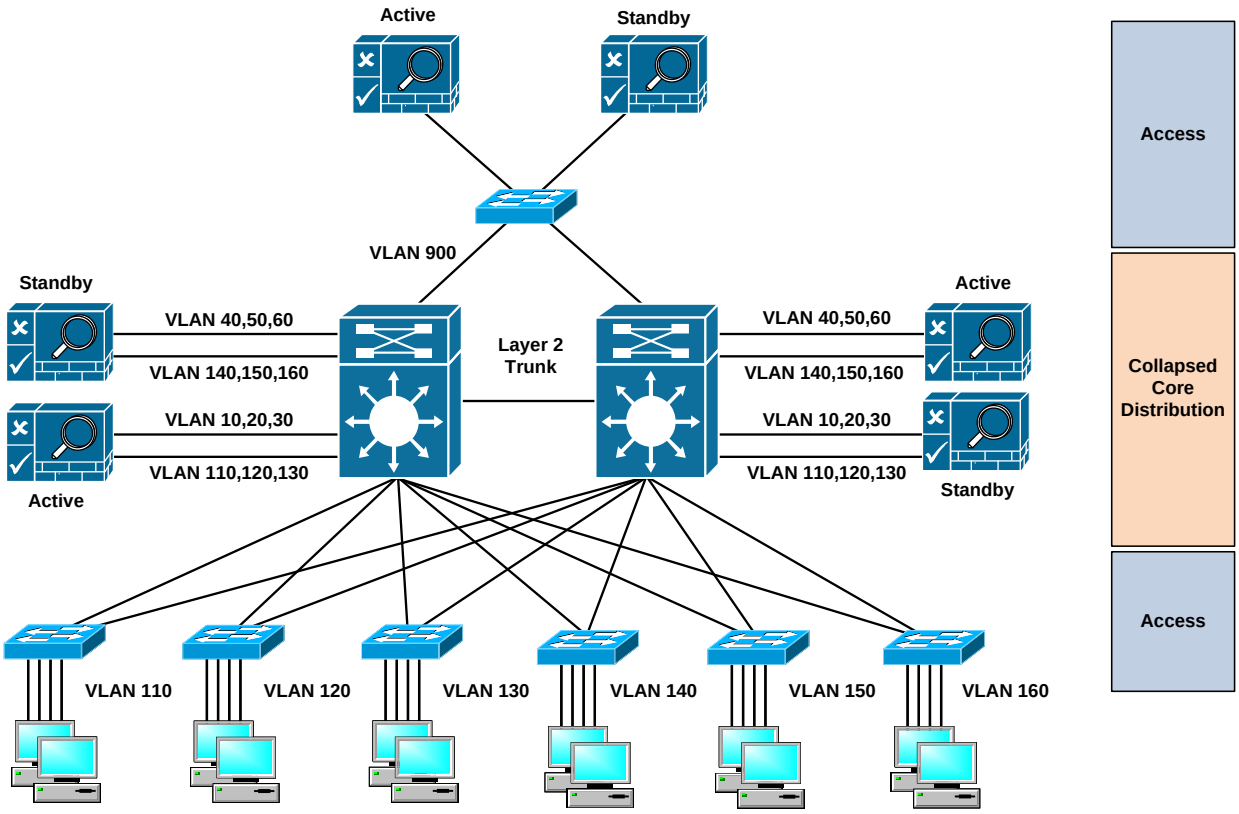
В този раздел ще направим преглед на някои общи проектантски решения.

Като препоръчителна практика, при внедряването на NAC Appliance се използва пълна резервираност. За защита от срив се проектират по две NAM устройства или NAS устройства. Двойката от NAM устройства ни предпазва от срив в управлението, докато двойката от NAS устройства осигурява резервираност на операциите за защитените устройства.

На Фиг.4 в мрежата имаме два комплекта от NAS двойки. Едната двойка NAS поддържа устройствата от VLAN 110, 120, и 130. Другата двойка NAS поддържа устройствата от VLAN 140, 150, и 160. Всички компоненти в този дизайн са или в активно състояние (active) или в състояние на готовност (standby). Всяка двойка има общ виртуален MAC и виртуален IP адрес. Поради споделения MAC адрес, е необходима връзка в слой 2 между компонентите. Двата комутатора от разпределителния слой са свързани с магистрала от слой 2 (layer 2 trunk).

В схемата на Фиг.4 не предполагаме, че една VLAN се разпростира в няколко комутатора в слоя за достъп, т.е. приемаме че дадена VLAN е ограничена в рамките на един комутатор. В този случай магистралата между двата комутатора в разпределителния слой е необходима само за нуждите на двойките NAS. NAM устройствата са свързани и към двата комутатора в разпределителния слой и поддържат всички NAS устройства в мрежата.

Излишеството от резервиращи устройства по-нататък няма да бъде показвано във фигурите. Това се прави единствено с цел те да се опростят и да станат по-лесно разбираеми. Все пак трябва дебело да се подчертае, че всички следващи схеми могат, и задължително трябва бъдат резервирани.



Фиг. 4 Проектиране на NAC Appliance с излишество.

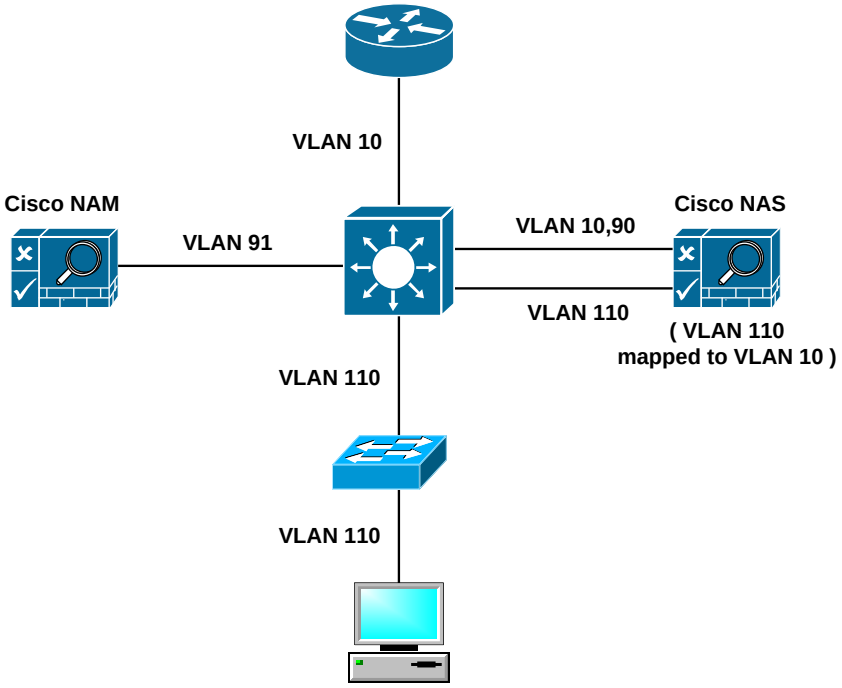
5.1 In-band дизайн в слой 2

Топологията in-band в слой 2 е най-често срещания вариант на внедряване. При нея NAS е логически заедно с клиентския трафик (inline), но не и физически. Когато използваме режим на виртуален шлюз, NAS извършва mapping между отделните VLAN, т.е. променя тяхните номера и етикети.

На Фиг.5, NAS преобразува (т.е. извършва mapping) на VLAN 110 във VLAN 10. Целият клиентски трафик преминава през NAS. След оценката на състоянието NAS надеждно управлява целия трафик. MAC адреса на клиента се използва за идентифициране на устройството. VLAN 90 и VLAN 91 са управляващи VLAN за NAS и NAM.

Това е най-мащабируемият дизайн в прехода от слой 2 към разпределителния слой, тъй като този дизайн може да бъде прозрачно прилаган към съществуващи мрежи с много комутатори в слоя за достъп. Той се поддържа от всички инфраструктурни устройства. Cisco NAS поддържа списъци за достъп (Access Control List - ACL) за всеки потребител.

