Описание системы удаленного доступа (СУД)

Москва, 2010 г.

Содержание

1. Общие сведения

1.1. Наименование системы

Система удаленного доступа к ресурсам корпоративной информационной сети Компании (СУД) представляет собой комплекс программных и аппаратных средств, осуществляющих безопасные соединения удаленных пользователей с ресурсами внутренней информационной сети Компании.

1.2. Назначение системы

Система удаленного доступа к ресурсам КИС предназначена для выполнения следующих задач:

- Получение доступа в определенный сегмент КИС с помощью технологии VPN.
- Получение доступа к Web-сервисам при помощи технологии SSL/VPN.
- Получение доступа из локальной КИС к ресурсам другой (внешней) локальной сети при помощи технологии LAN-to-LAN на основе протокола IPSec.

1.3. Класс системы

Система относится к классу *Business support* – системы вспомогательного характера, отказ или сбой которых не оказывает существенного влияния ни на работу подразделений Компании, ни на предоставление услуг абонентам Компании.

2. Поддерживаемые бизнес-процессы

Название процесса	**Характер взаимодействия**
Работа с WEB-приложениями КИС	Обеспечение безопасного доступа удаленным пользователям к WEB-приложениям КИС
Обмен информацией	Реализация безопасного обмена информацией между удаленными локальными сетями. Могут быть вовлечены сети партнерских организаций, а также сети филиалов компании
Доступ к данным	Обеспечение доступа удаленным пользователям к ресурсам КИС

3. Архитектура системы

3.1. Описание сущностей системы

Сущность (синонимы)	**Отношения**	**Описание, свойства**
КИС(может именоваться также локальной сетью)	Обобщает понятие локальной сети Компании, состоящей из ряда сегментов LAN	Корпоративная информационная сеть Компании (филиала Компании) или омпании-партнера является одной из сущностей, между которыми устанавливается безопасное соединение
WEB-ресурс (WEB–приложение, WEB-сайт)	Входит в состав КИС	Под WEB-ресурсами подразумеваются внутренние WEB-ресурсы и WEB-приложения КИС, доступ к которым осуществляется с помощью технологии SSL/VPN
Удаленный пользователь	Является участником безопасного соединения	Удаленные пользователи являются субъектами безопасных удаленных соединений с ресурсами КИС

3.2. Пользовательские функции и профили доступа

ИТ услуга, роль (профиль доступа)	**Сервисы**
Удаленный доступ пользователей к ресурсам КИС компании	• Аутентификация • Сервисы VPN (осуществление «прозрачных» взаимодействий удаленного пользователя с локальной сетью Компании)

ИТ услуга, роль (профиль доступа)	**Сервисы**
Доступ пользователей локальной сети филиала, компании-партнера к ресурсам КИС компании	• Аутентификация • Сервисы VPN (осуществление «прозрачных» взаимодействий по технологии LAN-to-LAN между двумя удаленными локальными сетями)
Использование удаленными пользователями WEB-сервисов компании	• Аутентификация • Сервисы VPN (осуществление аутентифицированного доступа к WEB-ресурсам КИС Компании, на основе технологии SSL/VPN)

3.3. Интерфейсы

3.3.1. Реализуемые системой интерфейсы

IPSec	Установление безопасных соединений на основе технологии VPN с использованием IPSec-туннелей.
SSL	Доступ к WEB-ресурсам КИС Компании.
HTTP	Доступ к списку отозванных сертификатов (CRL).

3.3.2. Используемые системой интерфейсы

HTTP	Публичная сеть (интернет). Используется как транспортная среда для передачи данных безопасных соединений.

3.4. Описание подсистем

Название	Назначение	Функции
Система аутентификации	Аутентификация пользователей	Обеспечивает двухфакторную аутентификацию удаленного пользователя в КИС на базе технологии RSA SecurID при использовании удаленными пользователями токенов SecurID
Система VPN	Установка VPN соединений	Обеспечивает доступ пользователей к ресурсам КИС по технологии IPSec/VPN в необходимый сетевой сегмент или SSL/VPN при доступе к Web приложениям
Система LDAP	Хранение информации о субъектах КИС	Обеспечивает хранение сертификатов центров сертификации, входящих в состав УЦ Компании, и списков отозванных сертификатов
Удостоверяющий центр	Выдача, отзыв сертификатов	Обеспечивает выпуск сертификатов пользователей СУД и списков отозванных сертификатов

