Архитектура безопасности в продуктах и технологиях SharePoint

Михаэль Штеттен

Система безопасности продуктов и технологий Microsoft SharePoint имеет многоуровневую структуру, надстраиваемую над службами безопасности таких базовых продуктов и технологий, как ASP.NET, IIS (Internet Information Services), SQL Server 2000, Windows Server 2003, и зависящую от этих служб. Несомненно, важное значение имеют также безопасность связи и конфигурация межсетевого экрана. Как и любое веб-приложение, узел SharePoint защищен настолько, насколько защищено его самое слабое звено; проблема безопасности затрагивает все компоненты развертывания продуктов и технологий SharePoint. Поскольку спектр технологий безопасности SharePoint весьма широк, необходимо понять принципы их реализации, чтобы обеспечить слаженную и безопасную работу всех составных частей развернутой среды SharePoint.

Ключевое значение имеет многоуровневый подход к структурированию безопасности — так называемая *эшелонированная защита*. Ее применение означает, что контроль безопасности распределен по нескольким уровням, включая политики безопасности организации и настройки Windows Server 2003, IIS, ASP.NET, продуктов и технологий SharePoint, безопасности связи, межсетевого экрана и т. д.

В SharePoint используется ряд технологий, снижающих риск нарушения безопасности, в том числе следующие:

- Проверка подлинности: опирается на концепцию участников безопасности Windows, что позволяет использовать методы строгой проверки, политики паролей, политики блокировки учетных записей и шифрование.
- Авторизация: основана на модели разрешений и обеспечивает высокую степень детализации контроля доступа к содержимому узла.
- Разграничение доступа кода: политика .NET Framework, позволяющая управлять доступом программного кода к защищенным ресурсам и операциям.
- Протоколы безопасности, такие как SSL (Secure Sockets Layer) и IPSec: обеспечивают защиту данных, передаваемых внутри и вне зоны действия межсетевого экрана.
- Защита внешних узлов с помощью межсетевого экрана.

В этой главе основное внимание уделяется вопросам проверки подлинности, авторизации, разграничения доступа кода и безопасности связи в продуктах и технологиях SharePoint. Как показывают исследования, заблаговременное проектирование проверки подлинности и авторизации значительно снижает число потенциально уязвимых мест. Разграничение доступа кода позволяет назначать программному коду различные уровни доверия, в зависимости от его источника и других отличительных особенностей. Безопасность связи — составная часть системы безопасности, отвечающая за защиту данных, передаваемых между пользователями и узлом, а также между серверами развернутой среды. Политики безопасности для продуктов и технологий SharePoint рассматриваются в главе 24,

«Политики информационной безопасности в продуктах и технологиях SharePoint».

Проверка подлинности

Проверка подлинности — это процесс, позволяющий точно идентифицировать пользователей узла. Проверка подлинности гарантирует, что пользователи действительно являются теми, за кого себя выдают. Клиенты, прошедшие проверку подлинности, называются участниками безопасности.

В продуктах и технологиях SharePoint проверка подлинности выполняется на основе учетных записей безопасности Windows.

Для узлов SharePoint производится настройка ASP.NET на использование проверки подлинности Windows. Файлы web.config содержат раздел проверки подлинности следующего вида:

В режиме проверки подлинности Windows для выполнения необходимой проверки клиента в ASP.NET привлекается служба IIS. Она проверяет подлинность пользователя, выдавшего запрос, по учетным записям безопасности Windows. Установив подлинность клиента, IIS передает удостоверение пользователя в ASP.NET. (См. **рис. 1**.)

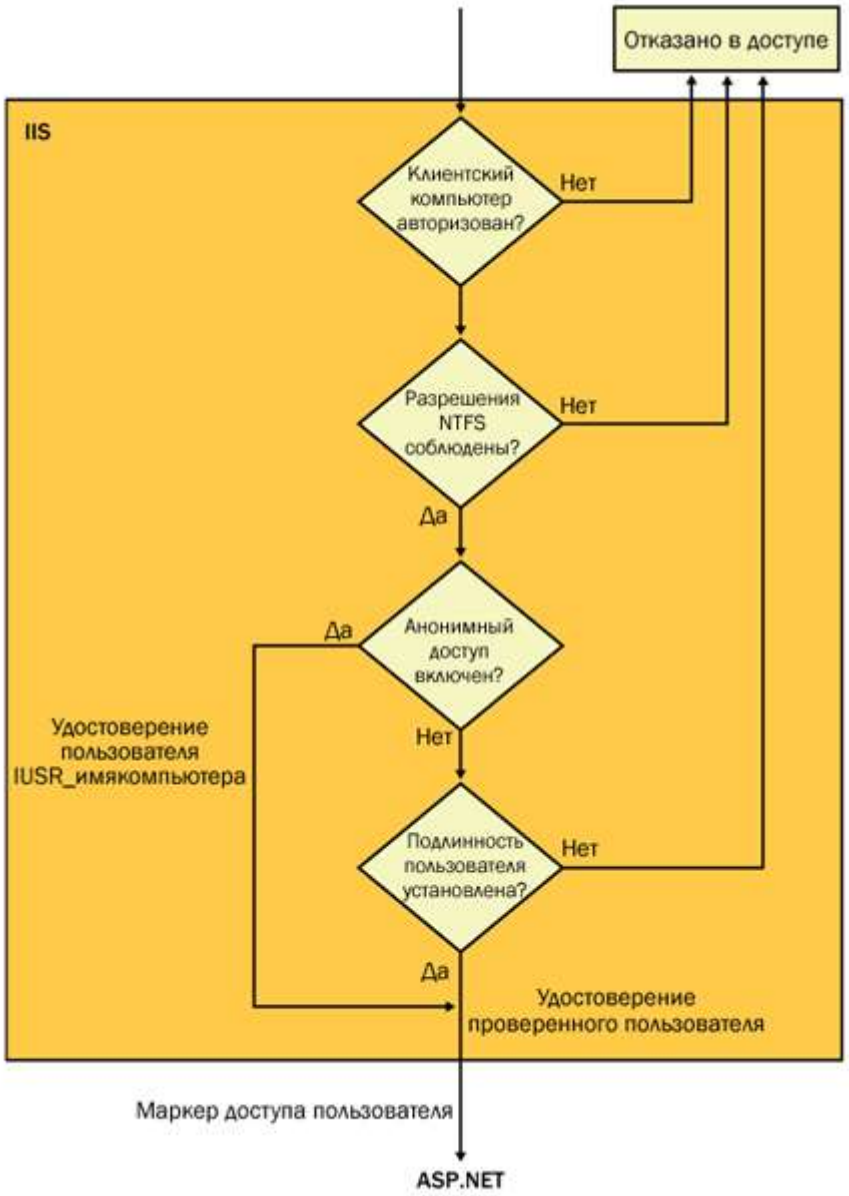

Рис. 1. Передача удостоверения пользователя в режиме проверки подлинности Windows

В продуктах и технологиях SharePoint применяются различные схемы проверки подлинности пользователей на базе IIS.