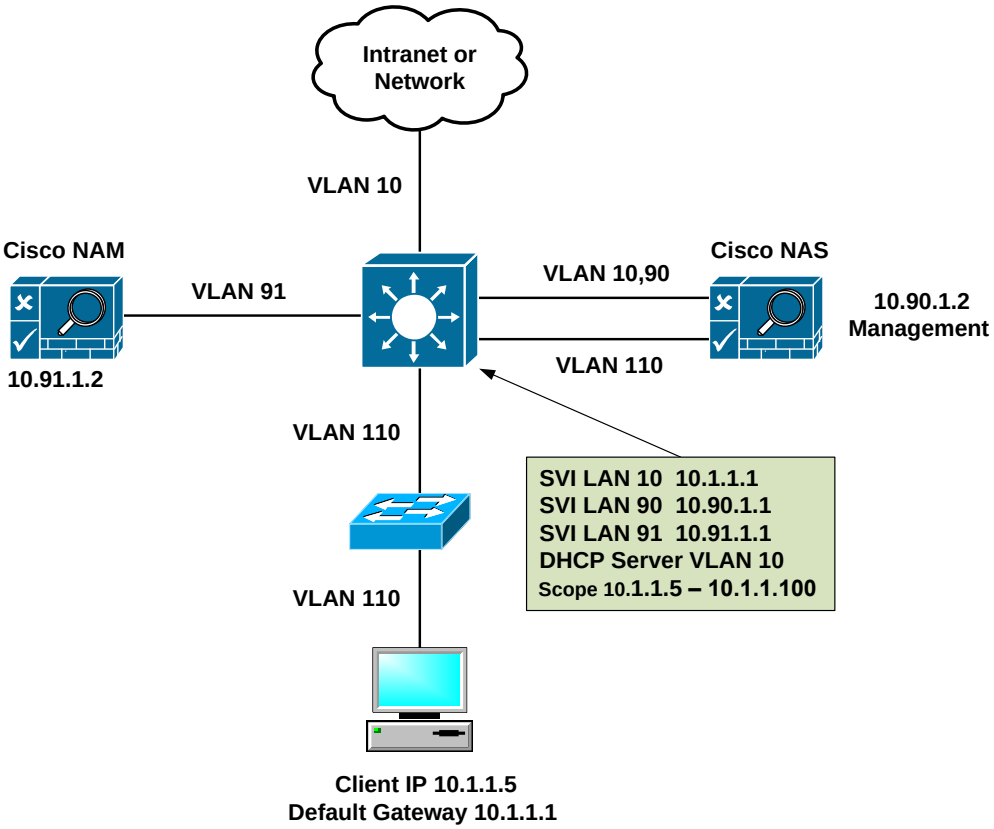
За съжаление този NAC подход не може да се използва, когато връзката към комуникационните шкафове е от слой 3.



Фиг. 5 In-band дизайн в слой 2

5.1.1 Пример: Виртуален шлюз при in-band дизайн в слой 2

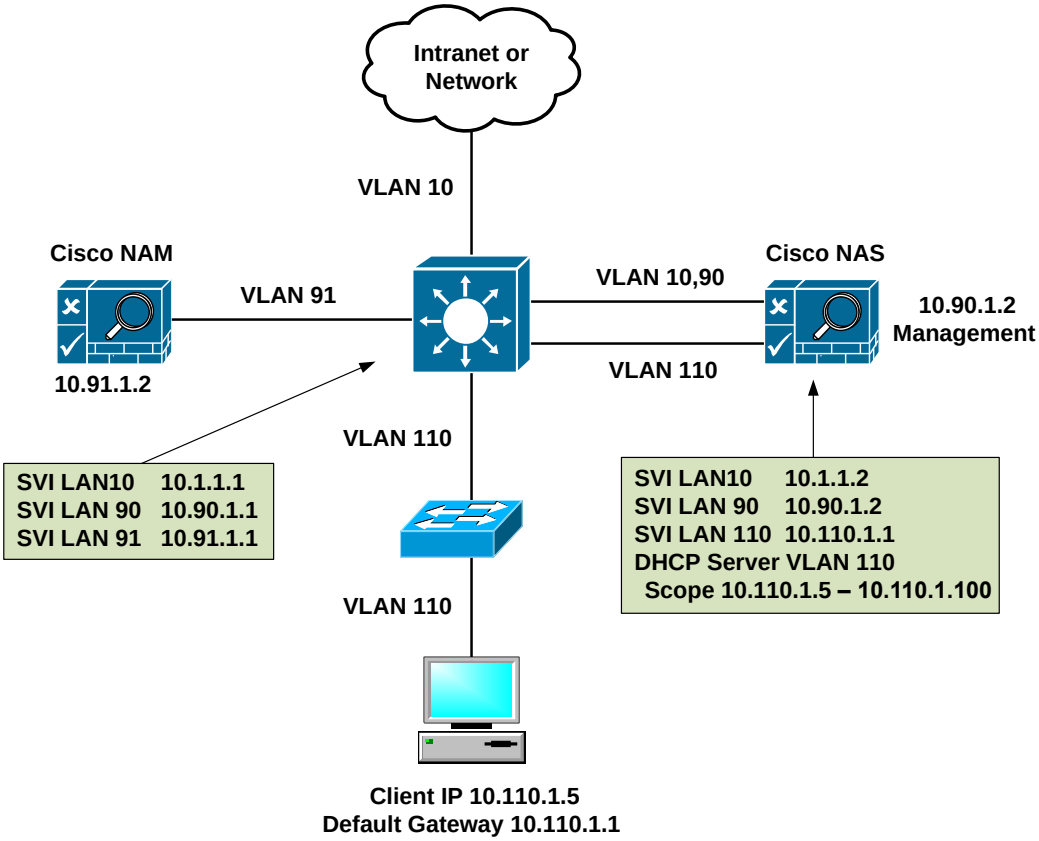
На Фиг. 6 е показан виртуален шлюз при in-band дизайн в слой 2. NAS извършва mapping на трафика от VLAN 110 във VLAN 10. Мрежите VLAN 90 и VLAN 91 са виртуални мрежи за управление на NAS и NAM. В комутатора от слой 3 на разпределителния слой са дефинирани комутируеми виртуални интерфейси (SVI) за VLAN свързани с NAM, NAS и устройствата в слоя за достъп. Този комутатор също служи за DHCP сървър и за шлюз по подразбиране на устройствата в слоя за достъп. Съществуващата IP адресна схема в мрежата не се променя когато внедряваме виртуален шлюз.



Фиг. 6 Виртуален шлюз при in-band дизайн в слой 2

5.1.2 Пример: Реален IP шлюз при in-band дизайн в слой 2

На Фиг. 7 е показан реален IP шлюз при in-band дизайн в слой 2. Сега NAS служи за DHCP сървър и за шлюз по подразбиране за устройствата в слоя за достъп. NAS има дефинирани статични маршрути към останалите подмрежи на организацията. Разпределителния комутаторът от слой 3 има SVI за VLAN свързани с NAM, NAS и устройствата в слоя за достъп. Съществуващата IP адресна схема трябва да се промени когато внедряваме реален IP шлюз. Мрежите VLAN 90 и VLAN 91 са виртуални мрежи за управление на NAS и NAM.



Фиг. 7 Реален IP шлюз при in-band дизайн в слой 2

Един недостатък на този дизайн е, че той изисква статични маршрути в комутаторите за достъп.

5.2 Out-of-Band дизайн в слой 2

Връзките в слой 2 при out-of-band дизайн са подобни на връзките в слой 2 при in-band дизайн, с изключение на това, че връзката между комутатора за достъп и многослойния комутатор в разпределителния слой сега е магистрала, по която преминават пакетите както на VLAN за оценяване, така и на VLAN за достъп до мрежата.

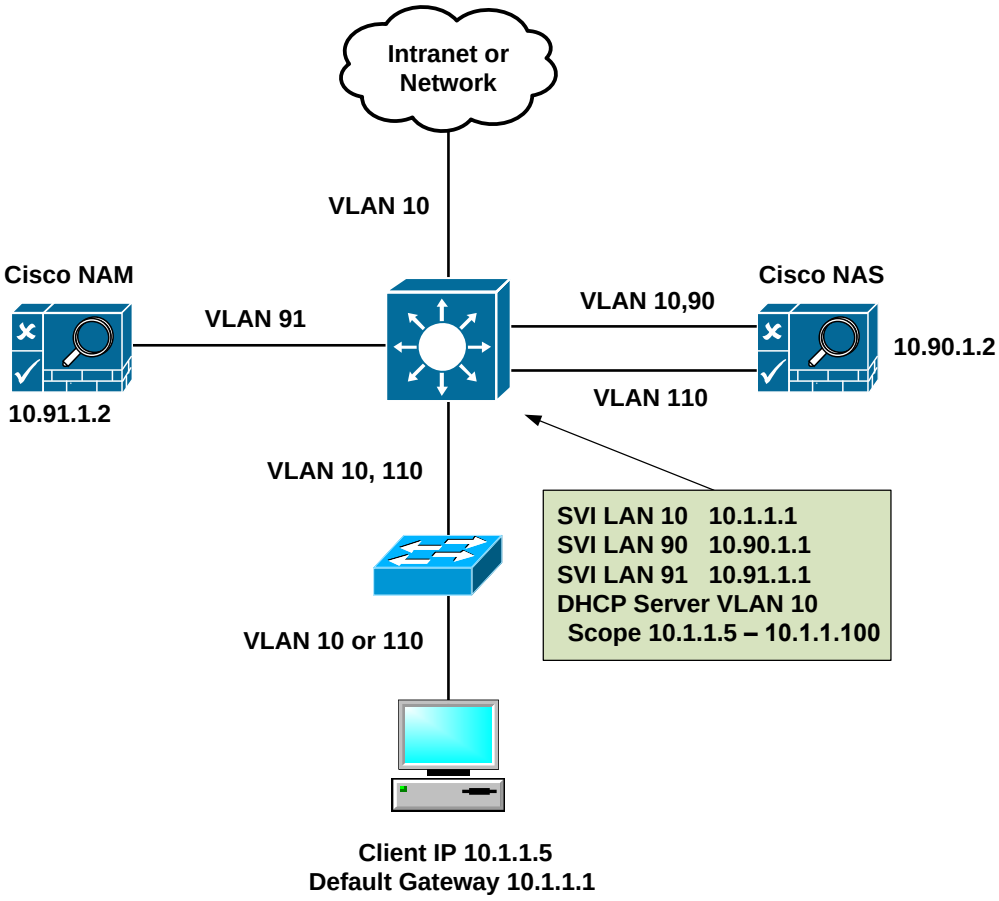
Клиентът е свързан с NAS преди и по време на оценяването. VLAN на клиента се променя и NAS се прескача след успешна оценка на състоянието. Следователно NAS управлява сигурно трафика само по време на оценяването. ACL за потребителите трябва да бъдат дефинирани за техните виртуални мрежи, а не в NAS, тъй като след оценяването потребителския трафик не преминава през него.