4. Модули системы и требования по их развертыванию

Элемент ИТ инфраструктуры	Тип и название модуля	Описание деталей установки и конфигурации
Сервер аутентификации	RSA Authentication Manager (master)*	Обеспечивает двухфакторную аутентификацию удаленного пользователя в КИС на базе технологии RSA SecurID при использовании удаленными пользователями токенов SecurID
Реплика сервера аутентификации	RSA Authentication Manager (replica)*	Обеспечивает балансировку нагрузки и неотказуемость системы

Элемент ИТ инфраструктуры	**Тип и название модуля**	**Описание деталей установки и конфигурации**
Устройство VPN	Cisco ASA 5520 (master)	Обеспечивает доступ пользователей к ресурсам КИС по технологии IPSec/VPN в необходимый сетевой сегмент или SSL/VPN при доступе к Web приложениям
Дублирующее устройство VPN	Cisco ASA 5520 (backup)	Обеспечивает функционал Cisco ASA (master) в случае прекращения его функционирования
Пользовательское ПО для установки VPN соединений	Cisco VPN Client	Обеспечивает доступ пользователей по технологии IPSec/VPN в необходимый сетевой сегмент
Сервер каталогов	LDAP Server*	Обеспечивает хранение сертификатов центров сертификации, входящих в состав УЦ Компании, и списков отозванных сертификатов
Удостоверяющий центр	RSA Keon CA*	Обеспечивает выпуск сертификатов пользователей СУД и списков отозванных сертификатов
Устройство для хранения ключевой информации пользователя	CyberFlex SmartCard	Обеспечивает хранение ключевого материала пользователей
Устройство для хранения ключевой информации пользователя	eToken	Обеспечивает хранение ключевого материала пользователей
Генератор одноразовых паролей	RSA SecurID token SD600	Обеспечивает создание одноразовых паролей пользователей, используемых при аутентификации

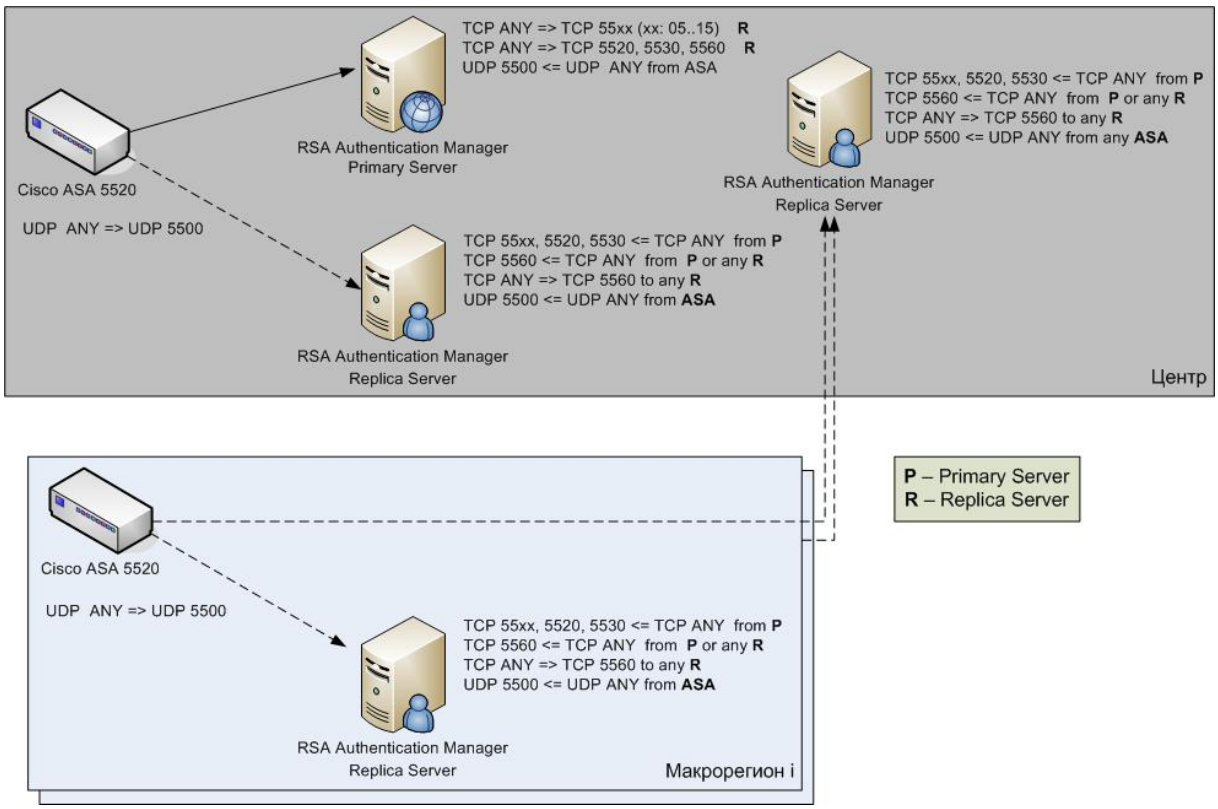

Рис. 1. Общая архитектура системы аутентификации

4.1. Архитектура централизованной системы аутентификации

В документе приводится общее описание централизованной архитектуры системы аутентификации Компании в контексте ее использования в СУД как в Москве, так и в регионах.