Обычная проверка

- Обычная проверка подлинности реализована в составе протокола HTTP 1.1, который поддерживается практически всеми обозревателями. При использовании продуктов и технологий SharePoint такой метод можно применять в экстрасети. Учетные данные передаются в незашифрованном виде. Обычная проверка подлинности должна осуществляться только по протоколу SSL; в противном случае безопасность не гарантируется.

Встроенная проверка Windows

- Встроенная проверка подлинности Windows — это безопасный метод проверки подлинности, наиболее подходящий для узлов SharePoint в интрасети. Он не работает через прокси-серверы. Такая проверка

реализуется на базе протоколов Kerberos или NTLM. Для использования Kerberos необходимо, чтобы на компьютерах серверов и клиентов была установлена операционная система Windows 2000 или более поздние версии.

Сопоставление клиентских сертификатов

- Клиенты должны иметь сертификаты X.509. Речь идет о необязательном механизме проверки подлинности, который можно использовать, если между клиентом и сервером включена поддержка SSL. Например, такой метод подходит для экстрасетей с политикой безопасности, требующей двухуровневой проверки подлинности: клиент должен предъявить нечто, имеющееся у него (сертификат), а пользователю предлагается предоставить некоторую соответствующую информацию (учетные данные проверки подлинности). Дополнительные сведения о настройке см. в главе 27, «Безопасность экстрасети на основе SSL и сертификатов».

Анонимная проверка

- Анонимная проверка подлинности позволяет получить анонимный доступ к веб-узлу. Для анонимного доступа по умолчанию используется удостоверение пользователя IUSR_имякомпьютера. Получая анонимный запрос, IIS олицетворяет учетную запись IUSR_имякомпьютера. В этом случае в ASP.NET передается удостоверение IUSR_имякомпьютера.

В продуктах и технологиях SharePoint доступ пользователей осуществляется в соответствии с полномочиями участников безопасности Windows, в качестве которых могут выступать учетные записи отдельных пользователей и учетные записи групп безопасности (DOMAIN\пользователь и DOMAIN\группа_безопасности).

В Windows SharePoint Services для управления доступом к содержимому нельзя использовать списки рассылки, поскольку они не относятся к числу участников безопасности Windows.

Помимо проверки подлинности пользователей при доступе к узлам SharePoint, сервер SharePoint Portal Server поддерживает функцию единого входа в систему (SSO), которая позволяет проверить подлинность пользователя, обратившегося к узлу портала, а затем извлечь из базы данных SSO сохраненные учетные данные пользователя, когда они потребуются другим корпоративным бизнес-приложениям с идентификацией пользователей. Функция SSO реализуется с помощью службы Microsoft Single Sign-On (SSOSrv). Служба SSOSrv обеспечивает хранение и сопоставление учетных данных (имен учетных записей и паролей), чтобы приложения портала могли извлекать необходимую информацию из сторонних приложений и внутренних систем. Пользователи избавляются от необходимости повторной проверки подлинности, когда приложению портала потребуется информация из других бизнес-приложений и систем. Сведения о включении и настройке SSO в SharePoint Portal Server см. в главе 26, «Единый вход в SharePoint Portal Server 2003».

Авторизация

Авторизация определяет, к каким ресурсам и операциям разрешается доступ пользователю, прошедшему проверку подлинности. В Windows SharePoint Services и SharePoint Portal Server доступ к узлам контролируется с помощью системы

ролевой принадлежности, в которой каждому пользователю явным или неявным образом назначается разрешение на выполнение определенных действий. Эта система основана на формировании групп узла. Создавая группу узла, можно настроить права пользователей, исходя из того, какого рода задачи они выполняют.

Группы узла определяют, какими правами обладают пользователи в данном узле. Эти права указывают конкретные действия, которые пользователи могут выполнять на узле. Принципы использования групп узлов в Windows SharePoint Services и SharePoint Portal Server одни и те же, однако в SharePoint Portal Server поддерживается набор дополнительных возможностей, в связи с чем имеются некоторые различия в правах пользователей и соответствующих разрешениях, а также в группах узла, определяемых по умолчанию. В силу этих различий авторизация в Windows SharePoint Services будет рассматриваться отдельно от авторизации в SharePoint Portal Server.

Авторизация в Windows SharePoint Services

В этом разделе описывается процесс авторизации пользователей, обращающихся к узлам Windows SharePoint Services, а также административные задачи, связанные с настройкой авторизации. В Windows SharePoint Services для управления безопасностью в масштабе всего узла используются группы узла.

Действия, которые пользователи могут выполнять, задают права, то есть каждая группа узла — это совокупность прав.

Если требуется, чтобы просматривать содержимое узла могли все пользователи, достаточно разрешить анонимный доступ к узлу. По умолчанию анонимный доступ отключен.

После включения анонимного доступа пользователи могут просматривать узел, не проходя проверку подлинности, но не могут выполнять на узле никакие административные задачи. Доступ к страницам администрирования требует проверки подлинности.

Для запуска программы, написанной с использованием объектной модели Windows SharePoint Services, пользователь должен обладать соответствующими разрешениями, как при взаимодействии с узлом или списком через пользовательский интерфейс

Чтобы авторизоваться для выполнения административных задач, затрагивающих настройки всех веб-узлов и виртуальных серверов на компьютере сервера, пользователь должен стать членом группы локальных администраторов компьютера сервера или группы администраторов SharePoint.

Группы узла

В Windows SharePoint Services поддерживается 21 право, которые используются в пяти группах пользователей узла, определяемых по умолчанию. Эти пять стандартных групп пользовательских прав — «Гость», «Читатель», «Сотрудник», «Веб-дизайнер» и «Администратор». В таблице 6-1 перечислены права пользователей, которые по умолчанию включаются в каждую из этих групп.

Права, назначенные группам узла «Гость» и «Администратор», не могут быть изменены. Права же, включаемые в группы «Читатель», «Сотрудник» и «Веб-дизайнер», можно настроить, оставив в каждой из них лишь необходимые.

Можно добавлять новые группы узла, комбинируя различные наборы прав, изменять права, назначенные какой-либо группе, и удалять неиспользуемые группы.

Пользователей нельзя включать непосредственно в группу «Гость»: в нее автоматически добавляются пользователи, которым предоставлен доступ к спискам или библиотекам документов на основе разрешений для списков. Группа узла «Гость» не может быть настроена или удалена.

Управлять группами узла и разрешениями на доступ можно на страницах HTML-администрирования или с помощью средства командной строки Stsadm.exe. Подробное описание конкретных задач см. в главе 16, «Администрирование узла Windows SharePoint Services».