Да отбележим, че NAM може да поддържа както динамично присвояване на VLAN въз основа на роля, така и присвояване на VLAN на географски принцип в комутаторите. За всеки един порт на комутатор се поддържа само един MAC адрес, с изключение на устройствата за IP телефония.

Този дизайн изисква използване на комутатори, които поддържат технологията out-of-band. NAM използва протокола SNMP с неговите възможности за откриване на събития (trap съобщения) за да установи достъп на потребител по активиране на връзката (PC link-state up) и да извърши конфигурирането на комутатора.

5.2.1 Пример: Виртуален шлюз при out-of-band дизайн в слой 2

Фиг. 8 показва адресирането в схема с виртуален шлюз при out-of-band дизайн в слой 2. NAS извършва mapping на трафика от VLAN 110 във VLAN 10 по време на процеса на оценяване на състоянието. В комутатора от слой 3 на разпределителния слой са дефинирани комутируеми виртуални интерфейси (SVI) за VLAN свързани с NAM, NAS и устройствата в слоя за достъп. Този комутатор също служи за DHCP сървър и за шлюз по подразбиране на устройствата в слоя за достъп. Съществуващата IP адресна схема в мрежата не се променя когато внедряваме виртуален шлюз.



Фиг. 8 Виртуален шлюз при out-of-band дизайн в слой 2

5.3 In-band дизайн в слой 3

Когато имаме in-band в слой 3 топология, устройството на клиента не е в непосредствена близост до NAS. Използва се IP адреса на клиента за неговото идентифициране, тъй като MAC адреса предоставен на NAS не е на клиента. Този дизайн се използва за сигурно управление на трафика от отдалечени места или от VPN концентратори.

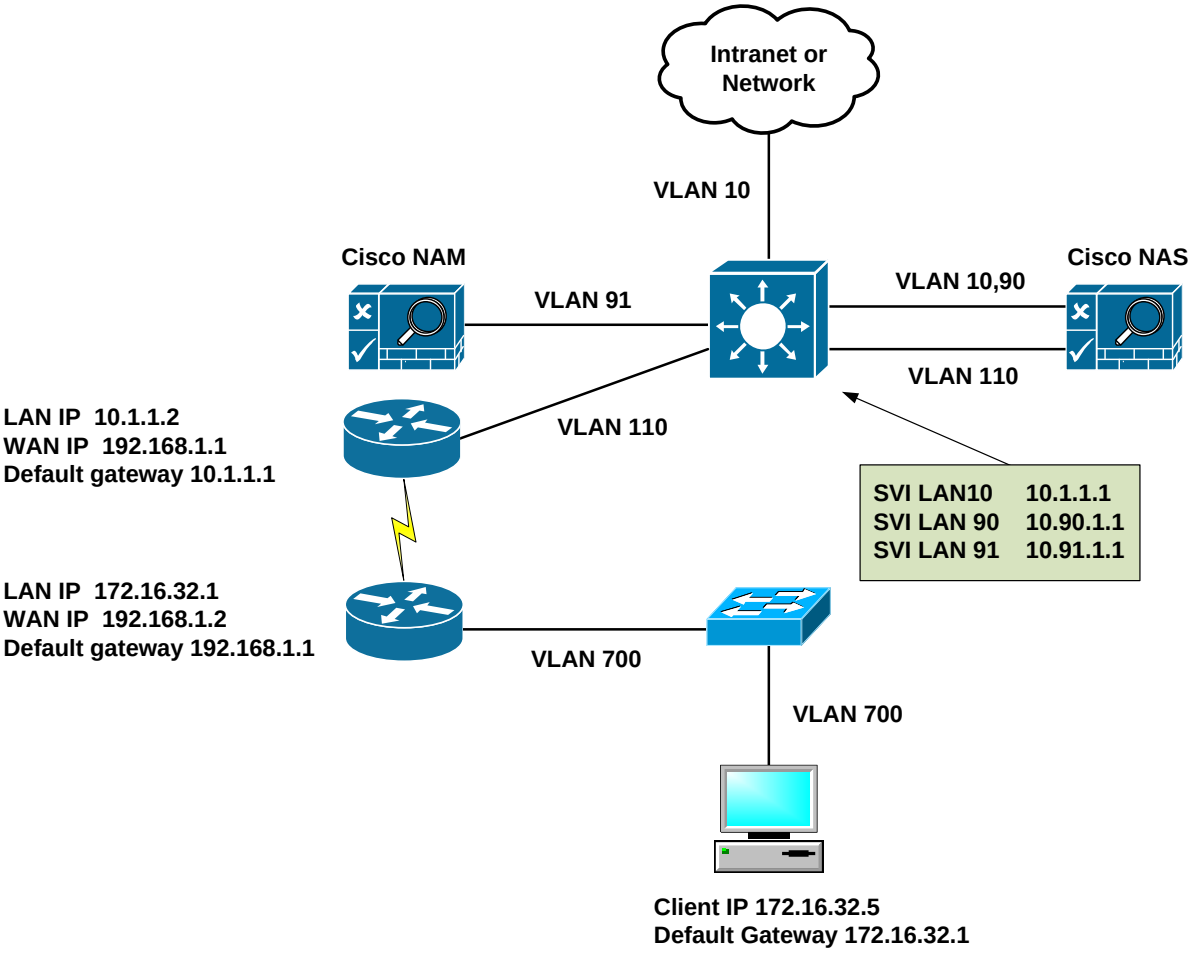
5.3.1 Пример: Виртуален шлюз при in-band дизайн в слой 3

Фиг. 9 илюстрира виртуален шлюз при in-band дизайн в слой 3. NAS извършва mapping на трафика от VLAN 110 в VLAN 10. Разпределителният комутаторът от слой 3 има SVI за VLAN свързани с NAM, NAS и устройствата в слоя за достъп. Разпределителният комутатор е шлюз

по подразбиране за устройствата от слоя за достъп. Като DHCP сървър обикновено служи отдалечен маршрутизатор.

Целият трафик от отдалечения сайт преминава през NAS.

Този дизайн също поддържа VPN концентратори. В този случай вместо отдалечената двойка маршрутизатори, към разпределителния комутатор е свързан VPN концентратор. Трафикът от VPN концентратора е насочен към NAS за оценяване и управление.

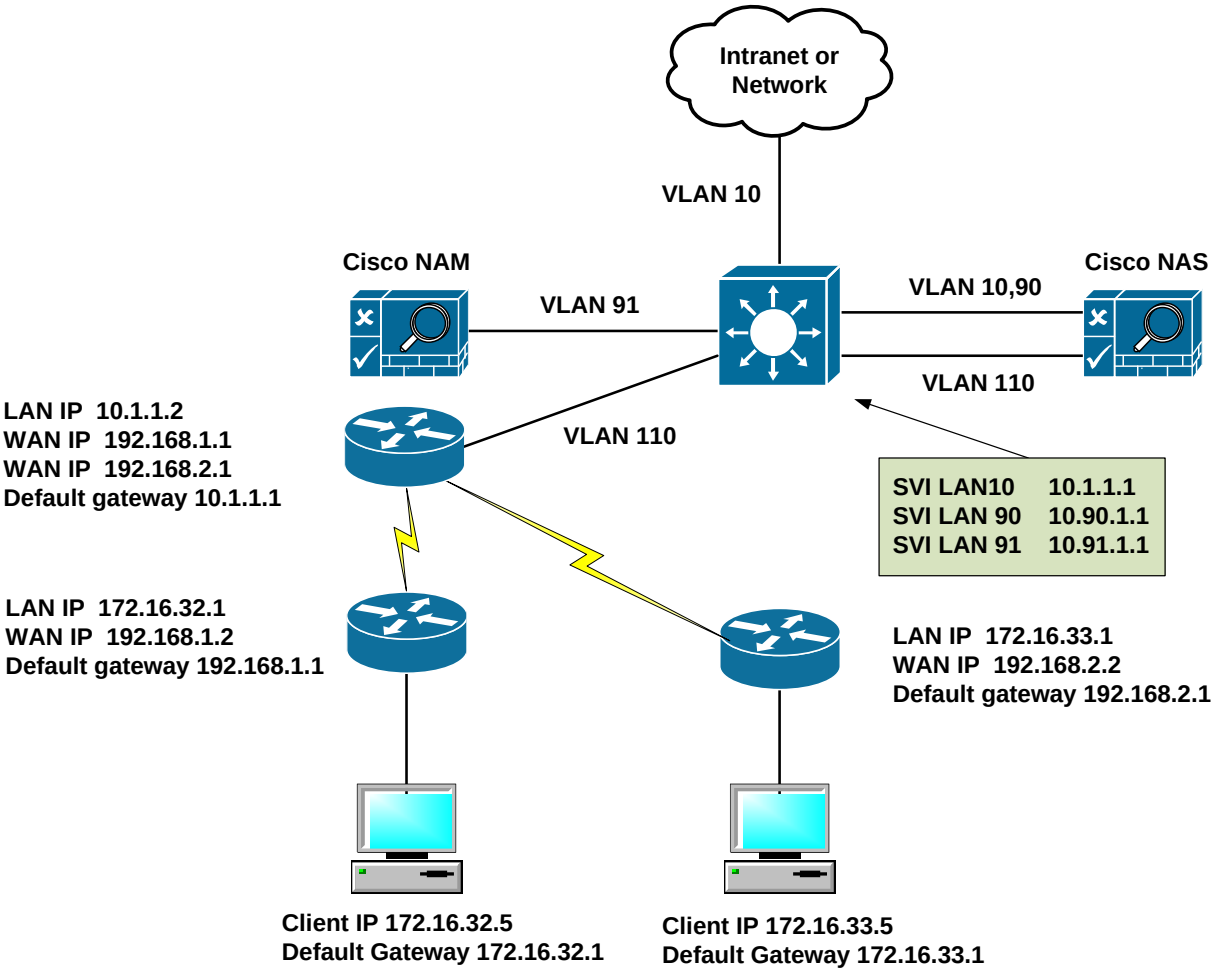


Фиг. 9 Виртуален шлюз при in-band дизайн в слой 3

5.3.2 Пример: In-band дизайн в слой 3 с множество отдалечени обекти

Фиг.10 илюстрира in-band дизайн в слой 3 с множество отдалечени обекти. NAS извършва mapping на трафика от VLAN 110 във VLAN 10. Трафикът към хостовете в центъра и към Интернет преминава през NAS.

