Infoblox
CONTROL YOUR NETWORK

ТЕХНИЧЕСКОЕ ОПИСАНИЕ

Вы готовы к отражению DNS-атак?

Укрепление защиты критически важной инфраструктуры DNS

Вы готовы к отражению DNS-атак?

Укрепление критически важной инфраструктуры DNS

В 2013 году число атак на инфраструктуру с использованием протокола DNS (Domain Name System) возросло на 216%[1]. Почему? Потому что по своей природе служба DNS весьма уязвима.

- Большинство межсетевых экранов в компаниях настраиваются таким образом, чтобы разрешать трафик через порт 53 для службы DNS, что позволяет атакующим легко обходить имеющиеся системы защиты.
- Поскольку DNS-запросы асимметричны, это может приводить к тому, что ответный трафик будет во много раз превышать размер запроса, то есть сама система DNS может усиливать атаку. Хакеры могут отправить один пакет данных и вызвать шквал ответных пакетов, усиленный в несколько раз, который способен буквально парализовать вашу работу.
- Атакующие легко могут скрыть свой адрес, поскольку протокол DNS не предусматривает предварительной установки соединений между системами.

DNS-атаки также используются для отвлечения внимания от главной цели прорыва защиты компании и кражи данных; этот метод называется «дымовой завесой». DNS-перехваты (DNS hijacking) нарушают целостность DNS и перенаправляют пользователей, пытающихся получить доступ к какому-либо веб-сайту, на ложный сайт, контролируемый хакерами, который может выглядеть как настоящий сайт. Затем хакеры могут получить имена пользователей, пароли и другие важные данные. Для бизнеса DNS-перехват может означать прямые убытки и ущерб деловой репутации.

У крупных IT-организаций и поставщиков услуг практически нет выбора, кроме как бороться с этими уязвимостями, поскольку в эру Интернет службы DNS являются важной и почти критической функцией современного бизнеса. Без использования DNS не будут работать смартфоны, компания не сможет вести online-бизнес, нарушится эффективность взаимодействия в коллективе, производительность снизится, степень удовлетворенности клиентов упадет, доход уменьшится, репутация компании подвергнется риску.

Настоящий документ посвящен решению проблемы угроз, нацеленных на DNS. В нем рассматриваются функции протокола DNS, систематизируются различные типы DNS-атак, чтобы дать читателю возможность осознать масштаб угрозы, и предлагается наилучшее имеющееся решение — Infoblox Advanced DNS Protection, первое решение для служб DNS, которое защищает само себя и закрывает брешь в структуре безопасности.

Безопасность, доступность и целостность — вот три проблемы инфраструктуры DNS, и Infoblox Advanced DNS Protection решает все три.

Как работает служба DNS и за что она отвечает

Прежде чем перейти к угрозам и способам их предотвращения, давайте рассмотрим основы DNS. Служба DNS — это адресная книга для каждого пункта назначения в Интернете. Она преобразует доменные имена, например infoblox.com, в IP-адреса вида 54.235.223.101. Это значит, что DNS определяет, будут ли запросы и обмен данными направлены по правильному адресу. Чтобы компании и поставщики услуг могли вести бизнес в режиме реального времени и/или в Интернет, им требуются быстрые и точные службы DNS для входящего и исходящего трафика. Обмен данными между поставщиками, клиентами и отделениями компании происходит посредством электронной почты, веб-сайтов и передачи данных по протоколу HTTP. Существенный недостаток обработки DNS-запросов заключается в том, что серверы DNS немного похожи на главные двери в торговом центре — они пропускают как покупателей, так и воров.

Серверы DNS бывают двух видов: авторитативные (полномочные) и рекурсивные.

- Авторитативные DNS-серверы являются точкой доступа к службам компании. Они отвечают только на запросы о доменных именах, для которых они были настроены, или именах в конкретном наборе зон. DNS-серверы, которые соединяются с Интернетом, обычно настраиваются в авторитативном режиме, и они являются мишенями для атак извне, таких как усиление (amplification), отражение (reflection) и эксплойты (exploits).