Для выполнения задач управления непосредственно в коде можно использовать объектную модель Windows SharePoint Services. Подробнее об этом см. в пакете разработки программного обеспечения (SDK) для продуктов и технологий SharePoint по адресу http://msdn.microsoft.com/library/default.asp?url=/library/en-us/spptsdk/html/SPSDKWelcome.asp (EN).

Табл. 1. Стандартные группы узлов Windows SharePoint Services и их права **Имя группы узла Права пользователей по умолчанию**	
Гость	Нет
Читатель	Использование самостоятельного создания узлов Просмотр страниц Просмотр элементов
Сотрудник	Все права, включенные в группу «Читатель», плюс: • Добавление элементов • Добавление и удаление личных веб-частей • Просмотр каталогов • Создание межузловых групп • Удаление элементов • Изменение элементов • Управление личными представлениями • Обновление персональных веб-частей
Сотрудник	Все права, включенные в группу «Сотрудник», плюс: • Добавление и настройка

	страниц • Применение тем и границ • Применение таблиц стилей • Отмена извлечения • Управление списками
Сотрудник	Все права, включенные в группу «Веб-дизайнер», плюс: • Создание дочерних узлов • Управление разрешениями списка • Управление группами узла • Просмотр сведений об использовании

Можно определять не только группы узла, но и межузловые группы. Межузловая группа пользователей может быть включена в группе узла на любом веб-узле в составе семейства узлов. По умолчанию никакие межузловые группы не определяются.

Группы узлов создаются в рамках конкретного узла. В дочерних узлах могут использоваться разрешения родительского веб-узла (наследуемые от групп узла и пользователей, доступных в родительском веб-узле) либо уникальные разрешения. При создании дочернего узла можно выбрать один их этих вариантов — наследование разрешений родительского веб-узла или создание уникальных разрешений.

Уникальные разрешения можно задавать для каждого списка. В список, в отличие от узла, пользователей можно добавлять непосредственно, вместе с указанными разрешениями; при этом пользователи автоматически включаются в группу «Гость» текущего узла, если тот уникален и не наследует разрешения родительского узла. Если текущий узел наследует разрешения, пользователи добавляются в группу «Гость» ближайшего уникального узла-предка.

Пользователям предоставляются разрешения на доступ к узлу или списку на основании прямой или косвенной принадлежности к той или иной группе узла. Их можно добавлять непосредственно в группу узла или в межузловую группу, являющуюся членом группы узла, или пользователь может быть членом группы домена Windows, включенной в группу узла. Кроме того, отдельный пользователь может быть непосредственно добавлен в список вместе с указанным разрешением. На **рис. 2** показано, какими способами пользователям предоставляются разрешения на доступ к узлу или списку.

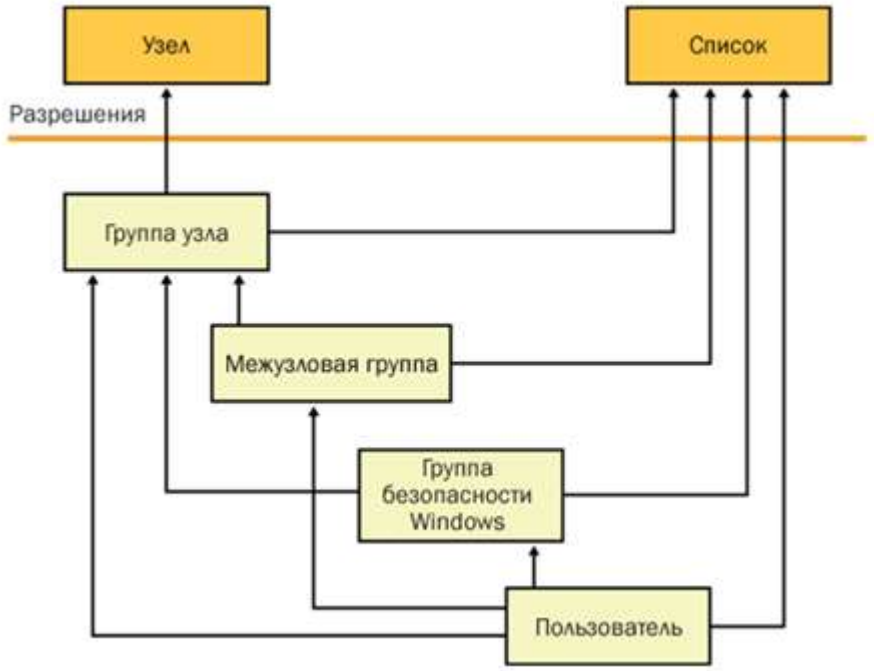

Рис. 2. Предоставление пользователям разрешений на доступ к узлу или списку в Windows SharePoint Services

Большинство пользовательских прав зависит от других прав. Например, чтобы получить возможность изменять элементы, необходимо иметь право их просмотра. Если из группы узла удаляется какое-либо право, вместе с ним удаляются и все зависящие от него права. Дополнительные сведения о зависимостях между правами пользователей см. в **таблице 2.**

В объектной модели Windows SharePoint Services, в отличие от пользовательского интерфейса, права не зависят от других прав. Чтобы запустить программу, написанную с использованием типов и членов объектной модели продуктов и технологий SharePoint, пользователь или группа должны обладать соответствующими разрешениями, как при взаимодействии с узлом или списком через пользовательский интерфейс. Однако в этом случае зависимости не устанавливаются: права можно назначать индивидуально, не включая зависимые права, и их можно назначать пользователям и группам в любом сочетании.

Табл. 2. Зависимости между правами Windows SharePoint Services **Право Разрешения Группы, включаемые по умолчанию Зависимые права**			
Добавление и настройка страниц	Создание страниц ASP.NET, ASP и HTML для веб-узла	«Веб-дизайнер», «Администратор»	Просмотр каталогов, просмотр

			страниц
Добавление элементов	Добавление элементов в списки и документов в библиотеки документов	«Сотрудник», «Веб-дизайнер», «Администратор»	Просмотр элементов, просмотр страниц
Добавление и удаление личных веб-частей	Добавление и удаление веб-частей для индивидуальной настройки страниц веб-частей	«Сотрудник», «Веб-дизайнер», «Администратор»	Обновление персональных веб-частей, просмотр элементов, просмотр страниц
Применение таблиц стилей	Применение таблицы стиля ко всему веб-узлу	«Веб-дизайнер», «Администратор»	Просмотр страниц
Применение тем и границ	Применение темы или границы ко всему веб-узлу	«Веб-дизайнер», «Администратор»	Просмотр страниц
Просмотр каталогов	Просмотр структуры каталогов веб-узла	«Сотрудник», «Веб-дизайнер», «Администратор»	Просмотр страниц
Отмена извлечения	Отмена действия извлечения, выполненного другим пользователем	«Веб-дизайнер», «Администратор»	Просмотр страниц
Создание межузловых групп	Создание и удаление межузловых групп или изменение принадлежности к межузловой группе	«Сотрудник», «Веб-дизайнер», «Администратор»	Просмотр страниц
Создание дочерних узлов	Создание нового дочернего узла или узла рабочей области (например, узла рабочей области документа или узла рабочей области собрания)	«Читатель», «Сотрудник», «Веб-дизайнер», «Администратор»	Просмотр страниц
Удаление элементов	Удаление элементов списков и документов из веб-узла	«Сотрудник», «Веб-дизайнер», «Администратор»	Просмотр элементов, просмотр страниц