Да обърнем внимание, че ако не се вземат допълнителни конфигурационни мерки, трафикът между клиентите и отдалечените обекти не преминава през NAS защото маршрутизаторът на кампуса позволява маршрутизация между граничните маршрутизатори (edge routers). За да се управлява сигурно трафика с отдалечените обекти, трябва да се приложат и други мрежови технологии, като например Policy-Based Routing (PBR) за да се изолират отдалечените обекти. Внедряването на NAS в отдалечените обекти също ще гарантира сигурен трафик.



Фиг. 10 In-band дизайн в слой 3 с множество отдалечени обекти

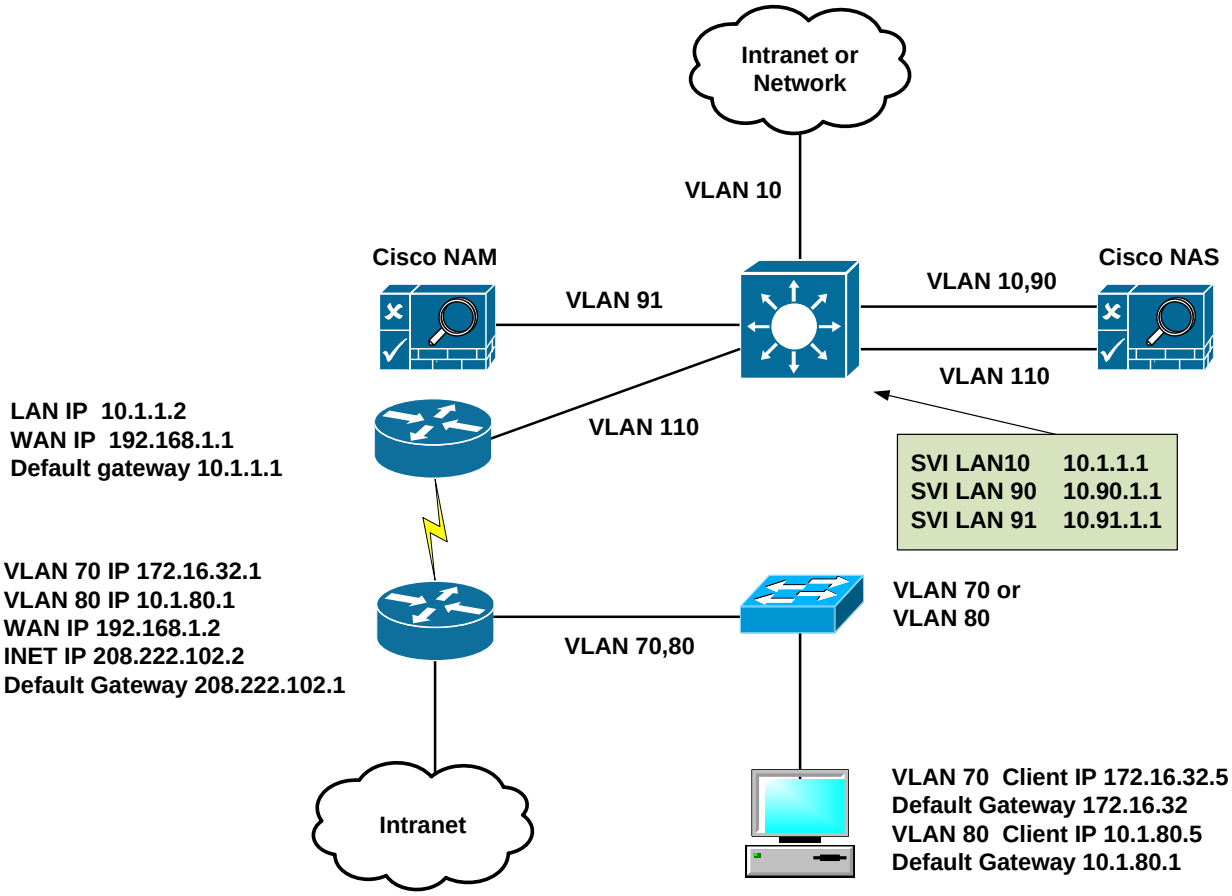
5.4 Out-of-band дизайн в слой 3

Out-of-band дизайнът в слой 3 позволява на администраторите да разположат NAS централно в ядрото или в разпределителния слой на мрежата за обслужване на потребители намиращи се зад комутаторите за достъп от слой 3 и отдалечени потребители зад WAN маршрутизаторите. Потребителите, които се намират на няколко скока от NAS, могат да бъдат обслужени с удостоверяване и оценяване на състоянието на техните устройства. След това потребителският трафик не преминава повече през NAS.

При тази технология се използва IP адреса на клиента (и неговия MAC адрес, започвайки от Cisco NAA версия 4.0 в Layer 3 out-of-band приложения) за уникална идентификация на устройството. Необходими са и комутатори с out-of-band възможности, с подходящ софтуер и конфигурация. NAM използва SNMP за следене и промени в конфигурацията на комутаторите. За правилното маршрутизиране на потребителския трафик е необходимо използването на PBR или друг подходящ механизъм.

5.4.1 Пример: Адресиране при out-of-band дизайн в слой 3

На Фиг. 11 е показан пример за адресиране при out-of-band дизайн на виртуален шлюз в слой 3 за обслужване на отдалечени потребители. NAS извършва mapping на трафика от VLAN 110 във VLAN 10 в процеса на оценяване на състоянието. Разпределителния комутаторът от слой 3 има SVI за VLAN свързани с NAM, NAS и устройствата в слоя за достъп. Отдалеченият граничен маршрутизатор се използва за DHCP сървър и за шлюз по подразбиране за клиентските устройства. Отдалеченият граничен маршрутизатор използва магистрала към отдалечения комутатор за обслужване както на VLAN за оценяване, така и на VLAN за нормална работа. За правилното насочване на трафика се използва PBR.



Фиг. 11 Адресиране при out-of-band дизайн в слой 3

6. Преглед на NAC Framework

NAC Framework е архитектурно рамково решение предназначено да се възползва от съществуващите изградени системи за сигурност и управление както на Cisco, така и на други производители. На Фиг.12 са показани ключовите компоненти на NAC Framework архитектурата.

NAC Framework оценява състоянието на хостовете с цел да предотврати достъпа до мрежата на неоторизирани или уязвими крайни точки. Процесът на NAC за валидиране на състоянието съдържа три главни архитектурни компонента:

- **Субекти (Subjects):** Това са управляеми или неуправляеми хостове, които имат достъп до мрежата в която се изпълнява NAC. Обикновено хостовете са настолни компютри, лаптопи и сървъри, но могат също така да бъдат и IP телефони, мрежови принтери и други свързани към мрежата устройства. Субектите използват софтуерен агент за оценка на състоянието и чрез него общуват с устройствата на NAC. Например програмата Cisco Trust Agent представлява една решение на Cisco за такъв агент.

- **Изпълнителни устройства (Enforcement devices):** Това се мрежови устройства, действащи като точки за прилагане на правилата на NAC. Към тях причисляваме маршрутизаторите за достъп, VPN шлюзовете, комутаторите Catalyst на Cisco работещи в слой 2 и слой 3, както и безжичните точки за достъп.