4.1.1. Общая архитектура системы

Система аутентификации состоит из 10 серверов с установленным и функционирующим ПО RSA Authentication Manager 6.0 (см. рис. 1). При этом в каждом МР для аутентификации пользователей используется сервер, на котором ПО RSA Authentication Manager выполняется в режиме Replica (всего восемь инсталляций). В центре располагается основной сервер (Primary) и две реплики (Replica) RSA Authentication Manager, одна из которых используется для обеспечения отказоустойчивости в случае выхода из строя какого-либо из Replica-серверов, расположенных в регионе.

4.1.2. Разграничение доступа региональных администраторов

Для разграничения полномочий администраторов по различным регионам, используется концепция сайтов (sites). Сайт представляет собой объединенную группу сетевых узлов, на которых будет производиться аутентификация пользователей. В свою очередь пользователи могут быть объединены в группы (groups) в соответствии с теми регионами, в которых они находятся.

4.1.3. Средства администрирования

В качестве основного средства администрирования в регионах предлагается использовать GUI-консоль RSA Authentication Manager Remote Mode, что позволяет избавиться от необходимости развертывания/использования WEB-сервера для системы Quick Admin.

5. Требования к техническим и программным средствам

Продукт или его компоненты	**Аппаратные требования**	**Программные требования**
RSA Authentication Manager	• Процессор: Sun Solaris Ultra SPARC • Физическая память: от 256 MB на каждый процессор + 1 MB на каждую 1000 пользователей + удвоенное значение физической памяти на файл подкачки • Дисковое пространство: от 400MB + 1 MB на каждую 1000 пользователей и резерв 1GB на базу данных логов	Solaris 8/9/10

Продукт или его компоненты	**Аппаратные требования**	**Программные требования**
RSA Keon CA	• Процессор: Sun Solaris Ultra Sparc 400MHz или лучший • Физическая память: от 256MB RAM • Дисковое пространство: от 100 MB	Solaris 8/9/10
Рабочее место пользователя	Рекомендуется: ПК, Pentium 4, 1GB RAM, наличие сетевого интерфейса	Windows, MAC OS X - операционная система с поддержкой сети и установленным ПО Cisco VPN client

6. Требования к безопасности

Роль/Профиль доступа	**Полномочия**	**Ответственность**
Системный администратор RSA Authentication Manager	Должен быть наделен всеми правами доступа к RSA Authentication Manager master и replica	Техническая поддержка системы аутентификация RSA Authentication Manager, регистрация агентов, создание групп пользователей, настройка отказоустойчивости, оказание квалифицированной помощи при проведении плановых работ по повышению надежности системы, изменение топологии и конфигурации, модернизация оборудования и программного обеспечения

Роль/Профиль доступа	**Полномочия**	**Ответственность**
Системный администратор VPN-устройств	Должен быть наделен всеми правами доступа к Cisco ASA master и backup	Заведение групп пользователей, настройка LAN-2-LAN, создание резервных копий конфигурации
Системный администратор УЦ	Должен быть наделен всеми правами доступа к RSA Keon CA	Настройка параметров жизненного цикла сертификатов, настройка публикации сертификатов и списков отзыва
Системный администратор LDAP-сервера	Должен быть наделен всеми правами доступа к LDAP серверу	Техническая поддержка и сопровождение LDAP-сервера
Системный администратор Sun SPARC Solaris	Должен быть наделен достаточными правами для сопровождения Sun Solaris	Техническая поддержка и сопровождение Sun SPARC Solaris
Администратор по работе с пользователями	Должен быть снабжен пакетом пользовательского ПО, а также достаточными для воспроизведения действий других пользователей правами	Техническая поддержка и сопровождение пользовательского окружения

7. Требования к доступности

Название системы	**Характер взаимосвязи**
Cisco ASA 5520 (master и replica)	Обеспечивают установление VPN соединений. При отключении master его функции будет выполнять replica. При отключении обоих устройств доступность системы равна нулю (система неработоспособна).