Изменение элементов	Редактирование существующих элементов списков и документов в веб-узле	«Сотрудник», «Веб-дизайнер», «Администратор»	Просмотр элементов, просмотр страниц
Управление списками	Создание, изменение и удаление списков и настройка их параметров	«Веб-дизайнер», «Администратор»	Просмотр элементов, просмотр страниц, управление личными представлениями
Управление разрешениями списка	Изменение разрешений для списка или библиотеки документов	«Администратор»	Управление списками, просмотр элементов, просмотр страниц, управление личными представлениями
Управление личными представлениями	Создание, изменение и удаление личных представлений для списков	«Сотрудник», «Веб-дизайнер», «Администратор»	Просмотр элементов, просмотр страниц
Управление группами узла	Создание, удаление и изменение групп узлов, включая изменение назначенных им прав и изменение состава группы	«Администратор»	Просмотр страниц
Управление веб-узлом	Выполнение задач администрирования определенного узла или дочернего узла	«Администратор»	Просмотр страниц
Обновление персональных веб-частей	Обновление веб-частей, отображающих индивидуально настроенную информацию	«Сотрудник», «Веб-дизайнер», «Администратор»	Просмотр элементов, просмотр страниц
Использование самостоятельного создания узлов	Использование средства самостоятельного	«Читатель», «Сотрудник», «Веб-дизайнер»,	Просмотр страниц

	создания узлов для построения веб-узла верхнего уровня	«Администратор»	
Просмотр элементов	Просмотр элементов в списках, документов в библиотеках и примечаний к веб-обсуждениям	«Читатель», «Сотрудник», «Веб-дизайнер», «Администратор»	Просмотр страниц
Просмотр страниц	Просмотр страниц веб-узла	«Читатель», «Сотрудник», «Веб-дизайнер», «Администратор»	Нет
Просмотр сведений об использовании	Просмотр отчетов об использовании веб-узла	«Администратор»	Просмотр страниц

Права создания узлов

Права создания узлов («Использование самостоятельного создания узлов» и «Создание дочерних узлов») определяют, может ли пользователь создавать веб-узлы верхнего уровня, дочерние узлы или рабочие области.

Члены группы узла «Администратор» могут создавать в своих веб-узлах дочерние узлы. Самостоятельное создание узлов означает немного другое: это средство, предоставляемое администраторами и позволяющее пользователям создавать собственные веб-узлы верхнего уровня. Пользователям не требуются административные разрешения на сервере или виртуальном сервере — лишь разрешения на веб-узле, на котором размещено средство самостоятельного создания узлов. По умолчанию право использования самостоятельного создания узлов включается во все группы узла, кроме группы «Гость», и предоставляет пользователям доступ к странице входа и к самому средству самостоятельного создания узлов.

Право самостоятельного создания узлов доступно только в веб-узле верхнего уровня в семействе узлов.

Средство самостоятельного создания узлов позволяет пользователям автоматически конструировать собственные веб-узлы верхнего уровня и управлять ими. По умолчанию это средство отключено; чтобы использовать его, необходимо его включить. Включить самостоятельное создание узлов для отдельного виртуального сервера можно на странице «Настройка самостоятельного создания узлов» этого виртуального сервера. Чтобы сделать это средство доступным на всех виртуальных серверах фермы, его необходимо включить для каждого из них в отдельности.

Для включения и настройки самостоятельного создания узлов можно использовать страницы HTML-администрирования или средства командной строки enablessc.exe и disablessc.exe. Оба этих метода позволяют включить или отключить самостоятельное создание узлов и указать тип сведений, которые должны запрашиваться при создании узла. Дополнительные сведения см. в главе 15, «Настройка Windows SharePoint Services».

Анонимный доступ

Анонимный доступ позволяет пользователю просматривать страницы и вносить изменения в списки и опросы, оставаясь анонимным. Включение анонимного доступа в Windows SharePoint Services разрешает доступ к узлу для анонимной учетной записи IIS — IUSR_имякомпьютера.

Анонимный доступ по умолчанию отключен; он контролируется на уровне узла. Чтобы включить анонимный доступ, необходимо сначала убедиться, что служба IIS настроена для разрешения анонимного доступа, а затем включить анонимный доступ к веб-узлу на странице «Параметры узла». Анонимный доступ к конкретным спискам контролируется с помощью разрешений для списков. Если анонимный доступ отключен для узла, его нельзя включить для списка в этом узле.

Можно также предоставить доступ всем пользователям, прошедшим проверку подлинности: это позволит всем участникам домена обращаться к веб-узлу без включения анонимного доступа.

Подробное описание процедуры настройки анонимного доступа см. в главе 16.

Выполнение задач администрирования

Пользователи, включенные в группу узла «Администратор», являются администраторами только данного веб-узла. Для выполнения административных задач, затрагивающих настройки всех веб-узлов и виртуальных серверов на компьютере сервера, пользователь должен быть администратором компьютера сервера (*локальным администратором*) или членом группы администраторов SharePoint, а не просто членом группы «Администратор» своего узла.

Страницы администрирования виртуальных серверов доступны только локальным администраторам компьютера и членам группы администраторов SharePoint. Этот доступ настраивается с помощью авторизации URL-адресов в файле web.config центра администрирования, расположенном в папке :\Program Files\Common Files\Microsoft Shared\web server extensions\60\TEMPLATE\ADMIN\1033. Элемент определяется следующим образом:

Группа администраторов SharePoint — это группа домена Windows, которой наряду с группой локальных администраторов предоставляется административный доступ к Windows SharePoint Services. Члены этой группы локальных администраторов определяют имя группы Windows, назначаемой группой администраторов SharePoint, на страницах центра администрирования. Имя, указываемое на страницах центра администрирования, совпадает с именем в файле web.config; при изменении группы администраторов SharePoint изменяется и ее имя в элементе файла web.config.

Добавляя пользователей в группу администраторов SharePoint вместо группы локальных администраторов, можно отделить административный доступ к Windows SharePoint Services от административного доступа к локальному компьютеру сервера. Члены как группы администраторов SharePoint, так и группы локальных администраторов имеют право просмотра всех узлов, созданных на их серверах, и управления этими узлами.