- **Устройства за решаване и възстановяване (Decision and remediation devices):** В тази група много и различни мрежови устройства поддържат NAC рамковата архитектура:

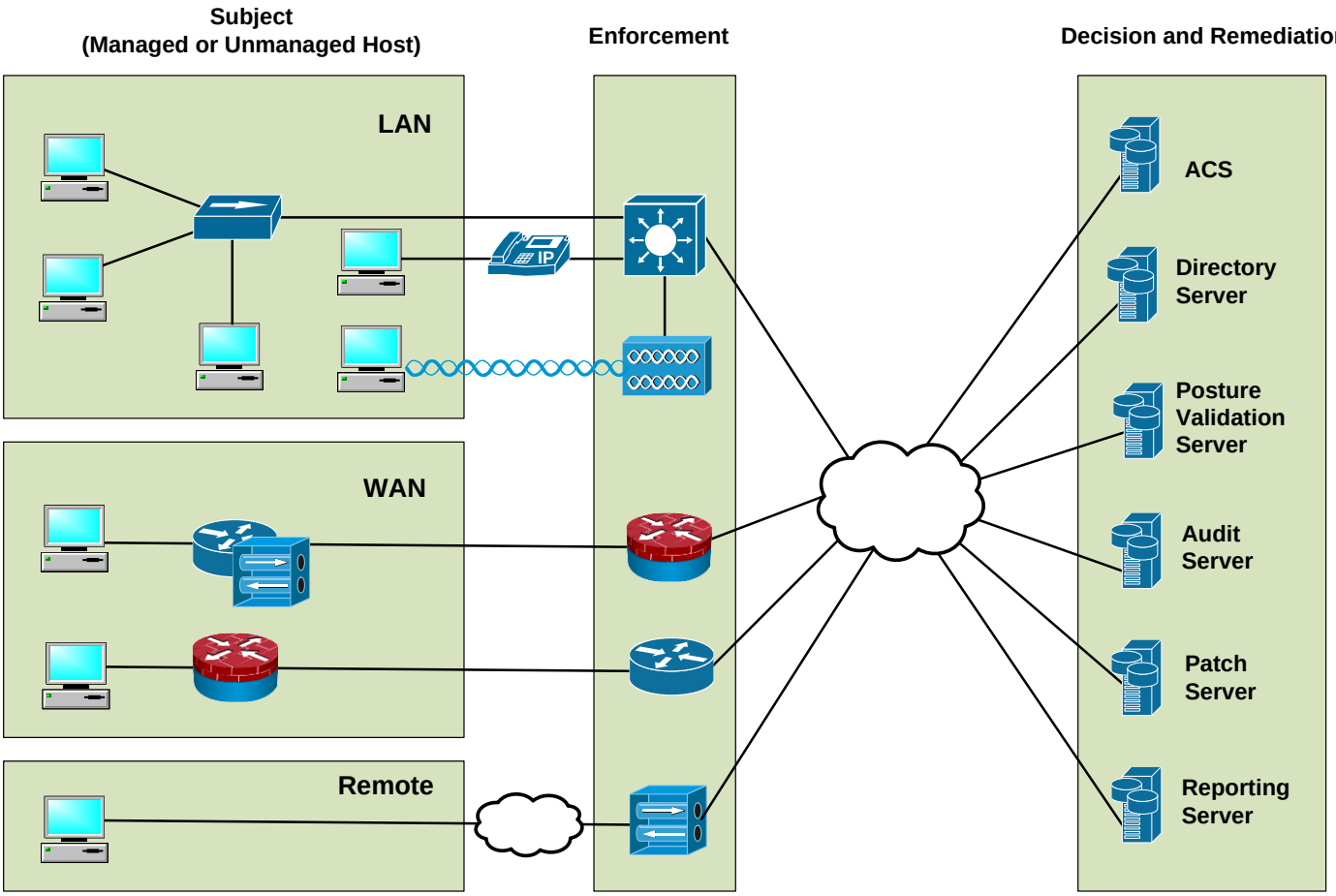
- **Authentication, authorization, and accounting (AAA) server:** Това е централният сървър за политика, който обобщава едно или няколко удостоверявания и разрешения в едно решение, което записва в мрежовия профайлер за изпълнение от мрежовите устройства за достъп. Сървърът AAA на Cisco, който поддържа NAC, се нарича Cisco Secure Access Control Server (ACS).

- **Директориен сървър (Directory server)**: Това е централният директориен сървър, който удостоверява самоличността на потребителя или машината. Като примери тук можем да дадем Microsoft Active Directory, Novell Directory Services (NDS), и сървърите за еднократни пароли.

- **Сървър за валидиране на състоянието (Posture validation server - PVS)**: Този сървър действа като точка за взимане на решения в зависимост от конкретната политика в NAC. В зависимост от възприетата политика той определя набора от необходимите идентификационни данни. Като примери можем да посочим антивирусните сървъри и сървърите за сигурни приложения.

- **Сървър за възстановяване (Remediation server):** В него се прилагат управляващите решения за привеждане на несъответстващите хостове в съответствие. Това може да става със специализирани приложения за управление на кръпките или просто това да е уеб сайт за разпространение на софтуер.

- **Сървър за одит (Audit server)**: Това е сървър или софтуер, който извършва оценка на уязвимостта на хоста за да определи неговото ниво на съответствие или риск преди допускането му до мрежата.



Фиг. 12 Архитектура на NAC Framework

6.1 Поддръжка на NAC Framework от маршрутизаторите

Механизмът на IP NAC в слой 3 използва протоколите EAP (Extensible Authentication Protocol) и UDP (User Datagram Protocol). Маршрутизаторите които поддържат този механизъм се разглеждат като устройства от типа NAC Release 1.0. Те могат да действат като система предотвратяваща проникването в мрежата (Network Intrusion-Prevention System - NIPS). Такива устройства се появиха за първи път в средата на 2004 година и бяха включени в операционната система Cisco IOS Software Release 12.3(8)T. Тогава бяха въведени защитните стени, NIPS и криптографската поддръжка. При механизма IP NAC в слой 3 се извършват само идентификационни проверки за издаване на разрешения за достъп, URL пренасочване и изтегляне на ACL. Този механизъм се задейства от входящ пакет в интерфейса на маршрутизатора когато в него е конфигуриран ACL. Той се използва главно при внедряване на агрегирани решения (WAN, VPN, WLAN, и други) и главно в разпределителния слой на корпорацията, тъй като Catalyst Layer 3 комутаторите не го поддържат.

Хостове без агенти на NAC (NAC Agentless Host - NAH) е друг механизъм на NAC, който позволява достъп до мрежата на хостове, които не могат да бъдат привеждани в съответствие с NAC. Към тази категория принадлежат принтерите, скенерите, фотокопирните машини, камерите, сенсорите и специализираното оборудване. Тук попадат също компютрите с неподдържани операционни системи, с вградените операционни системи, както и персоналните защитни стени. За тях могат да бъдат конфигуриране статични изключения, които да позволяват заобикалянето на процеса на валидиране на състоянието за отделни MAC и IP адреси. Тези статични изключения могат да бъдат конфигурирани в ACS. При конфигурирането могат да се използват както индивидуални, така и заместващи (wildcard) адреси.

Устройствата, които поддържат или механизма на IP NAC в слой 2 (протоколи EAP и UDP) или NAC 802.1X в слой 2 (протоколи EAP и 802.1X), се смятат за устройства от типа NAC Release 2.0. Механизмът IP NAC в слой 2 се задейства от появата на ARP или евентуално DHCP трафик в интерфейса на комутатора. При него също се извършват само идентификационни проверки за издаване на разрешения за достъп, URL пренасочване и изтегляне на ACL. Сесиите при IP NAC в слой 2 са активни докато хостът отговаря на периодичните съобщения за неговото състояние имплементирани в ARP. Списъците за контрол на достъпа ACL, които определят политиката по подразбиране в даден порт на IP NAC в слой 2 комутатора са реализирани хардуерно. Едно от основните предимства на механизма IP NAC в слой 2 е това, че той е проектиран да поддържа множество хостове за даден порт. Все пак администраторът на мрежата трябва да е наясно, че за разлика от механизма IP NAC в слой 3, при механизма IP NAC в слой 2 броят на хостовете за даден порт е ограничен. Някои модули на комутаторите от платформата Cisco ISR поддържат IP NAC в слой 2 или NAC 802.1X в слой 2.

6.2 Поддръжка на NAC Framework от комутаторите

NAC извършва валидиране на състоянието на границата на слой 2 за хостовете със или без позволен 802.1X. Уязвимите и несъответстващи хостове могат да бъдат изолирани, като получат непълен, намален достъп до мрежата, или пренасочени към сървърите за възстановяване в зависимост от организационната политика. Като гарантират, че всеки хост отговаря на политиката за сигурност, организациите могат значително да намалят щетите, причинени от заразени хостове.

Само някои комутатори от определени платформи магат да бъдат използвани при такова внедряване.

7. Преглед на IDS и IPS

Системите за откриване на нарушители и за предотвратяване на нарушения са част от архитектурата SAFE на Cisco. Създадени да идентифицират и спират различните вируси, червеи и друг злонамерен трафик, тези системи могат да помогнат за защита на мрежата. Cisco предоставя широка гама от решения за откриване и предпазване от нарушители както за мрежата, така и за нейните крайни точки.

В този раздел е направен преглед на системите за откриване на нарушители (intrusion-detection systems - IDS) и на системите за предотвратяване на нарушения (intrusion-prevention systems - IPS), които се използват в корпоративните мрежи.

7.1 Откриване на заплахи и ограничаване на тяхното въздействие

Откриването на заплахите и атаките, както и ограничаването на тяхното въздействие, е много важна част от стратегията за мрежова сигурност.