- Рекурсивные DNS-серверы, еще называемые «кэширующими серверами», отвечают на запросы, отправляя запросы другим серверам имен, чтобы получить ответ. Иногда они извлекают ответ из кэша, чем и объясняется их второе название. Если рекурсивный сервер не находит необходимый ответ в кэше, он перемещается по дереву пространства имен, повторяя запрос и следуя по ссылкам с авторитативных серверов, пока не найдет сервер имен, который даст ответ. Другими словами, рекурсивные серверы имен зависят от авторитативных серверов имен. Рекурсивные серверы имен обычно разворачиваются во внутренней сети, чтобы предоставлять услуги внутренним пользователям. Они уязвимы для атак, исходящих от пользователей, которые находятся в компании или являются ее клиентами (в случае с провайдерами).

Каталог DNS-угроз

Число потенциальных угроз на момент написания той статьи поистине угрожающее. Мы перечислили их здесь и привели краткое описание каждой.

Прямые DNS-атаки с усилением (amplification) направлены на перегрузку исходящего канала DNS-сервера. Они начинаются с отправки большого количества DNS-запросов, специально созданных таким образом, чтобы получить очень большой ответ, размер которого может до 70 раз превышать размер запроса. Поскольку DNS использует протокол User Datagram Protocol (UDP), атакующий может использовать исходящий трафик малого размера, чтобы заставить DNS-сервер генерировать гораздо больший объем, что приведет к перегрузке исходящего канала DNS-сервера и в конечном счете к отказу в обслуживании (denial of service — DoS).

Атаки с отражением (reflection) используют сторонний DNS-сервер (обычно открытый рекурсивный сервер имен) в Интернете для распространения DoS- или DDoS-атаки путем отправки запросов на рекурсивный сервер. Рекурсивные серверы будут обрабатывать запросы с любого IP-адреса и возвращать ответы. При такой атаке адрес, с которого отправляются DNS-запросы, подменяется IP-адресом жертвы, и запрос будет иметь данные сервера жертвы, а не атакующего. В результате, когда рекурсивный сервер имен будет получать запросы, он будет отправлять все ответы на IP-адрес жертвы. Большой объем такого «отраженного» трафика может вывести из строя сайт жертвы.

Распределенные DoS-атаки с отражением (DrDoS) сочетают в себе атаки отражения и усиления, что значительно увеличивает вероятность нарушения работоспособности сервера жертвы. Как это ни парадоксально, но модули безопасности DNS Security Extensions (DNSSEC), разработанные для защиты ответов DNS путем шифрования и предотвращения «отравления» кэша, могут сделать атаки такого типа еще более эффективными, поскольку зашифрованные подписи DNSSEC увеличивают размер сообщений DNS. Усиление может доходить до 100 крат, а атакующие могут использовать сети botnet — в которые могут входить тысячи компьютеров — для увеличения числа отправленных запросов.

Это особенно опасная угроза, которой трудно противостоять. В сети Интернет существует около 33 миллионов открытых рекурсивных DNS-серверов[2], и 28 миллионов из них не имеют контроля доступа и могут использоваться для DrDoS-атак.