Члены группы администраторов SharePoint не имеют доступа к метабазе IIS и потому не могут выполнять в Windows SharePoint Services следующие действия: расширять виртуальные серверы, управлять путями, изменять группу администраторов SharePoint, изменять параметры базы данных конфигурации и пользоваться средством командной строки Stsadm.exe. Они могут выполнять все остальные административные действия, используя страницы HTML-администрирования или объектную модель Windows SharePoint Services.

Авторизация в SharePoint Portal Server

В этом разделе рассматриваются принципы авторизации доступа пользователей к узлам SharePoint Portal Server, библиотекам документов, совместимым с предыдущими версиями, и результатам поиска.

Как и в Windows SharePoint Services, в SharePoint Portal Server для управления безопасностью в масштабе узла используются группы узла. Каждый пользователь является членом по крайней мере одной группы узла, и доступ к узлам портала контролируется системой принадлежности к группам узла. Создав узел портала, можно предоставлять пользователям доступ к нему, включая их в группы узла. Пользователь, не назначенный ни одной группе узла, не получит доступ к узлу портала.

Помимо авторизации на основе принадлежности к группам узлам, SharePoint Portal Server поддерживает безопасность на основе ролей для библиотек документов, совместимых с предыдущими версиями.

Группы узла

В SharePoint Portal Server используются шесть стандартных групп узла, в каждую из которых объединяются пользователи с конкретным набором настраиваемых прав. Можно также создать свою группу узла для определенной области или списка и назначить ей требуемый набор прав. Разрешается изменять права, назначенные группе узла, создавать новые группы и удалять неиспользуемые.

Шесть стандартных групп SharePoint Server, определяемых по умолчанию, перечислены ниже:

- «Читатель»: пользователям разрешается выполнять поиск и просмотр содержимого узла.
- «Участник»: пользователям разрешается представлять списки и создавать личные узлы.
- «Сотрудник»: пользователям разрешается размещать содержимое в областях узла, на которые им предоставлены права.
- «Веб-дизайнер»: пользователям разрешается изменять макет и параметры веб-страницы, на которую им предоставлены права.
- «Администратор»: пользователям предоставляется полный контроль над веб-узлом.
- «Менеджер содержимого»: пользователям разрешается управлять всеми параметрами и содержимым в области, на которую им предоставлены права.

Группы узла можно использовать как для управления общим доступом к узлу

портала, так и для управления доступом к определенным областям узла.

Хотя группы узлов SharePoint Portal Server во многих отношениях схожи с группами Windows SharePoint Services, между ними имеется ряд различий.

- В SharePoint Portal Server предусмотрены две стандартные группы узла, которых нет в Windows SharePoint Services: «Участник» и «Менеджер содержимого». Пользователям, входящим в эти группы, доступны возможности, имеющиеся только в SharePoint Portal Server: группе «Участник» разрешается создавать личные узлы, а группе «Менеджер содержимого» — управлять областями, группируя содержимое по критериям, определенным пользователем.
- В SharePoint Portal Server не определяется стандартная группа узла «Гость». В Windows SharePoint Services такая группа используется автоматически при назначении разрешений по списку.
- Между SharePoint Portal Server и Windows SharePoint Services имеются различия в правах пользователей и соответствующих разрешениях. Это связано с различиями в функциональных возможностях данных продуктов. Некоторые права совпадают — например, просмотр страниц. Однако права, связанные с управлением областями, оповещениями, профилями пользователей, аудиториями и поиском, различаются принципиально, поскольку эти возможности присутствуют только в SharePoint Portal Server.

Права пользователей SharePoint Portal Server и соответствующие разрешения перечислены в **таблице 3**.

Табл. 3. Права пользователей SharePoint Portal Server и соответствующие разрешения **Право**	**Разрешения**
Добавление и настройка страниц	Добавление, изменение и удаление HTML-страниц и страниц веб-частей, редактирование узла портала в редакторе, совместимом с Windows SharePoint Services
Добавление элементов	Добавление элементов в списки, документов в библиотеки документов SharePoint, примечаний в веб-обсуждения
Добавление и удаление личных веб-частей	Добавление и удаление веб-частей на индивидуально настроенной странице веб-частей
Применение таблиц стилей	Применение таблицы стилей (файл .CSS) к области или узлу портала
Просмотр каталогов	Просмотр каталогов в области
Отмена извлечения	Возврат документов без сохранения внесенных изменений
Создание области	Создание области на узле портала
Создание личного узла	Создание личного узла SharePoint

Создание узлов	Создание узлов SharePoint с помощью средства самостоятельного создания узлов
Удаление элементов	Удаление элементов из списков, документов из библиотек документов, примечаний к веб-обсуждениям в документах
Изменение элементов	Изменение элементов в списках и документов в библиотеках документов SharePoint, настройка страниц веб-частей в библиотеках документов SharePoint
Управление оповещениями	Изменение параметров оповещений для узла портала и управление оповещениями для пользователей
Управление областью	Удаление или изменение свойств области узла портала
Управление разрешениями для области	Добавление, удаление и изменение прав пользователей в отношении области
Управление аудиториями	Добавление, изменение и удаление аудиторий
Управление личными представлениями	Создание, изменение и удаление личных представлений списков
Управление узлом портала	Задание свойств узла портала и управление параметрами узла
Управление поиском	Добавление, изменение и удаление параметров поиска и индекса на узле портала
Управление профилями пользователей	Добавление, изменение и удаление содержимого профилей пользователей и их свойств
Поиск	Поиск на узле портала и во всем связанном содержимом
Обновление персональных веб-частей	Обновление веб-частей, отображающих индивидуально настроенную информацию
Использование личных возможностей	Использование оповещений и личных узлов
Просмотр области	Просмотр области и ее содержимого
Просмотр страниц	Просмотр страниц в области

Как и в Windows SharePoint Services, пользователю предоставляются разрешения на доступ к узлу портала в зависимости от его прямой или косвенной принадлежности к той или иной группе узла. Однако здесь есть одно отличие: в SharePoint Portal Server не поддерживаются межузловые группы — они предусмотрены только в Windows SharePoint Services. В SharePoint Portal Server пользователь может быть

включен непосредственно в группу узла, или он может быть членом группы домена Windows, включенной в группу узла. На **рис. 3** показано, какими способами пользователям предоставляются разрешения на доступ к узлу портала.

