14. Лекция: Туннелирование и управление

Туннелирование

На наш взгляд, ***туннелирование*** следует рассматривать как самостоятельный сервис безопасности. Его суть состоит в том, чтобы "упаковать" передаваемую порцию данных, вместе со служебными полями, в новый "конверт". В качестве синонимов термина "*туннелирование*" могут использоваться "***конвертование***" и "***обертывание***".

Туннелирование может применяться для нескольких целей:

- передачи через сеть пакетов, принадлежащих протоколу, который в данной сети не поддерживается (например, передача пакетов IPv6 через старые сети, поддерживающие только IPv4);
- обеспечения слабой формы *конфиденциальности* (в первую очередь *конфиденциальности трафика*) за счет сокрытия истинных адресов и другой служебной информации;
- обеспечения *конфиденциальности* и целостности передаваемых данных при использовании вместе с криптографическими сервисами.

Туннелирование может применяться как на сетевом, так и на прикладном уровнях. Например, стандартизовано *туннелирование* для IP и двойное *конвертование* для почты X.400.

На рис. 14.1 показан пример обертывания пакетов IPv6 в формат IPv4.

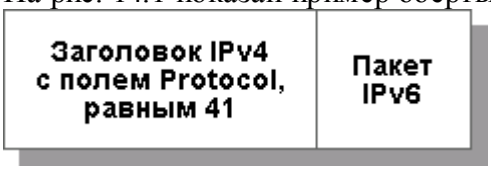

Рис. 14.1. Обертывание пакетов IPv6 в формат IPv4 с целью их туннелирования через сети IPv4.

Комбинация *туннелирования* и шифрования (наряду с необходимой криптографической инфраструктурой) на выделенных шлюзах и экранирования на маршрутизаторах поставщиков сетевых услуг (для разделения пространств "своих" и "чужих" сетевых адресов в духе виртуальных локальных сетей) позволяет реализовать такое важное в современных условиях защитное средство, как ***виртуальные частные сети***. Подобные сети, наложенные обычно поверх Internet, существенно дешевле и гораздо безопаснее, чем собственные сети организации, построенные на выделенных каналах. Коммуникации на всем их протяжении физически защитить невозможно, поэтому лучше изначально исходить из предположения об их уязвимости и соответственно обеспечивать защиту. Современные протоколы, направленные на поддержку классов обслуживания, помогут гарантировать для *виртуальных частных сетей* заданную пропускную способность, величину задержек и т.п., ликвидируя тем самым единственное на сегодня реальное преимущество сетей собственных.

Рис. 14.2. Межсетевые экраны как точки реализации сервиса виртуальных частных сетей.

Концами *туннелей*, реализующих *виртуальные частные сети*, целесообразно сделать *межсетевые экраны*, обслуживающие подключение организаций к внешним

сетям (см. рис. 14.2). В таком случае *туннелирование* и шифрование станут дополнительными преобразованиями, выполняемыми в процессе фильтрации сетевого трафика наряду с трансляцией адресов.

Концами *туннелей*, помимо корпоративных *межсетевых экранов*, могут быть мобильные компьютеры сотрудников (точнее, их персональные МЭ).

Управление

Основные понятия

Управление можно отнести к числу инфраструктурных сервисов, обеспечивающих нормальную работу компонентов и средств безопасности. Сложность современных систем такова, что без правильно организованного управления они постепенно деградируют как в плане эффективности, так и в плане защищенности.

Возможен и другой взгляд на управление – как на интегрирующую оболочку информационных сервисов и сервисов безопасности (в том числе средств обеспечения высокой доступности), обеспечивающую их нормальное, согласованное функционирование под контролем администратора ИС.

Согласно стандарту X.700, управление подразделяется на:

- **мониторинг** компонентов;
- **контроль** (то есть выдачу и реализацию управляющих воздействий);
- **координацию** работы компонентов системы.

Системы управления должны:

- позволять администраторам планировать, организовывать, контролировать и учитывать использование информационных сервисов;
- давать возможность отвечать на изменение требований;
- обеспечивать предсказуемое поведение информационных сервисов;
- обеспечивать защиту информации.

Иными словами, управление должно обладать достаточно богатой функциональностью, быть результативным, гибким и информационно безопасным.