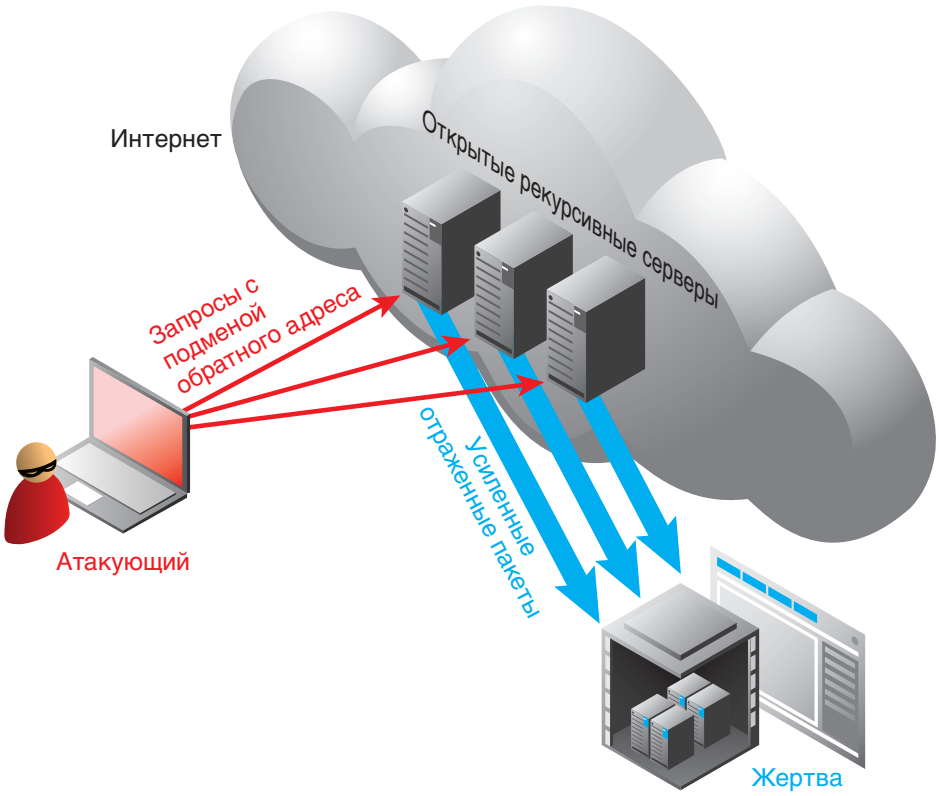

Рисунок 1. Распределенная DoS-атака с отражением

Атаки, направленные на перегрузку канала TCP/UDP/ICMP (flood-атаки) представляют собой объемные атаки с большим количеством пакетов, которые потребляют сетевые ресурсы и заполняют собой канал. Они используют протоколы TCP, UDP и ICMP.

UDP flood — это отправка большого числа UDP-пакетов на случайные порты удаленного сервера, который ведет проверку на наличие установленных на нем приложений, слушающих этот порт, но не находит их. В результате удаленный сервер будет вынужден возвратить большое число пакетов вида ICMP Destination Unreachable атакующему, сообщая, что данный объект назначения недоступен. Атакующий также может подменить обратный IP-адрес, чтобы ответы поступали не на сервер атакующего. Отправка ответов расходует все ресурсы сервера жертвы и приводит к тому, что сервер становится недоступен.

TCP SYN-flood заключается в установлении большого количества полуоткрытых TCP соединений, что приводит к тому, что сервер перестает отвечать на другие запросы клиентов на открытие новых соединений. Эта атака использует способ установления соединений по протоколу TCP. Каждый раз, когда клиент, например программа браузер, пытается открыть соединение, информация сохраняется на сервере. Поскольку это занимает память и ресурсы операционной системы, число устанавливаемых соединений ограничено, обычно оно меньше десяти. Затем сервер отправляет ответ клиенту, который отправляет в ответ уведомление, и соединение устанавливается. В этот момент ресурсы, находящиеся в очереди, освобождаются для приема других соединений.

При этой атаке специальная программа создает поддельные пакеты, которые сервер принимает за новые соединения. Эти пакеты помещаются в очередь, но соединение никогда не завершится, поэтому ложные соединения останутся в очереди, пока не истечет время ожидания. Атакуемая система перестает отвечать на запросы новых клиентов, пока атака не прекратится.

ICMP-атаки используют сетевые устройства, например роутеры, для отправки сообщений об ошибке, когда запрашиваемая служба недоступна или доступ к удаленному серверу отсутствует. Примерами ICMP-атак являются: ping-flood, ping-of-death и smurf.

Ping-flood быстро отправляет ICMP пакеты, не дожидаясь ответа, в результате канал жертвы переполняется echo-ответами ICMP, которые он отправляет обратно.

Ping-of-death отправляет разбитые на части ICMP-пакеты, превышающие допустимый размер. Когда сервер-получатель собирает эти части, размер пакета становится больше допустимого, что приводит к остановке работы сервера в результате переполнения буфера.

Smurf-атаки включают отправку поддельных ICMP пакетов, в которых адрес отправителя подменен на адрес жертвы. Все устройства в сети отвечают на эти пакеты и ответы переполняют сервер жертвы.

DNS-эксплойты используют ошибки в программном коде и реализации обработки протокола, чтобы воспользоваться уязвимостями ПО сервера DNS. Отправляя ложные DNS-пакеты на сервер DNS, атакующий может заставить сервер прекратить отвечать на запросы или вывести его из строя.