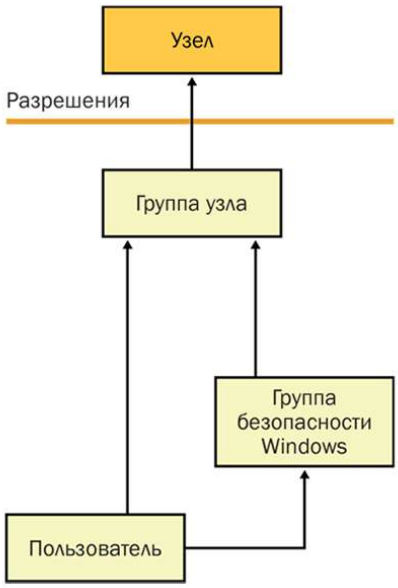

Рис. 3. Предоставление пользователям разрешений на доступ к узлу портала

Доступ к областям узла портала можно регулировать, назначая пользователей группе узла для определенной области. Безопасность каждой области портала можно настраивать путем добавления, изменения и удаления пользователей или групп узла.

По умолчанию параметры безопасности родительской области автоматически применяются ко всем ее дочерним областям. Добавление пользователей или групп в конкретную область нарушает порядок наследования параметров безопасности: после настройки параметров безопасности дочерняя область перестает наследовать изменения, вносимые в родительскую область.

Права создания узлов

Права создания узлов («Создание узлов» и «Создание личного узла») определяют, может ли пользователь создавать узлы портала и личные узлы.

Право «Создание узлов» позволяет создавать узлы портала с помощью средства самостоятельного создания узлов. Как и в Windows SharePoint Services, самостоятельное создание узлов в SharePoint Portal Server по умолчанию отключено — чтобы использовать это средство, необходимо его включить. Новые узлы по умолчанию создаются с использованием стандартной базы данных содержимого; можно настроить также альтернативную базу данных. Дополнительные сведения см. в главе 18, «Управление сервером SharePoint Portal Server 2003».

Право «Создание личного узла» позволяет пользователю создать личный узел, щелкнув «Мой узел» в строке заголовка на домашней странице портала.

Администраторы узлов контролируют расположение личных узлов в портале и формат их имен, используя страницу «Управление личными узлами».

Анонимный доступ

Анонимный доступ позволяет пользователю просматривать страницы на узле портала и выполнять поиск, оставаясь анонимным. Включение анонимного доступа в SharePoint Portal Server разрешает доступ к узлу для анонимной учетной записи IIS — IUSR_имякомпьютера.

Анонимный доступ по умолчанию отключен; он контролируется на уровне узла портала. Чтобы включить анонимный доступ, необходимо сначала убедиться, что служба IIS настроена для разрешения анонимного доступа, а затем включить анонимный доступ к узлу портала, используя страницы центра администрирования SharePoint Portal Server.

Если, наряду с анонимным доступом, необходимо сохранить проверку подлинности пользователей, можно создать новый виртуальный сервер, расширить его, а затем включить анонимный доступ к этому виртуальному серверу, используя центр администрирования SharePoint Portal Server. В этом случае при доступе к первоначальному узлу портала пользователи должны будут проходить проверку подлинности, а доступ к новому виртуальному серверу будет анонимным.

Создавать и расширять виртуальные серверы могут только члены группы локальных администраторов. Чтобы включить анонимный доступ и управлять его параметрами, необходимо быть администратором узла портала, членом группы администраторов SharePoint или членом группы локальных администраторов.

Включив анонимный доступ к узлу портала, можно разрешить анонимным пользователям просматривать страницы и выполнять поиск на узле портала. Если анонимный доступ отключен для узла, его нельзя включить только для просмотра областей или выполнения поиска.

Подробные инструкции по настройке анонимного доступа для узла портала см. в главе 18, «Управление сервером SharePoint Portal Server 2003».

Выполнение задач администрирования

Сервер SharePoint Portal Server сконструирован на основе Windows SharePoint Services, поэтому неудивительно, что разрешения на выполнение задач администрирования в обоих продуктах практически одинаковы.

- Для выполнения административных задач, затрагивающих настройки всех узлов портала и виртуальных серверов на компьютере сервера, пользователь должен быть администратором компьютера сервера или членом группы администраторов SharePoint.
- Пользователи, включенные в группу узла «Администратор», являются администраторами только данного узла портала.

Безопасность библиотек документов, совместимых с предыдущими версиями

Часто возникает необходимость ограничить доступ к содержимому библиотек документов, совместимых с предыдущими версиями (основанных на системе веб-

хранения). В некоторых случаях требуется ограничить просмотр документа, разрешив его только пользователям, редактирующим и утверждающим документ, — до тех пор, пока он не будет готов для широкой аудитории.

Для библиотек документов, совместимых с предыдущими версиями, в ролях SharePoint Portal Server появляются новые действия — в дополнение к традиционным разрешениям на чтение, запись и изменение файлов, — например: извлечение, возврат, публикация, утверждение. Существуют три фиксированные роли, каждая из которых определяет конкретный набор разрешений.

- Координаторы: выполняют задачи управления.
- Авторы: добавляют и обновляют файлы.
- Читатели: могут только читать опубликованные документы.

Разрешения на доступ для этих трех ролей являются фиксированными и не подлежат изменению. SharePoint Portal Server также предлагает возможность отказа пользователям в доступе к определенным документам. Роли обычно устанавливаются на уровне папки, хотя координаторов задач управления можно добавлять на уровне библиотеки документов.

Результаты поиска

При выполнении поиска SharePoint Portal Server учитывает политики безопасности, используемые на серверах организации, в общих файловых ресурсах и базах данных. Такая авторизация имеет важное значение, поскольку не позволяет пользователям при поиске на узле портала находить документы, к которым у них нет доступа. Подробное описание архитектуры, функциональных возможностей и настройки поиска см. в главе 21, «Архитектура средства сбора данных» и в главе 22, «Управление внешним содержимым в Microsoft Office SharePoint Portal Server 2003».

Разграничение доступа кода

Разграничение доступа кода используется службами продуктов и технологий SharePoint для управления доступом к защищенным ресурсам. Разграничение доступа кода — это механизм безопасности, который позволяет назначать приложениям продуктов и технологий SharePoint настраиваемый уровень доверия, с которым связан предварительно определенный набор разрешений. Для программного кода могут устанавливаться различные уровни доверия, в зависимости от его источника и других отличительных особенностей. Средство разграничения доступа кода выполняет следующие функции.

- Определяет разрешения и наборы разрешений, составляющие права доступа к тем или иным системным ресурсам
- Позволяет администраторам настраивать политику безопасности, связывая наборы разрешений с группами кода
- Позволяет программному коду запрашивать разрешения, необходимые для его выполнения, а также разрешения, которые могут оказаться целесообразными, и определяет, какие разрешения предоставлять нельзя
- Предоставляет разрешения для каждой загружаемой сборки, исходя из разрешений, запрошенных кодом, и операций, допускаемых политикой

безопасности

- Разрешает коду требовать наличия определенных разрешений у пользователей, вызывающих код
- Разрешает коду требовать наличия цифровой подписи у вызывающих его пользователей, чтобы защищенный код могли вызывать только пользователи из конкретной организации или узла
- Вводит ограничения для кода на этапе выполнения, сравнивая разрешения, предоставленные каждому вызывающему пользователю в стеке вызовов, с разрешениями, которые они должны иметь

Чтобы определить, разрешается ли коду доступ к ресурсу или выполнение операции, система безопасности среды выполнения проходит по стеку вызовов, сравнивая разрешения, предоставленные каждому вызывающему пользователю, с требуемыми разрешениями. Если у какого-либо пользователя в стеке вызовов нет необходимых разрешений, генерируется исключение безопасности и происходит отказ в доступе.