В X.700 выделяется пять функциональных областей управления:

- **управление конфигурацией** (установка параметров для нормального функционирования, запуск и остановка компонентов, сбор информации о текущем состоянии системы, прием извещений о существенных изменениях в условиях функционирования, изменение конфигурации системы);
- **управление отказами** (выявление отказов, их изоляция и восстановление работоспособности системы);
- **управление производительностью** (сбор и анализ статистической информации, определение производительности системы в штатных и нештатных условиях, изменение режима работы системы);
- **управление безопасностью** (реализация политики безопасности путем создания, удаления и изменения сервисов и механизмов безопасности, распространения соответствующей информации и реагирования на инциденты);
- **управление учетной информацией** (т.е. взимание платы за пользование ресурсами).

В стандартах семейства X.700 описывается модель управления, способная обеспечить достижение поставленных целей. Вводится понятие управляемого объекта как совокупности характеристик компонента системы, важных с точки зрения управления. К таким характеристикам относятся:

- **атрибуты объекта**;
- **допустимые операции**;
- **извещения**, которые объект может генерировать;
- связи с другими управляемыми объектами.

Согласно рекомендациям X.701, системы управления распределенными ИС строятся в архитектуре **менеджер/агент**. Агент (как программная модель управляемого

объекта) выполняет управляющие действия и порождает (при возникновении определенных событий) извещения от его имени. В свою очередь, менеджер выдает агентам команды на управляющие воздействия и получает извещения.

Иерархия взаимодействующих менеджеров и агентов может иметь несколько уровней. При этом элементы промежуточных уровней играют двоякую роль: по отношению к вышестоящим элементам они являются агентами, а к нижестоящим – менеджерами. **Многоуровневая архитектура** менеджер/агент – ключ к распределенному, масштабируемому управлению большими системами.

Логически связанной с многоуровневой архитектурой является концепция **доверенного** (или **делегированного**) **управления**. При доверенном управлении менеджер промежуточного уровня может управлять объектами, использующими собственные протоколы, в то время как "наверху" опираются исключительно на стандартные средства.

Обязательным элементом при любом числе архитектурных уровней является **управляющая консоль.**

С точки зрения изучения возможностей систем управления следует учитывать разделение, введенное в X.701. Управление подразделяется на следующие аспекты:

- информационный (атрибуты, операции и извещения управляемых объектов);
- функциональный (управляющие действия и необходимая для них информация);
- коммуникационный (обмен управляющей информацией);
- организационный (разбиение на области управления).

Ключевую роль играет **модель управляющей информации**. Она описывается рекомендациями X.720. Модель является объектно-ориентированной с поддержкой инкапсуляции и наследования. Дополнительно вводится понятие **пакета** как совокупности атрибутов, операций, извещений и соответствующего поведения.

Класс объектов определяется позицией в **дереве наследования**, набором включенных пакетов и внешним интерфейсом, то есть видимыми снаружи атрибутами, операциями, извещениями и демонстрируемым поведением.

К числу концептуально важных можно отнести понятие **"проактивного"**, то есть **упреждающего управления**. Упреждающее управление основано на предсказании поведения системы на основе текущих данных и ранее накопленной информации. Простейший пример подобного управления – выдача сигнала о возможных проблемах с диском после серии программно-нейтрализуемых ошибок чтения/записи. В более сложном случае определенный характер рабочей нагрузки и действий пользователей может предшествовать резкому замедлению работы системы; адекватным управляющим воздействием могло бы стать понижение приоритетов некоторых заданий и извещение администратора о приближении кризиса.

Возможности типичных систем

Развитые системы управления имеют, если можно так выразиться, двухмерную настраиваемость – на нужды конкретных организаций и на изменения в информационных технологиях. Системы управления живут (по крайней мере, должны жить) долго. За это время в различных предметных областях администрирования (например, в области **резервного копирования**) наверняка появятся решения, превосходящие изначально заложенные в управляющий комплект. Последний должен уметь эволюционировать, причем разные его компоненты могут делать это с разной скоростью. Никакая жесткая, монолитная система такого не выдержит.

Единственный выход – наличие **каркаса**, с которого можно снимать старое и "навешивать" новое, не теряя эффективности управления.

Каркас как самостоятельный продукт необходим для достижения по крайней мере следующих целей:

- сглаживание разнородности управляемых информационных систем, предоставление унифицированных программных интерфейсов для быстрой разработки управляющих приложений;
- создание инфраструктуры управления, обеспечивающей наличие таких свойств, как поддержка распределенных конфигураций, масштабируемость, информационная безопасность и т.д.;
- предоставление функционально полезных универсальных сервисов, таких как планирование заданий, генерация отчетов и т.п.