«Отравление» кэша DNS включает добавление ложной записи адреса домена Интернет в DNS-запрос. Если DNS-сервер принимает запись, на последующие запросы адреса домена отправляется ответ с адресом сервера, контролируемого атакующим. До тех пор пока ложный адрес будет находиться в кэше, входящие веб-запросы и сообщения электронной почты будут поступать на адрес атакующего. Новые атаки с отравлением кэша, например «парадокс дня рождения», используют метод перебора с одновременным увеличением количества запросов и поддельных ответов в расчете получить совпадение по одному из ответов и отравить кэш.

Аномалии протоколов отправляют неправильно сформированные DNS-пакеты, содержащие некорректные значения заголовков или их значение, на сервер жертвы, заставляя его прекратить отвечать на запросы или полностью выводя его из строя, создав бесконечный цикл в потоках на сервере. Иногда атаки маскируются под работу другого пользователя.

Разведка (reconnaissance) состоит из попыток получить информацию о сетевом окружении до запуска большой DDoS-атаки или любого другого типа атаки. Метод заключается в сканировании портов и определении используемого ПО и их версий. Для этих атак характерно нетипичное поведение, которое, при его обнаружении, может служить ранним предупреждением о последующих угрозах.

DNS-туннелирование включает создание туннеля через DNS-порт 53, который открыт, если межсетевой экран настроен для передачи не-DNS трафика с целью обеспечить пропуск данных. Для атак такого рода широко используется бесплатно распространяемое приложение для туннелирования трафика IPv4 через DNS-серверы.

DNS-перехват изменяет параметры записи DNS (иногда в кэше), чтобы указать DNS-сервер или домен мошенника. При этом пользователи, пытающиеся получить доступ к какому-либо веб-сайту, перенаправляются на ложный сайт, контролируемый хакерами, который может выглядеть как настоящий. Затем хакеры могут получить имена пользователей, пароли и другие важные данные.

Атака NXDOMAIN переполняет DNS-сервер запросами о несуществующих доменах. Это приводит к тому, что DNS-сервер отправляет ответы NXDOMAIN (несуществующий домен). Когда DNS-сервер переполняется большим объемом таких запросов, все ответы NXDOMAIN, которые он вынужден отправлять обратно, вызывают перегрузку исходящего канала.

Фантомный домен атакует рекурсивный DNS сервер большим количеством запросов к несуществующим доменам. Атака этого типа отличается от атаки NXDOMAIN, поскольку запросы этого типа не создают ответов NXDOMAIN, а заставляют DNS-сервер продолжать опрос доменов, которые в действительности не существуют, или предоставлять ответ. Сервер потребляет ресурсы, ожидая ответ от несуществующих доменов, что в конечном итоге приводит к падению производительности или прекращению работы.

Недостаточность имеющихся мер безопасности

Имеются решения, направленные на защиту DNS, но в действительности их возможности защиты ограничены. Большинство из них представляет собой внешние продукты, которые «прикручиваются» в качестве надстройки, вместо того, чтобы создаваться с самого начала для защиты от атак на DNS. В этих решениях используются такие подходы, как выделение избыточных ресурсов, глубокая проверка пакетов, общая защита от DDoS-атак, простое ограничение скорости и использование облачных технологий.

Подход 1: выделение избыточных ресурсов.

Для реагирования на DDoS-атаки можно использовать технологии типа систем балансировки нагрузки, увеличивающие производительность сети, с расчетом на то, что атака в какой-то момент времени прекратится. Такой подход не позволит успевать за быстро растущим масштабом DDoS-атак, и кроме того, его нельзя использовать для мониторинга злонамеренного или искаженного DNS-трафика.

Подход 2: глубокая проверка пакетов.

Межсетевые экраны и устройства на основе систем предотвращения вторжений (intrusion prevention system, IPS) следующего поколения предоставляют определенную защиту от обычных уязвимостей и DDoS-атак уровня 3. Однако они не могут выявлять или подавлять аномалии протоколов, связанные с DNS, или атаки на основе DNS. Они требуют чрезвычайно высокой вычислительной мощности, чтобы точно определять атаки на основе DNS, что делает глубокую проверку непрактичным подходом с точки зрения стоимости и числа необходимых точек распределения.

Подход 3: общая защита от DDoS-атак.

Эти решения охватывают широкий диапазон DDoS-атак, однако не содержат глубокого понимания атак на основе DNS.

Подход 4: облачные решения.