Название системы	**Характер взаимосвязи**
RSA Authentication manager (master и replica)	Обеспечивает аутентификацию пользователей. При сбое master его функции берет на себя replica. При сбое или остановке обоих сервисов последующие запросы пользователей на соединение будут отклонены из-за ошибки аутентификации.
RSA Keon CA	Осуществляет выдачу, отзыв пользовательских сертификатов, а также публикацию списков отозванных сертификатов(CRL) в LDAP. Остановка сервиса сказывается на доступности системы в момент истечения срока действия CRL: в отсутствие нового списка пропадет возможность проверки пользовательских сертификатов. Кроме того, пропадет возможность отзыва скомпрометированных сертификатов, что является потенциальной уязвимостью и выдачи новых.
LDAP server	Обеспечивает хранение информации обо всех объекта КИС, включая информацию об удостоверяющем центре. Остановка сервиса отрицательно сказывается на доступности системы. В частности невозможной станет проверка пользовательских сертификатов, так как CRL будет недоступен. Исчезнет возможность добавления новых пользователей в каталог, а также удаление старых. Невозможной станет синхронизация каталога с RSA Authentication Manager.

8. Описание функционирования

Система удаленного доступа к ресурсам КИС Компании может функционировать согласно следующим сценариям:

1) Получение доступа в определенный сегмент КИС при помощи технологии VPN.

   Пользователь осуществляет соединение с Internet любым доступным ему способом. При помощи Cisco VPN Client осуществляет соединение с Cisco ASA 5520. При этом пользователю, согласно политике безопасности, необходимо аутен-

тифицироваться либо при помощи цифрового сертификата, либо при помощи одноразового пароля согласно технологии RSA SecurID:

- Использование цифрового сертификата.

  В зависимости от политики безопасности, цифровой сертификат и надлежащий ключевой материал могут находиться либо на смарт-картах CyberFlex SmartCard, либо на токенах eToken. В процессе аутентификации пользователю необходимо ввести соответствующий PIN-код для получения доступа к ключевому материалу. После получения доступа к ключевому материалу осуществляется проверка компонентом Cisco ASA предоставленного сертификата на предмет его наличия в списках отозванных сертификатов, хранящихся на сервере каталогов LDAP Server. На основании пользовательского сертификата и факта его отсутствия в соответствующих списках принимается решение о принадлежности пользователя к определенной группе и предоставляется доступ в определенный сегмент сети согласно политике безопасности для данной группы.

- Использование одноразового пароля согласно технологии RSA SecurID.

  Пользователь выбирает определенный профиль, в составе которого присутствует название группы и разделяемый секрет (pre-shared key). В соответствии с технологией SecurID, пользователю необходимо ввести действительный одноразовый пароль (PASSCODE). Эти данные безопасным способом будут проверены RSA Authentication Manager (или его репликой, если основной сервер не доступен), который, на основании данной информации выдает ответ относительно успешности аутентификации удаленного пользователя. В случае успешного прохождения аутентификации, пользователю предоставляется доступ в определенный сегмент сети согласно политике безопасности для данной группы.

2) Получение доступа к Web-сервисам при помощи технологии SSL/VPN.

   Пользователь осуществляет соединение с Internet любым доступным ему способом. Для доступа к сайту пользователю необходимо указать действительный одноразовый пароль (PASSCODE). Эти данные передаются на основной сервер RSA Authentication Manager (или на реплику, если основной сервер не доступен), который, на основании данной информации, выдает ответ относительно успешности аутентификации удаленного пользователя. Далее, Cisco ASA осуществляет проброс (проксирование) пользователя к запрашиваемому Web-ресурсу.

3) Получение доступа из сетевого сегмента КИС к ресурсам внешнего сетевого сегмента и наоборот при помощи технологии LAN-to-LAN на основе протокола IPSec. Между двумя VPN устройствами (со стороны Компании – Cisco ASA) устанавливается защищенный IPSec-туннель, в который направляется весь трафик между двумя сетевыми сегментами. Аутентификация VPN-устройств осуществляется при помощи разделяемого секрета (pre-shared key).

Принятые сокращения

КИС	Корпоративная информационная сеть
ПО	Программное обеспечение
СУД	Системf удаленного доступа
УЦ	Удостоверяющий центр
CRL	Certificate Revocation List (список отозванных сертификатов)
CA	Certification Authority
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
NDA	Non-Disclosure Agreement
SLA	Service Level Agreement