КОСМИЧЕСКИЕ ТЕХНОЛОГИИ И ПРИБОРЫ; СЕРВЕРНЫЕ ТЕХНОЛОГИИ ДЛЯ СОЗДАНИЯ ГИС И ГЕОПОРТАЛЫ

УДК 004.771, 551.506

DOI: 10.23885/2500-123x-2018-2-3-90-93

ОПЫТ ПОСТРОЕНИЯ ИНТРАНЕТ СРЕДЫ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБРАБОТКИ СИНОПТИЧЕСКОЙ ИНФОРМАЦИИ

А.И. Скрипников, С.Е. Жмуров

Северо-Кавказское управление по гидрометеорологии и мониторингу окружающей среды, г. Ростов-на-Дону
askripnikov@yugmeteo.donpac.ru, szhm@yandex.ru

Аннотация. Рассмотрены вопросы реализации защищенной интранет-сети в условиях развития интернет технологий и внедрения протоколов взаимодействия на основе сертификатов и шифрования.

Ключевые слова: интранет, DNSSEC, IPv6, IPv4

Задача реализации среды функционирования систем хранения и обработки синоптической и климатической информации появляется при необходимости обеспечить защиту внутренней сети от атак из публичных сетей. Особенно это актуально при наличии территориально разнесенных устройств и сетей – центров служб, расположенных в городах двух федеральных округов. Связь данных подразделений обычно осуществляется при помощи виртуальных цифровых VPN-каналов, организованных с помощью белых адресов в сети Интернет.

Эта технология хорошо работающая в сетях, поддерживающих протокол IPv4, превращает частные сети в общественные с включением в базовую конфигурацию протоколов IPv6. Этот процесс вошел в практику с появлением Windows сервера 2008R2 и развился в серверах 2012–2016. При этом, такие компоненты технологии как NAT64 и DNS64, создание туннелей в среде IPv4 позволяют обходить настроенные системы защиты [1]. Шифрование потока в IPSec является обязательной для этого протокола, а в старших версиях Windows серверов включена вне зависимости от используемых технологий. И кроме того, все адреса машин локальной сети получают белые адреса Интернет. Присоединив к этому принципиальное отсутствие NAT-технологии при использовании IPv6 протокола, мы получаем большие проблемы при обеспечении безопасности и целостности сетей, ранее считавшихся защищенными.

Усугубляет ситуацию массовое внедрение в практику Интернет технологии DNSSEC. Определение имен в Интернете происходит с помощью запросов к DNS-серверам, организованным по иерархическому принципу. Основу Интернета состав-

ляют корневые сервера, находящиеся на вершине пирамиды, которые находятся в ведении ICANN – корпорации по управлению доменными именами и IP-адресами (Internet Corporation for Assigned Names and Numbers). Это некоммерческая организация, несущая ответственность за координацию обслуживания нескольких баз данных уникальных идентификаторов, связанных с использованием доменных имен в Интернете, а также обеспечения стабильной и безопасной работы в сети. Она осуществляет функции IANA (Администрация адресного пространства Интернет). Процесс внесения изменения в корневую зону показан на рис.1 [2].

Сейчас в мире 13 корневых ДНС серверов от a-root до m-root и один скрытый мастер-сервер, что было связано с ограничением на размер UDP-запроса, но под этими именами скрывается более 200 серверов-зеркал с одинаковыми IP-адресами. Ближайшее к нам зеркало корневого L-сервера находится в городе Ростове-на-Дону. Операторами корневых серверов являются различные организации, получившие право управления серверами в относительно отдаленном прошлом. Среди них ICANN, VeriSign, NASA, Министерство обороны США, Internet Systems Consortium, Inc. В начале 2008 года в корневой зоне был внедрен протокол IPv6, что обеспечило полную поддержку этого протокола глобальной системой доменных имен.