Облачные решения нацелены только на объемные атаки и не обеспечивают защиты от других типов атак. Кроме того, они ставят под угрозу конфиденциальность[3] данных, их можно обойти[4], и они могут вызывать проблемы, связанные с увеличением времени ответа на запросы.

Подход 5: простое ограничение скорости ответа (Response-Rate Limiting — RRL).

Простое («неинтеллектуальное») ограничение скорости ответа — это решение «на все случаи», заключающееся в установке порогового значения. Однако такой подход может привести к блокировке легитимного трафика. Различные источники DNS-трафика могут иметь разные требования. Например, расположенный по направлению основного трафика сервер кэша DNS может генерировать в 100 раз больший трафик, чем обычный настольный компьютер, и этот трафик может быть легитимным. Прокси-сервер для передачи данных по протоколу HTTP или сообщений электронной почты может иметь более интенсивный трафик DNS. Поэтому простое ограничение скорости создаст слишком много ложноположительных срабатываний, что означает, что сотрудники и клиенты могут не получить доступа к ресурсам в то время, пока выявляется DDoS-атака.

Комплексная защита от угроз от компании Infoblox закрывает брешь

В настоящее время есть только один эффективный способ ответить на эти DNS-угрозы безопасности вашей сети: непосредственно на самих DNS-серверах. Компания Infoblox может помочь в этом, поскольку у нас есть глубокие знания протокола DNS.

Решение Infoblox Advanced DNS Protection это сервер DNS с интегрированной защитой **в широком диапазоне** от атак на DNS, включая объемные атаки,

такие как перегрузка, усиление и отражение, а также атаки, не связанные с объемом запросов, например эксплойты. Оно также обеспечивает целостность DNS, которой могут угрожать атаки перехвата DNS. В отличие от подходов, основанных на выделении избыточных ресурсов или простом ограничении скорости, решение Advanced DNS Protection интеллектуальным образом определяет и подавляет DNS-атаки, отвечая только на легитимный трафик. Кроме того, оно использует технологию Infoblox Threat Adapt для автоматического обновления защиты от новых и усовершенствованных угроз по мере их возникновения без необходимости устанавливать пакеты исправлений. Возможности этого решения описаны ниже.

Защищенный сервер DNS — наилучшее решение для противодействия атакам на DNS

Сервер Infoblox Advanced Appliance — это усиленный сервер DNS со встроенной системой защиты. В нем эффективно используются выделенные вычислительные мощности, чтобы фильтровать атаки до того, как они достигнут сервиса DNS. Его можно настроить как авторитативный сервер или как рекурсивный сервер DNS.

Защита от DNS-угроз с самым большим охватом из имеющихся на рынке решений

Advanced DNS Protection осуществляет постоянный мониторинг, выявление и предотвращение всех типов DNS-атак, включая объемные и другие атаки, такие как эксплойты, одновременно отвечая на легитимные запросы. Оно также обеспечивает целостность DNS, которой могут угрожать атаки подмены DNS.

Технология Infoblox Threat Adapt

Расширенная защита DNS использует технологию Infoblox Threat Adapt для автоматического обновления правил защиты от новых и усовершенствованных угроз по мере их возникновения. В технологии Threat Adapt для обновления правил защиты используется анализ и изучение усовершенствованных видов атак, включая те, которые мы наблюдали в сетях клиентов, а также данные изменений конфигурации DNS.

Глобальная видимость атак и создание отчетов

Благодаря созданию подробных отчетов Advanced DNS Protection предоставляет подробную картину точек и типов атак по всей сети и предлагает интеллектуальное решение по выбору необходимого действия. Отчеты доступны через сервер отчетов Infoblox.

Быстрое развертывание

Решение Advanced DNS Protection легко развернуть и запустить, что позволяет сразу же блокировать атаки, даже если вы их уже испытываете.

Почему так высока эффективность Infoblox Advanced DNS Protection

Ни одно решение не может обеспечить защиту от множества разнообразных методов, используемых для атак через серверы DNS, поэтому Infoblox Advanced DNS Protection сочетает ряд конкретных технологий реагирования.