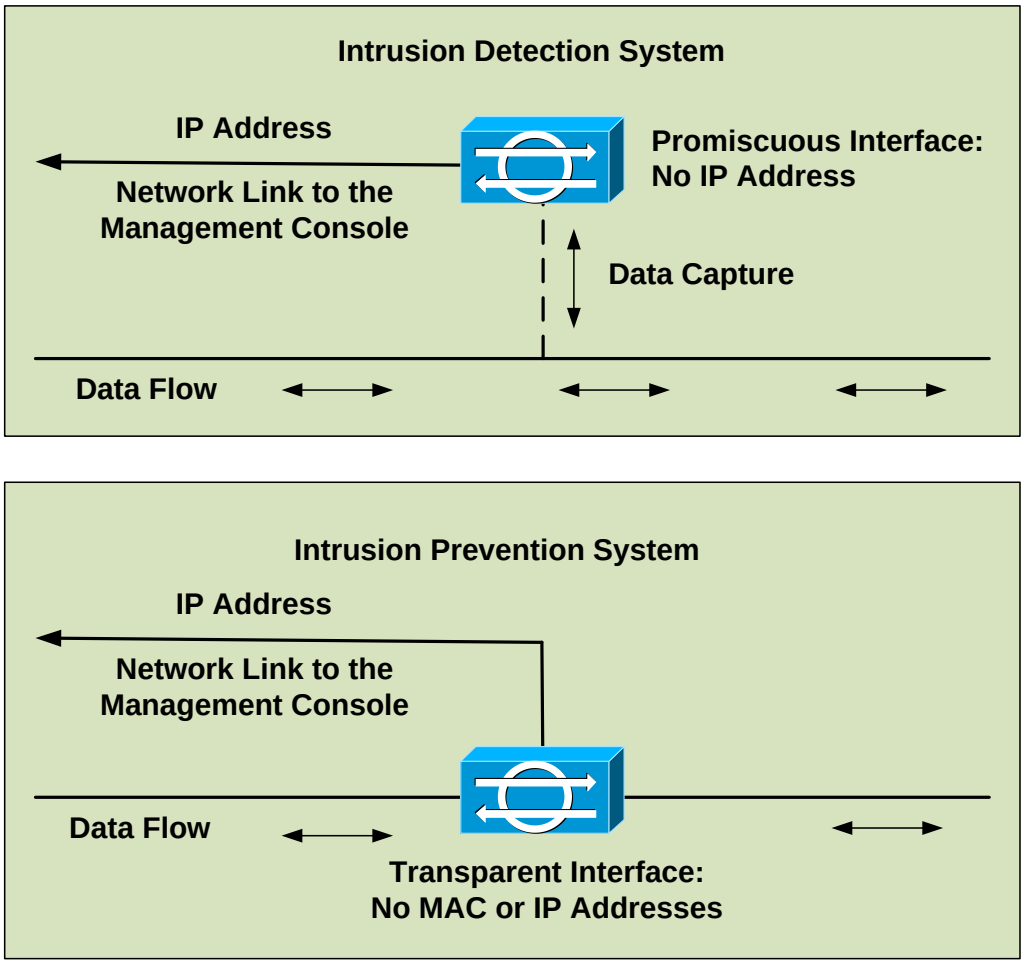
Поради все по-усъвършенстваните атаки, решенията за проверка на сигурността само в определени точки не са вече така ефективни. Сегашната обстановка изисква усъвършенствано наблюдение, което се постига с по-висока интелигентност на инфраструктурата и на сътрудничество между мрежовите устройства. Системата SAFE на Cisco използва различни форми на мрежова телеметрия намиращи се в мрежовото оборудване, в специализираните устройства за сигурност, както и в крайните потребителски точки, с което се постига последователна и точна видимост на мрежовата активност. Информацията за събитията, която се генерира в маршрутизаторите, комутаторите, защитните стени, IPS и крайните точки, се събира, следят се различни трендове и се изчисляват определени зависимости. Архитектурата също използва възможностите за сътрудничество на отделните платформи за сигурност, като IPS, защитните стени и защитаващия крайните точки софтуер.

Системата SAFE на Cisco използва вградената интелигентност и възможностите за сътрудничество на продуктите на Cisco за да контролира и намалява отрицателния ефект от добре известните, както и от напоследък появилите се атаки. Системите за предотвратяване на нарушения, защитните стени, NAC, софтуерът защитаващ крайните точки, както и системите за наблюдение и анализ, работят съвместно за да се идинтифицират атаките и те да получат динамичен отговор. Архитектурата е в състояние да идентифицира източника на заплахата, да визуализира пътя на атаката и да предложи (и дори динамично да наложи) ответни действия. Тези ответни действия включват изолиране на компрометираните сестеми, ограничаване на скоростта, прекратяване на връзки, филтриране на пакети и филтриране на източници.

IDS и IPS са жизнено важни компоненти в този процес. Тези устройства могат да бъдат реализирани както хардуерно, така и да бъдат част от операционната система на защитните стени.

7.2 Системи за откриване на нарушители

Системите IDS пасивно подслушват мрежовия трафик, както е показано на Фиг. 13. IDS не се намира на пътя на трафика, но разполага с копие на целия трафик и го следи внимателно. Обикновено само един интерфейс на IDS следи и наблюдава дадена мрежа. Останалите интерфейси могат да се използват за наблюдение на други мрежи. Когато системата IDS открие зловреден трафик, тя изпраща сигнал към управляващата станция. Също така тя може да изпрати и искане към крайния хост за прекратяване на всички зловредни TCP връзки.



Фиг. 13 IDS и IPS

При този случаен, хаотичен режим (promiscuous mode), пакетите не преминават през сензора. Сензорът анализира копие на наблюдавания трафик. Предимството на работа в този режим е, че сензорът не оказва никакво влияние върху препредавания трафик. Недостатък обаче е това, че сензорът не може да спре зловредния трафик и той достига предвидената цел. При атакуване с единични пакети това може да се окаже фатално. Ответните акции при устройства в този режим настъпват по-късно и обикновено е необходима помощта на други мрежови устройства (например маршрутизатори и защитни стени), за да се отговори на атаката.

7.3 Системи за предотвратяване на нарушения

Както е показано на Фиг. 13, IPS са активни устройства на пътя на трафика. IPS слуша мрежовия трафик и разрешава или забранява потока и пакетите да преминат през него. Входящите (inline) интерфейси нямат MAC или IP адреси и не могат да бъдат открити директно. Целият трафик преминава през IPS за проверка. Трафикът пристига по един IPS интерфейс и напуска по друг. Когато IPS открие зловреден трафик, системата изпраща сигнал към управляващата станция и може да блокира този трафик незабавно. Оригиналният и последващ зловреден трафик е блокиран, така че IPS активно предотвратява атаки и предпазва мрежата от вируси, червеи, зловредни приложения и други уязвимости. Един IPS прилича на мост в каналния слой. По подразбиране IPS пропуска всички пакети, освен ако не изпълнява специална политика за отказ.

Тъй като IPS директно е включен в потока на трафика, то тази система оказва влияние на скоростите на препредаване, като внася забавяне. Това позволява на сензора да спре атаките като изхвърли зловредния трафик преди той да достигне до целта, осигурявайки по този начин защитата. Трафикът може да бъде проверяван и за по-сложни вградени атаки

засягащи елементи от трети до седми слой. Такъв по-задълбочен анализ позволява на системата да идентифицира и да спре или блокира атаки, които нормално биха преминали през традиционните защитни стени.

7.4 Компоненти на IDS и IPS

Има два основни компонента в IDS и IPS:

- **Сензори (Sensors):** Сензорът може да се разположи или във хоста, като например агент за сигурност (Cisco Security Agent), или в мрежата, като например IPS устройство (IPS appliance). Сензорите за мрежа (network-based sensors) използват специализиран софтуер и хардуер за събиране и анализиране на мрежовия трафик. Те могат да бъдат както отделни устройства, така и модули в маршрутизаторите и комутаторите. Има три вида IDS или IPS технологии:

    - Съдържателно претърсващи (signature-based) IDS или IPS, които претърсват трафика за специфични, предварително дефинирани модели или образци. Тези образци се сравняват с база данни от известни атаки и се изпраща сигнал към управляващата станция или такъв трафик се блокира когато се намери съвпадение.

    - IDS или IPS системи, които търсят дефекти или аномалии в пакетите и протоколите (anomaly detection systems) и проверяват дали има някакво ненормално поведение на трафика.

    - IDS или IPS основани на политика (policy-based), чието конфигуриране следва определена мрежова политика за сигурност и чията задача е да открият трафик неоговарящ на тази политика.

- **Управление на сигурността и наблюдение на инфраструктурата (Security management and monitoring infrastructure):** Конфигурира сензорите и служи като място за събиране на алармите, за наблюдение и управление на сигурността. Задачата на приложенията за наблюдение и управление е да разпознават алармите, да агрегират информацията и да търсят взаимни свързаности. Тук се използва система за централизирано конфигуриране и наблюдение на защитните стени, VPN и IPS, която има и наблюдателни функции. Системата на Cisco за наблюдение на сигурността, анализ и отговор (Cisco Security Monitoring, Analysis, and Response System - MARS) осигурява наблюдение на устройствата по сигурността в мрежата и хостовете. Cisco IPS Device Manager (IDM) е уеб базирано Java приложение, което позволява конфигурирането и управлението на IPS сензорите. IDS Event Viewer е Java приложение, което позволява на мрежовите администратори да наблюдават и управляват алармите на до 5 сензора.

Забележка: Приложението Cisco IPS Device Manager беше заменено със Cisco IPS Manager Express. IPS Manager Express (IME) комбинира възможностите на IDM и на IDS Event Viewer, като едновременно с това е добавена и възможността за наблюдение и управление на до 5 сензора. IME изисква наличието на последните версии на софтуера на сензорите. Това приложение не е проектирано да работи със сензорната имплементация в Cisco IOS.