Вопрос о том, что, помимо каркаса, должно входить в систему управления, является достаточно сложным. Во-первых, многие системы управления имеют мэйнфреймовое прошлое и попросту унаследовали некоторую функциональность, которая перестала быть необходимой. Во-вторых, для ряда функциональных задач появились отдельные, высококачественные решения, превосходящие аналогичные по назначению "штатные" компоненты. Видимо, с развитием объектного подхода, многоплатформенности важнейших сервисов и их взаимной совместимости, системы управления действительно превратятся в каркас. Пока же на их долю остается достаточно важных областей, а именно:

- управление **безопасностью**;
- управление **загрузкой**;
- управление **событиями**;
- управление **хранением данных**;
- управление **проблемными ситуациями**;
- генерация **отчетов**.

На уровне инфраструктуры присутствует решение еще одной важнейшей функциональной задачи – обеспечение **автоматического обнаружения** управляемых объектов, выявление их характеристик и связей между ними.

Отметим, что управление безопасностью в совокупности с соответствующим программным интерфейсом позволяет реализовать платформно-независимое **разграничение доступа** к объектам произвольной природы и (что очень важно) вынести функции безопасности из прикладных систем. Чтобы выяснить, разрешен ли доступ текущей политикой, приложению достаточно обратиться к **менеджеру безопасности** системы управления.

Менеджер безопасности осуществляет **идентификацию/аутентификацию** пользователей, контроль доступа к ресурсам и протоколирование неудачных попыток доступа. Можно считать, что менеджер безопасности встраивается в ядро операционных систем контролируемых элементов ИС, перехватывает соответствующие обращения и осуществляет свои проверки перед проверками, выполняемыми ОС, так что он создает еще один защитный рубеж, не отменяя, а дополняя защиту, реализуемую средствами ОС.

Развитые системы управления располагают централизованной базой, в которой хранится информация о контролируемой ИС и, в частности, некоторое представление о **политике безопасности**. Можно считать, что при каждой попытке доступа выполняется просмотр сохраненных в базе правил, в результате которого выясняется наличие у пользователя необходимых прав. Тем самым для проведения единой политики безопасности в рамках корпоративной информационной системы закладывается прочный технологический фундамент.

Хранение параметров безопасности в базе данных дает администраторам еще одно важное преимущество – возможность выполнения разнообразных запросов. Можно получить список ресурсов, доступных данному пользователю, список пользователей, имеющих доступ к данному ресурсу и т.п.

Одним из элементов обеспечения **высокой доступности** данных является подсистема автоматического управления хранением данных, выполняющая резервное

копирование данных, а также автоматическое отслеживание их перемещения между основными и резервными носителями.

Для обеспечения высокой доступности информационных сервисов используется управление загрузкой, которое можно подразделить на управление прохождением заданий и **контроль производительности**.

Контроль производительности – понятие многогранное. Сюда входят и оценка быстродействия компьютеров, и анализ пропускной способности сетей, и отслеживание числа одновременно поддерживаемых пользователей, и время реакции, и накопление и анализ статистики использования ресурсов. Обычно в распределенной системе соответствующие данные доступны "в принципе", они поставляются точечными средствами управления, но проблема получения целостной картины, как текущей, так и перспективной, остается весьма сложной. Решить ее способна только система управления корпоративного уровня.

Средства контроля производительности целесообразно разбить на две категории:

- выявление случаев неадекватного функционирования компонентов информационной системы и автоматическое реагирование на эти события;
- анализ тенденций изменения производительности системы и долгосрочное планирование.

Для функционирования обеих категорий средств необходимо выбрать отслеживаемые параметры и допустимые границы для них, выход за которые означает "неадекватность функционирования". После этого задача сводится к выявлению нетипичного поведения компонентов ИС, для чего могут применяться статистические методы.

Управление событиями (точнее, сообщениями о событиях) – это базовый механизм, позволяющий контролировать состояние информационных систем в реальном времени. Системы управления позволяют классифицировать события и назначать для некоторых из них специальные процедуры обработки. Тем самым реализуется важный принцип автоматического реагирования.

Очевидно, что задачи контроля производительности и управления событиями, равно как и методы их решения в системах управления, близки к аналогичным аспектам систем **активного аудита**. Налицо еще одно свидетельство концептуального единства области знаний под названием "информационная безопасность" и необходимости реализации этого единства на практике.