- **Интеллектуальное ограничение скорости** может установить «тормоз» на атаки DNS DDoS и flood-атаки без прекращения предоставления услуг легитимным пользователям. Интеллектуальное ограничение скорости возможно благодаря способности Advanced DNS Protection различать разные типы запросов и их частоту. Например, расположенный по направлению основного трафика сервер кэша DNS может генерировать в 100 раз больший трафик, чем обычный настольный компьютер, и этот трафик может быть легитимным. Прокси-сервер для передачи данных по протоколу HTTP или сообщений электронной почты имеет большую потребность в DNS трафике, который является легитимным.

    - **Регулировка на основе источника** определяет аномальные запросы и запрещает работу различных методов перебора.

  - **Регулировка на основе целевого объекта** определяет аномальное увеличение трафика, сгруппированное по целевым доменам.

- **Проверка целостности DNS** поддерживает целостность записей DNS путем периодического выполнения проверок работоспособности и правильности делегирования, что обеспечивает устранение всех угроз целостности записей в результате DNS-перехватов.
- **Выделенные программируемые процессоры** обеспечивают высокопроизводительную фильтрацию трафика, что делает возможным удаление вредоносного трафика до того, как он достигнет сервиса DNS.
- **Выявление разведывательной активности и сообщение о ней** может помочь выявить атаки и позволить группам по обслуживанию сетей подготовиться к ним даже до того, как они начнутся.
- **Анализ пакетов на типы эксплойтов, направленных на конкретные уязвимости** позволяет остановить некоторые атаки до того, как они достигнут ПО DNS.
- **Полная видимость и возможности по созданию отчетов** позволяют группам по обслуживанию сетей распознавать атаки, которые происходят в различных частях сети. Таким образом создается широкомасштабное представление и предоставляется информация о масштабе и серьезности атак, чтобы можно было предпринять необходимые действия.
- **Защита от новых и усовершенствованных угроз с помощью технологии Infoblox Threat Adapt** гарантирует развитие Advanced DNS Protection в условиях меняющейся среды угроз.
- **Advanced DNS Protection — это сервер DNS**, и он НЕ будет обрабатывать нелегимный трафик, в отличие от сетевых устройств, которые не используют интеллектуальных алгоритмов или не используют знаний о трафике DNS.

Все эти методы вносят вклад в достижение одного результата: постоянное обеспечение отказоустойчивых, безопасных и надежных служб DNS, даже если на них совершается атака.

Пора закрыть брешь в вашей сети?

Надеемся, что в этом документе нам удалось привлечь ваше внимание к серьезной проблеме уязвимости DNS и убедить вас, что вы можете гарантировать надежность и производительность вашей сети, если примете меры безопасности, внедрив защиту DNS.

Встроенная система безопасности лучше той, которая внедрена позднее в качестве надстройки. Нет лучшего места для защиты от злонамеренных действий, использующих DNS, чем сами серверы DNS, которые являются их мишенями. И единственным решением, учитывающим эти факты, является Infoblox Advanced DNS Protection. Обратитесь к нам сейчас, чтобы узнать больше о критически важной защите от одних из самых опасных угроз, с которыми сталкивается ваша сеть.

О компании Infoblox

Компания Infoblox (NYSE:BLOX) со штаб-квартирой в г. Санта Клара, шт. Калифорния, разрабатывает решения для автоматизации сетевого управления, технологии, соединяющей конечных пользователей, устройства и сети. Эти решения позволяют более чем 7000 компаниям и поставщикам услуг во всем мире преобразовывать, защищать и масштабировать сложные сети. Infoblox (www.infoblox.com) помогает снизить нагрузку на администраторов по контролю за сложными сетями, сократить расходы и увеличить безопасность, точность и время безотказной работы сетевого окружения.

1 Prolexic Quarterly Global DDoS Attack Report , Q4 2013

2 http://openresolverproject.org/

3 http://www.renesys.com/2013/10/google-dns-departs-brazil-ahead-new-law/

4 http://www.crn.com/news/security/240159295/cloud-based-ddos-protection-is-easily-bypassed-says-researcher.htm

ШТАБ-КВАРТИРА КОРПОРАЦИИ:

+1 (408) 986-40-00
+1 (866) 463-62-56
(звонки из США и Канады бесплатны)
info@infoblox.com
www.infoblox.com

ШТАБ-КВАРТИРА В РЕГИОНЕ EMEA:

+32 (3) 259-04-30
info-emea@infoblox.com

ДИСТРИБЬЮТОР В РОССИИ:

+7 (495) 662-39-66
infoblox@netwell.ru
www.netwell.ru