7.5 IPS за хост

Внедряването на IPS за хост включва два компонента:

- **Агенти в крайните точки (Endpoint agents):** Те налагат политиката за сигурност, получена от сървъра за управление. Тези агенти изпращат информация за събитията към сървъра за управление и взаимодействат ако е необходимо с потребителя. Целта

на агента в крайната точка е да осигури защитата от заплаха за потребителската система. Като агент в крайните точки се използва Cisco Security Agent, който осигурява защитата на сървърите и настолните компютри. Той се намира между ядрото на операционната система на компютъра и приложенията, като осигурява максимална видимост на приложението с минимално въздействие върху стабилността и производителността на операционната система.

- **Управляващ сървър (Management server):** Внедрява политиките за сигурност в крайните точки. Управляващият сървър е отговорен за конфигурирането и поддържането на околната среда. Той получава и съхранява информацията за събитията и изпраща аларми към администраторите. В него се пазят и софтуерните актуализации на клиентите. Обикновено той е снабден с графична конзола, която позволява конфигурирането на определена политика и наблюдение на събитията. За големите системи в него е оформена и специализирана база данни в която се пази информацията. Центърът за управление на агентите предоставя всички функции необходими за внедряването на агентите.

7.6 Съображения при проектирането на IDS и IPS

Основната политика за сигурност трябва да бъде една и съща при разполагането на IDS или IPS. За да не пропуска определен трафик, IPS трябва да бъде разположена в потока на трафика, докато при IDS сензора трафикът не преминава през него. Всъщност IDS анализира копие на наблюдавания трафик, а не реално преминаващите пакети. Ако вашата политика за сигурност не предвижда отхвърляне на трафик, то използвайте IDS.

IDS или IPS сензорите се поставят на такива места в мрежата, където те могат ефективно да подкрепят основната политика за сигурност. Решенията за разполагане често се определят от това, къде възможно най-бързо можете да откриете и спрете нарушителя. Типичните сценарии предвиждат поставянето на сензорите в периметъра на мрежата извън защитната стена, където мрежата е най-експонирана, след защитната стена на границата между зоните за доверие, както и в критичните сървъри, където инцидент би струвал твърде скъпо. Например поставянето им извън защитната стена генерира много предупреждения които са сравнително маловажни понеже е малко вероятно да се предприемат действия въз основа на тази информация.

Използването на IPS оказва по-голямо влияние върху трафика отколкото IDS. Повреда в IDS означава, че просто наблюдаването на трафика ще спре. Повреда в IPS може да прекъсне потока на мрежовия трафик, освен ако не са взети специални мерки за неговото пренасочване. Освен това IPS въвежда забавяне на пакетите. Стараем се това забавяне да остане в границите под една милисекунда. IPS имат ограничения на размера на трафика, който може да премине през устройството. Превишаването на производителността на сензора води до отхвърлени пакети и общо влошаване на работата в мрежата.

7.7 Съображения за разполагане на IDS или IPS

IDS или IPS сензорите могат да бъдат разположени въз основа на приоритета на целите. Интернет и екстранет връзките обикновено се защитават първо поради експозицията си. IDS извън защитната стена може да открие всички атаки и да генерира множество аларми, но тя е изключително полезна за анализирането на това, какъв трафик е насочен към организацията и как се изпълняват атаките. IDS след защитната стена може да открие нейно неправилно конфигуриране, като покаже какъв вид трафик преминава през нея. IPS може да осигури по-фокусирана защита на приложенията и да подкрепи защитната стена в защитата на екстранет и ресурсите в демилитаризираната зоно (DMZ).

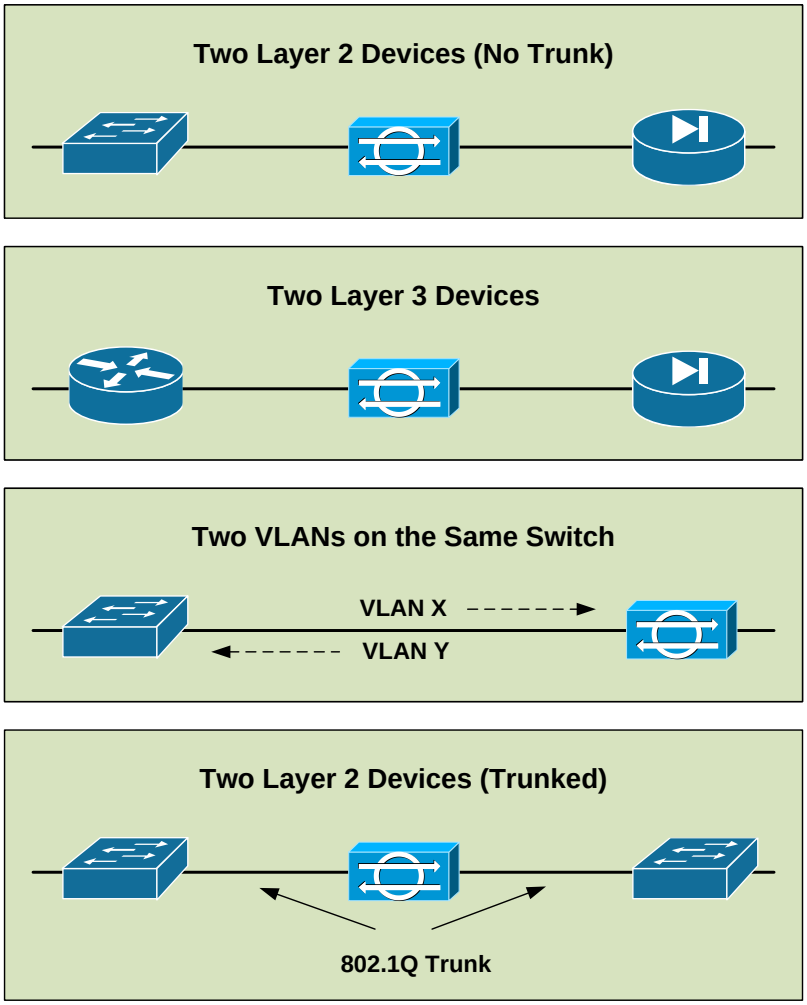
Мрежите за управление и изчислителните центрове често са следващи по приоритет. За максимална защита на зони с висока сигурност е подходящо използването на слоест подход.

Тук можем да имаме инсталирана една система след защитната стена и втора система във входната точка на зоната с висока сигурност, като например изчислителния център. IDS за хост може да открива атаките към определен сървър. IPS може да се използва да блокира специфичния трафик, който не трябва да достига до сървъра.

Внедряването на IPS в отдалечените офиси и клонове на фирмата защитава както клона от настъпили инциденти във фирмата, така и ресурсите на фирмата от неправилни практики прилагани в някои клонове. Системите за отдалечен достъп също трябва да бъдат защитени.

7.8 Избор на място на IPS устройствата

Когато избирате място на IPS сензора в корпоративната мрежа, имате на разположение няколко варианта в зависимост от инфраструктурата и очакваните резултати. На Фиг. 14 са показани тези варианти.



Фиг. 14 Място на IPS устройствата

- **Две устройства от слой 2, не магистрала (Two Layer 2 devices, no trunk):** Разполагането на сензора между две устройства от слой 2, като връзката между тях не е магистрала, е типично за кампуса на корпорацията. Устройството се поставя между два комутатора. IPS може да бъде в една VLAN между два различни комутатора, или между различни VLAN в обща подмрежа и два различни комутатора. Сценарият включва поставянето на устройството между различни зони на сигурност в кампуса или между критични устройства в изчислителния център.

- **Две устройства от слой 3 (Two Layer 3 devices):** Разполагането на сензора между две устройства от слой 3 е често срещано в Интернет, кампуса или изчислителния

център. Двете устройства от слой 3 са в една и съща подмрежа. Предимството при този сценарий е лесното конфигуриране, защото интегрирането се осъществява без да се налагат промени в които и да са други устройства.

- **Две VLAN в един комутатор (Two VLANs on the same switch):** Този дизайн позволява сензорът да свърже като мост две VLAN в един и същ комутатор. Сензорът получава пакетите по едната VLAN и ги изпраща в другата VLAN. Двете VLAN трябва да бъдат в една и съща подмрежа.

- **Две устройства от слой 2 свързани с магистрала (Two Layer 2 devices, trunked):** Поставянето на сензора на магистрала между комутатори е често срещан сценарий, при който от едно място защитаваме няколко VLAN.

IPS може да асоциира две VLAN върху физически интерфейс. Пакетите получавани по едната VLAN се анализират, след което се препращат по другата VLAN. Сензорът прехвърля пакетите от едната VLAN в другата, като и двете VLAN са на една и съща магистрала и в една и съща подмрежа. Сензорът променя полето VLAN ID в заглавната част на протокола IEEE 802.1Q. Този дизайн поддържа много VLAN двойки за един физически интерфейс, с което се намалява броя на необходимите физически интерфейси в дадено шаси.

7.9 Предизвикателства при разполагането на IPS

Предизвикателства при разполагането на IPS представляват асиметричния трафик и изискванията за висока степен на наличност (high availability).