Чтобы позволить администратору переключать уровни доверия, назначаемые приложению, Windows SharePoint Services в дополнение к файлам политик безопасности ASP.NET, действующих по умолчанию, вводит две собственные политики безопасности: Windows SharePoint Services Minimal (WSS_Minimal) и Windows SharePoint Services Medium (WSS_Medium). Когда виртуальный сервер расширяется для размещения Windows SharePoint Services, к нему по умолчанию применяется политика WSS_Minimal.

Политики разграничения доступа кода в продуктах и технологиях SharePoint

Файлы политик WSS_Minimal и WSS_Medium по умолчанию размещаются в папке :\Program Files\Common Files\Microsoft Shared\Web Server Extensions\60\config\. Имена этих файлов — соответственно wss_minimaltrust.config и wss_mediumtrust.config. Разрешения, определяемые в файлах политик WSS_Minimal и WSS_Medium, описываются в **таблице 4.**

Табл. 4. Разрешения, определяемые в политиках WSS_Minimal и WSS_Medium **Разрешение**	**WSS_Medium**	**WSS_Minimal**
AspNetHostingPermission	Medium	Minimal

Environment	Read: TEMP, TMP, OS, USERNAME, COMPUTERNAME	
FileIO	Read, Write, Append, PathDiscovery:	
IsolatedStorage	AssemblyIsolationByUser, с указанием свойства UserQuota	
Security	Execution, Assertion, ControlPrincipal, ControlThread, RemotingConfiguration	Execution
WebPermission	Подключение к хосту источника (если он настроен)	
DNS	Снятие ограничений или предоставление всех субразрешений	
SqlClientPermission	Снятие ограничений или предоставление всех субразрешений	
SharePointPermission	SharePointPermission.ObjectModel	
WebPartPermission	WebPartPermission.Connections	WebPartPermission.Connections

Политики WSS_Minimal и WSS_Medium расширяют файлы стандартных политик ASP.NET. Эти политики назначают уровень полного доверия сборкам, находящимся в глобальном кэше сборок (GAC) и папке $CodeGen, а сборкам, установленным в каталоге /bin виртуального сервера, — уровень частичного доверия.

В дополнение к стандартному набору разрешений, определенных в ASP.NET и среде CLR, для продуктов и технологий SharePoint вводятся два специальных разрешения SharePointPermission и WebPartPermission, как часть пространства имен Microsoft.SharePoint.Security, расположенного в библиотеке Microsoft.SharePoint.Security.dll. Для доступа к библиотекам классов продуктов и технологий SharePoint коду должно быть назначено разрешение SharePointPermission со свойством ObjectModel, имеющим значение true (истина). Полный список атрибутов разрешений SharePointPermission и WebPartPermission см. в документе «Microsoft Windows SharePoint Services и разграничение доступа кода» (EN).

Исходя из требований и уровня доверия для сборок, установленных в каталоге /bin виртуального сервера, расширенного с помощью продуктов и технологий SharePoint, администраторы могут изменять разрешения, связанные с этими сборками. Проще всего это сделать, изменив политику, применяемую к виртуальному серверу, а именно изменив атрибут уровня доверия в файле web.config этого виртуального сервера. По умолчанию могут устанавливаться следующие уровни доверия (перечислены в порядке сокращения разрешений).

- Full
- High (стандартный уровень ASP.NET, разрешения SharePointPermission и WebPartPermission не предоставляются)
- WSS_Medium
- Medium (стандартный уровень ASP.NET, разрешения SharePointPermission и WebPartPermission не предоставляются)
- Low (стандартный уровень ASP.NET, разрешения SharePointPermission и WebPartPermission не предоставляются)
- WSS_Minimal
- Minimal (стандартный уровень ASP.NET, разрешения SharePointPermission и WebPartPermission не предоставляются)

Если код пытается выполнить действие или получить доступ к ресурсу, защищенному средой CLR, стандартных разрешений может оказаться недостаточно; коду может потребоваться одно или несколько стандартных разрешений ASP.NET.

Для использования классов и членов пространства имен Microsoft.SharePoint.Portal.SingleSignOn коду потребуется дополнительное разрешение SingleSignonPermission.Access. Подробные инструкции см. в главе 26.

Предоставить коду все разрешения, необходимые для доступа к библиотекам классов в продуктах и технологиях SharePoint, можно несколькими способами.

- Создать собственную политику безопасности и назначить разрешение SharePointPermission со свойством ObjectModel, имеющим значение true (истина), конкретной сборке или набору сборок. Подробные инструкции см. в главе 39, «Использование Microsoft Office InfoPath вместе с продуктами и технологиями SharePoint».
- Установить сборку в глобальный кэш сборок, поскольку в нем код всегда пользуется полным доверием. Хотя установка сборки веб-частей в кэш GAC — вполне действенный метод, рекомендуется все же для большей безопасности устанавливать сборки веб-частей в каталог /bin. Полный список преимуществ и недостатков установки сборки в GAC см. по адресу http://msdn.microsoft.com/library/default.asp?url= /library/en-us/odc_sp2003_ta/html/sharepoint_wsscodeaccesssecurity.asp (EN).
- Повысить уровень доверия для виртуального сервера, расширенного с помощью продуктов и технологий SharePoint, изменив атрибут уровня доверия в файле web.config. Например, чтобы изменить уровень политики виртуального сервера с WSS_Minimal на WSS_Medium, выполните следующие действия:

    1. Откройте файл web.config виртуального сервера в текстовом редакторе, например в «Блокноте».
    2. Найдите строку .
    3. Измените уровень на следующий:
    4. Сохраните файл web.config.
    5. Выполните сброс IIS с помощью программы командной строки iisreset.

Безопасность связи

Безопасная связь между компонентами развернутой среды SharePoint — весьма существенный элемент архитектуры всесторонней безопасности. Для продуктов и технологий SharePoint важно, чтобы методы защиты связи применялись как внутри, так и вне зоны действия межсетевого экрана. Безопасная связь гарантирует конфиденциальность и целостность данных.

Конфиденциальность означает, что данные остаются закрытыми для доступа и не смогут просматриваться злоумышленниками, вооруженными средствами сетевого мониторинга. Конфиденциальность обеспечивается путем шифрования.

Целостность означает защищенность данных от случайного или умышленного изменения в процессе их передачи. Каналы безопасной связи должны обеспечивать целостность данных. Обычно целостность достигается за счет использования кодов проверки подлинности сообщения (MAC).

