Platinum Bank: информационная безопасность с решениями от Cisco

Внедрение Cisco Identity Services Engine для управления политиками доступа к корпоративной сети банка

Заказчик:
Platinum Bank

Отрасль:
Банковские услуги

Регион:
Киев, Украина

Интегратор:
Компания VERNA

Решение:

- проведение анализа сетевой инфраструктуры головного офиса банка в Киеве, проводного и беспроводного сегмента
- разработка проекта внедрения платформы Cisco Identity Services Engine в инфраструктуру банка и его реализация
- создание и согласование сценариев доступа в корпоративную сеть с проводных и беспроводных устройств
- управление гостевым доступом и подключением устройств в рамках концепции BYOD
- создание развитой системы администрирования и предоставления полномочий по доступу в сеть

Преимущества:

- единая политика информационной безопасности для всех уровней сетевого доступа
- единая точка управления и контроля подключений в корпоративную сеть
- гибкие сценарии предоставления доступа с атрибутами MSAD
- аутентификация по сертификатам с атрибутами MSCA для проводных и беспроводных подключений
- повышение гибкости применения политик безопасности благодаря технологии 802.1X

История успеха

Информационная безопасность: не снижая планки

Проект модернизации системы информационной безопасности в головном офисе Platinum Bank в Киеве можно назвать плановым. Основная проблема или задача, которую предполагалось решить, была четко сформулирована на самом старте проекта. Анализ сетевой инфраструктуры в ходе создания рабочего проекта инженерной командой VERNA позволил уточнить список требований. Необходимо было обеспечить автоматизацию настроек при подключении пользователей к сети, отключении или перемещении пользовательских устройств. Предполагалось, что должно быть обеспечено до 3500 подключений с возможностью увеличения их количества до 5000. Головной офис банка в Киеве – это три территориально разнесенныерабочие площадки, объединенные единой корпоративной сетью. На них в общей сложности работает порядка 500 сотрудников – для такого штата планируемое количество поддерживаемых подключений вполне достаточно.

На момент реализации проекта в банке успешно использовались удаленные подключения через Cisco VPN Client. Однако в связи с окончанием жизненного цикла этого продукта и завершением его поддержки было принято решение о переходе на новый клиент для удаленного доступа Cisco AnyConnect.

Сергей Попов, директор по информационным и коммуникационным технологиям Platinum Bank

---

Другой задачей была разработка единой политики информационной безопасности для проводных и беспроводных подключений к сети. Вместе с тем, унифицированный подход не исключает возможность гибкой настройки прав доступа, что для Platinum Bank было крайне важно. Особенно с учетом того, что банк предоставляет гостевой доступ своим партнерам и подрядчикам, и система должна управлять полным жизненным циклом гостевого подключения.

Наконец, менеджмент банка активно использует в офисе свои персональные устройства на различных платформах – iOS, Android и Windows 8. Для регистрации этих устройств в сети и контроля доступа специалисты VERNA предложили использовать технологию BYOD (от англ. Bring Your Own Device, что в переводе означает «Принеси на работу свое персональное устройство»), которая позволяет существенно снизить нагрузку на администраторов сети.

Cisco Identity Services Engine – для администратора и пользователя

Наряду с переходом на новый клиент для удаленного доступа Cisco AnyConnect, банку требовалось комплексное решение для управления доступом в сеть. Им стало Cisco Identity Services Engine (Cisco ISE). И это не удивительно. Корпоративным стандартом для сетевого оборудования в банке являются продукты Cisco, и по таблице совместимости уже установленное в банке сетевое оборудование Cisco полностью отвечало требованиям, предъявляемым Cisco ISE. Работающую инфраструктуру не нужно было менять. Но, разумеется, привлекательность Cisco Identity Services Engine объясняется далеко не только совместимостью с другими продуктами Cisco.

С точки зрения администратора, преимущества выбранного решения очевидны: централизованное управления практически всеми аспектами предоставления доступа к корпоративной сети и автоматизация многих процедур значительно упрощает работу. Так, например, если пользователь перемещается с одного рабочего места на другое, администратору не нужно менять настройки сети. Назначение соответствующих сетевых политик для этого пользователя происходит автоматически.

Управление доступом осуществляется с использованием политик для определенных групп безопасности. Причем система позволяет это делать достаточно гибко: если для одного или нескольких пользователей из группы необходимо запретить доступ к сетевым ресурсам, это можно легко сделать с помощью дополнительных атрибуты из каталога Active Directory, которые можно задать в ручном режиме. В согласовании политик предоставления доступа пользователям и ПК к корпоративной сети заключалась, пожалуй, основная сложность этого проекта. Необходимо было структурировать MSAD, создать шаблоны сертификатов и затем определить политики доступа на основании привязанности к группам MSAD.

Более 4000 заказчиков по всему миру используют Cisco ISE для централизованного управления всеми видами доступа в сеть. Внедрение ISE делает процесс подключения устройств в сеть безопасным, управляемым и наблюдаемым. Кроме того, для безопасного подключения гостевого или персонального мобильного устройства после внедрения ISE требуются минуты, а не часы, как раньше. Положительный эффект виден уже в первый год после внедрения.

Владимир Илибман,
менеджер по продуктам безопасности Cisco Systems

Проект завершен, полет нормальный

С момента согласования технического задания до ввода новой системы в эксплуатацию прошло 9 месяцев. За это время была создана концепция предоставления доступа в проводную и беспроводную сеть, решена задача поддержки подключения по VPN с помощью клиента Cisco AnyConnect, налажена система аутентификации для гостевых подключений, разработаны политики авторизации с привязкой к AD-группам. С помощью специалистов VERNA были проведены испытания работоспособности системы при сбое одного из серверов, а также создан план восстановления работоспособности системы. Одним из основных результатов стала большая прозрачность сетевой среды для администраторов.

После внедрения Cisco ISE все устройства, подключаемые к корпоративной сети, стали персонализированными. Каждое устройство и каждый пользователь видны под своим именем. Гостевые подключения также персонализированы. И на консоли управления можно отследить всю историю подключений ПК либо пользователя к корпоративной сети.

Кирилл Карнаухов,
ведущий специалист отдела «Сети и Телекоммуникации», компания VERNA

В результате модернизации системы информационной безопасности Platinum Bank получил масштабируемое и отказоустойчивое решение с централизованной системой AAA (Authentication, Authorization, Accounting) – системой аутентификации, авторизации и учета событий. Проще администрировать, удобнее пользоваться.

Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
Космодамианская наб.,
д. 52, стр. 1, 4 этаж
Телефон: +7 (495) 961 1410,
факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова,
д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230,
факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600,
факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691,
факс: +375 (17) 269 1699
www.cisco.ru, www.cisco.com

Казахстан, 050059, Алматы,
бизнес-центр «Самал Тауэрс»,
ул. О. Жолдасбекова,
97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101,
факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, «Лэндмарк»
здание III, 3 этаж
Телефон: +994 (12) 437 4820,
факс: +994 (12) 437 4821

Узбекистан, 100000, Ташкент,
бизнес-центр INCONEL,
ул. Пушкина, 75, офис 605
Телефон: +998 (71) 140 4460,
факс: +998 (71) 140 4465