Традиционните потоци в мрежата са симетрични и минават по едни и същи връзки в двете посоки. Много нови мрежови решения не гарантират симетричност на потоците, тъй като инженерите желаят да се възползват от всички налични връзки. Това значително увеличава вероятността трафикът да преминава по различни пътища към и от неговото местоназначение.

Тази асиметричност на трафика може да създаде проблеми с вградените IPS устройства. Понеже IPS сензорът проверява пълното състояние на трафика, т.е. инспектира го statefully, той трябва да се увери, че и двете страни на връзката функционират правилно. Наличността на асиметричен трафик може да причини валиден трафик да бъде отхвърлен.

Друго предизвикателство е изискването за висока степен на наличност. Повреда във всеки излишен (redundant) компонент в мрежата не трябва да води до прекъсване в наличността на мрежата. Това означава, че съществуващите сесии трябва да продължат нормално, а не да бъдат прекратени.

Сегашната версия 6.0 на софтуера на IPS не поддържа асиметрични потоци и висока наличност. Това се заобикаля, като се използва поддържането на огледално копие на целия трафик между два сензора в случай на срив. Двата IPS сензора в двойката наблюдават всички пакети преминаващи през дадена точка в мрежата. Ако единият сензор по някаква причина се повреди, мрежата преориентира целия трафик през другия сензор, тъй като той е на единствения път. Вторият сензор има вече напълно изградена таблица на състоянията на потоците, така че трафикът не се прекъсва. Асиметричният трафик също се поддържа от тази огледална технология.

7.10 Варианти за управляващия интерфейс на IDS или IPS

Наблюдението на IDS или IPS е един от най-важните елементи за осигуряване на бързото откриване на подозрителни действия и е показател за предотвратените атаки. Управлението на IDS или IPS обединява и централизира атаките от различни източници за да осигури необходимото виждане за мрежата.

Покупката на IDS или IPS без необходимото обучение на персонала и допълнителните инструменти значително намалява тяхната стойност. Основната разлика е, че при IDS без съответното наблюдение не се прави нищо за да се блокира злонамерения трафик. IDS без център по сигурността най-много да доведе до прекъсване на връзката на даден потребител. Ако това е направено без съществено основание, то такъв потребител най-вероятно ще бъде доста сърдит. Компенсирането на липсата на персонал с използване на IPS обикновено води до недобри отношения с потребителите.

На границата на мрежата сензорите обикновено се инсталират в близост до защитна стена. Наблюдението и управлението на интерфейсите на IPS може да се извършва от две различни мрежи. Това е особено важно, когато външният сензор трябва да комуникира с вътрешната мрежа.

Единият вариант е интерфейсът за наблюдение да се свърже към външната мрежа, а интерфейсът за управление директно към вътрешната мрежа. Цялото управление се извършва по вътрешната мрежа. Такава настройка е много проста, но дава път около защитната стена в случай, че сензорът е компрометиран. Това не се препоръчва.

За предпочитане е да оставим интерфейса за наблюдение във външната мрежа, а управляващия интерфейс да включим към отделна вътрешна VLAN. В този случай управляващият интерфейс е изолиран от останалата вътрешна мрежа. Ако тази VLAN е с достатъчна степен на доверие, то архитектурата осигурява добро отделяне на IDS или IPS сензора. Препоръчителната практика е да се използват протоколите Secure Shell (SSH) или Secure Sockets Layer (SSL) за управляващ достъп до IDS или IPS сензорите.

Използването на PVLAN за да свържем всички сензори към изолирани портове е препоръчително, тъй като сензорите не е необходимо да се свързват един с друг, освен когато възнамеряваме да използваме разпределено блокиране. Така при компрометиране на един сензор останалите остават незасегнати.

Друг вариант може да бъде управлението на IDS или IPS да се извършва с отделна мрежа (out-of-band) или през сигурни тунели, в зависимост от местонахождението на сензорите.

За устройствата извън периметъра на защитната стена, интерфейсът за наблюдение остава във външната мрежа, но управляващият итнерфейс завършва в отделна DMZ. Управлението се извършва през криптиран тунел. Защитната стена защитава външния сензор от вътрешните устройства и осигурява по-добро разделяне в сравнение с предишното решение. За вътрешните устройства намиращи се в по-защитените области управлението се извършва в отделни VLAN за управление.

7.11 Наблюдение и управление на IDS и IPS

Cisco Security MARS и CSM (Cisco Security Manager) са части от комплекта Cisco Security Management Suite, който доставя политиките за администриране и изпълнение в защитаваната мрежа. Тези два инструмента следва да работят в управляваща VLAN в защитено място, като например в изчислителния център.

Cisco Security MARS осигурява връзката между много производители и определя необходимата активна реакция, като разпространява информацията за IPS:

- Доставя предварително дефинирани и лесни за персонализиране доклади за съответствие.

- Съхранява информацията за настъпили събития за всеки тип устройство. Тази информация може да бъде групирана в един доклад.

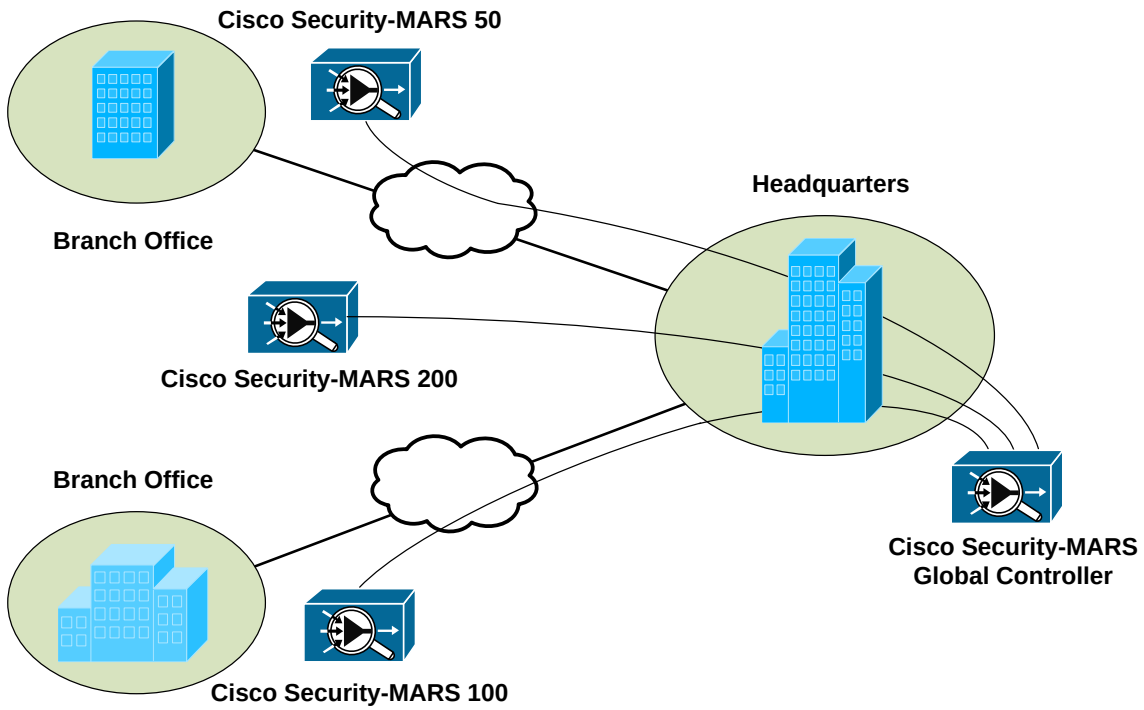
За организации с малък до среден размер Cisco Security MARS е изграден като локален контролер.

Забележка: В Cisco Security MARS под локален контролер (local controller) разбираме хардуерно устройство, което поддържа разгледаните функции за наблюдение, анализ и отговор. Глобалният контролер (global controller) е устройство използвано за централизиране на операциите и управлението на много локални контролери в разпределена среда

CSM дава възможност на организациите да управляват политиките си за сигурност като използват устройства за сигурност на Cisco. CSM осигурява интегрирана поддръжка на VPN и защитните стени от страна на Cisco IOS маршрутизаторите, Cisco PIX и ASA устройствата, както и от модулите за услуги на Cisco Catalyst 6500/Cisco 7600. CSM също така поддържа IPS технологиите в маршрутизаторите, в модулите за услуги и IPS устройствата.

CSM, чрез своя компонент Cisco IPS Manager, поддържа управлението и конфигурирането на IPS сензорите (устройства, комутиращи модули, мрежови модули, модули обслужващи сигурността). Потребителите конфигурират IPS сензорите и Cisco IOS IPS устройствата като използват политики, всяка една от които определя различна част от конфигурацията на сензора. Cisco Security Manager 3.1 осигурява напълно интегрирани IPS функции.

Глобалният контролер на Cisco Security MARS позволява мащабирането на наблюдението на мрежата, както е показано на Фиг. 15.



Фиг. 15 мащабиране на Cisco Security MARS с използване на глобален контролер

Ако една организация разполага с няколко локални контролери на Cisco Security MARS, тя може да въведе разпределено решение, като използва глобален контролер за да обощи информацията от два или повече локални контролера, както и да управлява тези локални контролери. Глобалният контролер комуникира по протокола Hypertext Transfer Protocol Secure (HTTPS), като използва сертификати. Глобалният контролер разпространява новини, правила, шаблони за отчети, правила за достъп, както и заявки към локалните контролери.