Для обеспечения безопасности передачи данных применяются следующие технологии.

Протокол SSL/TLS

- SSL — протокол безопасности на основе открытых ключей, который включает набор криптографических технологий, обеспечивающих подтверждение подлинности, конфиденциальность и целостность данных. Он широко применяется для защиты канала, связывающего обозреватель и веб-сервер. Однако его можно также использовать для защиты данных, передаваемых на сервер базы данных Microsoft SQL Server 2000 и обратно.

Протокол IPSec

- IPSec обеспечивает безопасную связь на транспортном уровне и может использоваться для защиты данных, передаваемых между двумя компьютерами. IPSec — механизм транспортного уровня, позволяющий обеспечить конфиденциальность и целостность данных, передаваемых между компьютерами по протоколу TCP/IP. IPSec полностью прозрачен для приложений, поскольку службы шифрования, контроля целостности и проверки подлинности реализованы на транспортном уровне.

В этом разделе будут рассмотрены вопросы безопасности связи в продуктах и технологиях SharePoint, в том числе следующие темы.

- Связь с Microsoft SQL Server
- Связь между сервером индексирования и сервером поиска в ферме серверов SharePoint Portal Server
- Защита узлов SharePoint с помощью межсетевых экранов
- Использование SSL для узлов экстрасети

Связь с Microsoft SQL Server

При развертывании продуктов и технологий SharePoint соединения между внешним веб-сервером и компьютером с сервером SQL Server не шифруются. Рекомендуется использовать протокол SSL или иным способом шифровать межсерверный обмен, например с помощью IPSec.

Если для обеспечения безопасности связи с SQL Server 2000 выбран протокол SSL, необходимо выполнить следующие действия.

1. На компьютере с запущенным SQL Server получите и установите сертификат сервера.
2. Центр сертификации, выдавший этот сертификат, должен быть надежным для клиентов, устанавливающих подключения. Чтобы добиться этого, установите сертификат данного центра сертификации на клиентских компьютерах, например на внешних веб-серверах.
3. На компьютере с сервером SQL Server воспользуйтесь служебной программой Server Network Utility и задайте, должны ли все клиенты принудительно использовать SSL, или им разрешается выбирать — использовать SSL или нет.
   Дополнительные сведения см. в статье 276553 базы знаний Майкрософт — HOW TO: Enable SSL Encryption for SQL Server 2000 with Certificate Server («Инструкции: включение шифрования SSL для SQL Server 2000 с сервером сертификатов»). Эту статью можно найти на веб-странице http://support.microsoft.com/default.aspx?scid=276553 (EN).

Если для обеспечения безопасности связи с SQL Server 2000 выбран протокол IPSec, необходимо выполнить следующие действия.

1. Создайте политику IP-безопасности (IPSec) на компьютере сервера базы данных.
2. Экспортируйте созданную политику IPSec и скопируйте ее на компьютер внешнего сервера.
3. Назначьте политику IPSec на компьютере сервера базы данных и на компьютерах удаленных серверов. Прежде чем стать активной, политика IPSec должна быть назначена.
   Дополнительные сведения о IPSec см. в материалах TechNet по адресу http://www.microsoft.com/technet/prodtechnol/windows2000serv/howto/ispstep.mspx
   (EN).

Связь между сервером индексирования и сервером поиска

В ферме серверов, использующей SharePoint Portal Server, передача при распространении индексов с сервера управления индексами на сервер поиска не шифруется и может оказаться небезопасной. Для обеспечения безопасности связи между сервером индексирования и серверами поиска рекомендуется использовать механизм IPSec.

Чтобы использовать IPSec для защиты распространяемых индексов, выполните следующие действия.

1. Создайте политику IPSec на компьютере сервера управления индексами.
2. Экспортируйте политику IPSec на каждый компьютер сервера поиска.
3. На компьютерах сервера индексирования и серверов поиска назначьте политику IPSec, чтобы активировать ее.

Использование межсетевых экранов для защиты узлов SharePoint

Если узел SharePoint предоставляет услуги в масштабе экстрасети или становится доступным через Интернет для широкой аудитории, необходимо позаботиться о том, чтобы внешний доступ к узлу осуществлялся через межсетевой экран. Межсетевой экран инспектирует весь входящий и исходящий трафик, а затем разрешает или запрещает его прохождение, исходя из предварительно настроенных политик.

На простейшем уровне межсетевые экраны выполняют фильтрацию пакетов: при поступлении трафика межсетевой экран проверяет данные, содержащиеся в IP-заголовке, по предварительно установленным правилам и определяет, следует ли разрешить доступ или отказать в нем. Однако для защиты развернутой среды SharePoint Portal Server от внешних атак необходимо также проверять содержимое заголовка HTTP. Межсетевой экран Microsoft Internet Security and Acceleration (ISA) Server 2000 — это межсетевой экран прикладного уровня, который, помимо фильтрации пакетов, выполняет анализ данных, содержащихся в пакетах протоколов прикладного уровня, таких как HTTP. В главе 25, «Использование межсетевого экрана при развертывании SharePoint Portal Server» подробно описывается, как настроить сервер ISA, чтобы узлы SharePoint стали доступны внешним пользователям без ущерба для безопасности внутренней сети.

Использование SSL в среде экстрасети

В веб-среде для создания безопасного канала связи между веб-обозревателем и внешним веб-сервером обычно используется протокол SSL. Для продуктов и технологий SharePoint протокол SSL служит безопасным средством установления шифруемого соединения с пользователями, подключающимися к узлам SharePoint с внешней стороны межсетевого экрана.

Подробное описание протокола SSL и инструкции по его включению в рабочей среде см. в главе 27, «Безопасность экстрасети на основе SSL и сертификатов».

Заключение

В этой главе рассматривались механизмы безопасности, используемые в продуктах и технологиях SharePoint для обеспечения безопасного доступа пользователей и снижения степени уязвимости. Проверка подлинности пользователей производится на базе таких технологий, как IIS и ASP.NET, а также концепции участников безопасности Windows, в то время как авторизация доступа основана на членстве в группах узла, которые связывают (прямо или косвенно) каждого пользователя с разрешением, указывающим, какие именно действия он может выполнять. Разграничение доступа кода позволяет детализировать возможности доступа для кода приложений продуктов и технологий SharePoint. Безопасность связи имеет ключевое значение для обеспечения безопасной передачи данных внутри и вне зоны действия межсетевого экрана. Система безопасности продуктов и технологий Microsoft SharePoint имеет многоуровневую структуру, которая строится на основе служб безопасности ряда базовых технологий, поэтому важно придерживаться всестороннего подхода к безопасности, формируя систему эшелонированной защиты, охватывающей все компоненты развернутой среды продуктов и технологий SharePoint.