Техника DNSSEC предполагает использование криптографической подписи и сертификатов при исполнении запросов определения имен сайтов. При этом для любого DNS-запроса любого клиента строится цепочка доверия – от корневого сервера до самого клиента проводится верификация

участвующих в запросе хостов и осуществляется идентификация клиента. И ни один из запросов без построения такой цепочки не будет исполнен. Для доменного имени каждая организация в цепочке должна подписать ключ следующей организации. Например для icann.org, зона.org подписывает ключи icann.org, а в корневой зоне подписываются ключи. При проверке по технологии DNSSEC запросы

идут по этой цепочке в направлении корневой зоны и автоматически сравниваются «дочерние» ключи с «родительскими» ключами. Сертификаты генерируются центрами сертификации, начиная от корня (VeriSign). Для обслуживания такой техники произошло разделение DNS-серверов на авторитарные, отвечающие за записи своей зоны, и рекурсивные, формирующие цепочки запросов.

Рис.1

Объединение техник шифрования, адресации и маршрутизации повышает защищенность Интернета, но кроме этого приводит к появлению спектра дополнительных возможностей управления клиентами, начиная от корневой зоны. Например, в зависимости от положения сертификата клиента на дереве сертификатов, клиентские машины могут получать разные ответы на одинаковый запрос.

Задача построения интранет-сети возникла из необходимости при территориальном разделении подразделений организации сохранить единую информационную среду, обслуживающую в том числе работу геоинформационных систем, внешних сайтов и других процессов. При взрывном внедрении в цифровое пространство технологий DNSSEC, IPv6, PQI (техника подписания и шифрования) обеспечение защищенности и целостности информационной среды представляет особую задачу. Для сохранения управляемости единая интранет-машина должна начинаться от точки (dot) – своей корневой

зоны, позволяющей обслуживать все запросы в адресном пространстве своей информационной среды.

Структура реализации интранет-сети показана на рис.2. Система расположена на трех различных площадках **a**, **b** и **c**, которые связаны между собой каналами связи, образующими доменные сети dot. и tld.dot. Домен tld.dot. предоставляет клиентам корневой DNS-сервер и служит инструментом развертывания и поддержки доменов dom1...domN. Общение и взаимодействие windows-доменов происходит в рамках данной интранет-машины.

Домен dot. служит для обеспечения связанности интранет-машины и осуществляет управление всеми доменами. Соответственно хосты домена dot. выполняют роль точки, контролирующей адресное пространство интранет-машины. Они же могут являться шлюзами взаимодействия с Интернет-машиной с полным контролем всего трафика. Сети Интернет и windows-доменов при этом функци-

онируют в режиме адресного пространства IPv4 и взаимодействие с ними осуществляется в рамках старого протокола IPv4. Хосты инструментальных доменов реализованы на базе открытого проекта FreeBSD и их программное обеспечение поддерживается в актуальном состоянии Интернет-технологий.

Такая система предоставляет клиентам минимально-необходимые функции цифровой среды, является масштабируемой, полностью поддерживает современный уровень информационных технологий. Дальнейшее развитие интранет-сети должно происходить в направлении полного перехода на адресное пространство IPv6.

Рис.2

Список литературы

1. Хамраева С. И., Маримбаева С.А. Безопасность IPV6 // Техника. Технологии. Инженерия. – 2017. – №2.1. – С. 40–41. – URL <https://moluch.ru/th/8/archive/57/2320/> (дата обращения: 13.07.2018)
2. Робачевский А. У корня ДНС [Электронный ресурс], – http://www.ripn.net/articles/at_the_root/ – статья в интернет

EXPERIENCE CREATING INTRANET ENVIRONMENT OF THE INFORMATION PROCESSING SYSTEM SYNOPTIC INFORMATION

A.I. Skripnikov, S.E. Zhmurov

North-Caucasian Department

Hydrometeorology and environmental monitoring

askripnikov@yugmeteo.donpac.ru, szhm@yandex.ru

Abstract. The issues of implementation of a secure intranet in the development of Internet technologies and the introduction of protocols based on certificates and encryption are considered.

Keywords: intranet, DNSSEC, IPv6, IPv4

References:

1. *Hamraeva S.I, Marimbaeva S.A.* IPV6 Security // Technique. Technologies. Engineering. – 2017. – №2.1. – С. 40–41. – URL <https://moluch.ru/th/8/archive/57/2320/> (date: 13.07.2018) (In Russian)
2. *Robachevskiy A.* At the root DNS [URL], – http://http://www.ripn.net/articles/at_the_root/ (In Russian)