

Защита от нарушений безопасности с помощью межсетевых экранов и системы предотвращения вторжений

Компания Barnhart Crane & Rigging использует ASA 5500-X с IPS в развертывании «активный-резервный».

ОСНОВНЫЕ СВЕДЕНИЯ
BARNHART CRANE & RIGGING <ul style="list-style-type: none"> • Подъем и транспортировка тяжелого оборудования • Мемфис, штат Теннесси, США • 600 сотрудников
ЗАДАЧА <ul style="list-style-type: none"> • Предотвратить хакерские вторжения в сеть. • Улучшить уровень контроля за состоянием межсетевого экрана для выявления потенциальных уязвимостей. • Сегментировать трафик для повышения уровня безопасности и эффективности администрирования. • Развернуть систему обеспечения сетевой безопасности с возможностью ее модификации в рабочее время без снижения уровня защиты.
СЕТЕВОЕ РЕШЕНИЕ <ul style="list-style-type: none"> • Межсетевые экраны нового поколения Cisco ASA серии 5500-X с модулями системы предотвращения вторжений (IPS). • Межсетевой экран и защита от вторжений в одном устройстве. • Конфигурация «активный-резервный»
РЕЗУЛЬТАТЫ <ul style="list-style-type: none"> • Надежное предотвращение вторжений • Упрощение администрирования с повышением уровня контроля и защиты • Большую часть технического обслуживания можно выполнять без перебоев в работе межсетевого экрана или сверхурочной работы ИТ-отдела.

Задача

Компания Barnhart Crane & Rigging с головным офисом в Мемфисе, штат Теннесси, и 28 филиалами в других городах США, обслуживающая требовательных клиентов в строительной и других чувствительных к задержкам отраслях, не может позволить себе простоя в работе компьютерной сети. Поэтому, когда хакеры воспользовались брешью в межсетевом экране стороннего производителя (не Cisco) для захвата полосы пропускания Интернета, системный инженер Жене Шиналь и его коллеги решили, что пришло время для решения более крупной проблемы — проблемы защиты данных и цифровых материалов компании.

«Они обошли наш межсетевой экран, взломали Windows и использовали компьютер с ОС Windows для проникновения на другой сервер, — заявил Шиналь. — После этого они использовали нашу полосу пропускания для атаки других систем за пределами нашей сети».

В результате интернет-соединение было практически недоступно для сотрудников компании Barnhart. Частью проблемы оказался сам межсетевой экран.

По словам Шиналя, «в прежней системе межсетевого экрана было очень сложно просматривать настроенные преобразования NAT и правила межсетевого экрана. Поэтому мы не смогли увидеть брешь в межсетевом экране».

ИТ-специалисты Barnhart пришли к выводу о необходимости более эффективного и простого в управлении решения для предотвращения вторжений. Им также требовалось решение, которое могло бы осуществлять сегментацию входящего и исходящего интернет-трафика, границы сети компании Barnhart и VPN-соединений сотрудников. Кроме того, им было нужно отказоустойчивое решение для обеспечения безопасности с поддержкой конфигурации «активный-резервный», которое позволило бы выполнять техническое обслуживание инфраструктуры обеспечения безопасности в рабочее время без угрозы для безопасности сети.

Сетевое решение

Компания Barnhart остановила свой выбор на устройствах Cisco® ASA серии 5500-X с модулями Intrusion Prevention System (IPS). А именно, компания разместила два устройства 5525-X в головном офисе в Мемфисе и еще одно на узле аварийного восстановления возле города Ноксвилл в штате Теннесси.

Два устройства в Мемфисе обеспечили полную поддержку конфигурации «активный-резервный» для компании Barnhart: теперь сеть компании защищена с помощью межсетевого экрана и системы предотвращения вторжений, даже когда одному из устройств требуется техническое обслуживание. Конфигурация «активный-резервный» также позволила ИТ-специалистам выполнять рутинное обслуживание и справляться с самыми непредвиденными событиями без сверхурочной работы.

Cisco ASA 5525-X повышает уровень эффективности и безопасности сети Barnhart, поддерживая ее простую сегментацию. При настройке устройств Шиналь выполнил сегментацию Интернета, границы сети Barnhart и VPN-соединений сотрудников. Благодаря этой сегментации ИТ-отдел сумел настроить различные политики доступа для разных устройств и служб в сети.

Поставщик сетевых услуг управляет сетью MPLS, к которой подключены 14 офисов Barnhart; этот поставщик услуг также управляет межсетевыми экранами подключения к Интернету в поддерживаемых филиалах. Остальные площадки находятся под управлением собственных ИТ-специалистов Barnhart и подключены к главному офису по VPN-туннелям. Для максимального повышения эффективности все филиалы разделяют трафик: веб-трафик поступает непосредственно на необходимый веб-сайт, а для трафика компании используется подходящая внутренняя сеть.

Сотрудники Barnhart считают службу поддержки клиентов Cisco одним из решающих факторов для расширения сетевой инфраструктуры с помощью решения для обеспечения безопасности от Cisco. «Каждый раз при обращении в службу поддержки я получал обслуживание высшего качества», — говорит Шиналь.

Полученные результаты

Cisco ASA 5525-X с IPS помогает ИТ-специалистам Barnhart блокировать атаки и выполнять сегментацию сети, обеспечивая как повышение уровня безопасности, так и упрощение администрирования. Это устройство также обеспечивает безопасный доступ сотрудников к ресурсам Barnhart с любой удаленной площадки компании, а также с площадок клиентов или из любого другого места. По словам Шиналя, после развертывания решения Cisco он чувствует себя «как за каменной стеной под защитой пары устройств ASA 5525-X в конфигурации "активный-резервный"».

Решение для обеспечения безопасности в головном офисе Barnhart интегрировано с оборудованием в филиалах, часть которого находится под управлением ИТ-отдела Barnhart, а часть — под управлением поставщика сетевых услуг. Подключение коммутатора к межсетевому экрану/устройству IPS Cisco обеспечило ряд преимуществ для ИТ-специалистов Barnhart. Поскольку система предотвращения угроз интегрирована в межсетевой экран, ИТ-отдел управляет только одним устройством, которое успешно выполняет две функции.

Кроме того, сетевая инфраструктура Barnhart и так состояла в основном из оборудования Cisco, включая коммутаторы и маршрутизаторы Cisco в главном офисе и филиалах. В результате ИТ-специалисты быстро разобрались в особенностях нового устройства. ASA 5525-X предоставляет ИТ-специалистам Barnhart более подробные сведения о конфигурации системы безопасности, что позволяет им быстрее и проще выявлять потенциальные проблемы.

ПЕРЕЧЕНЬ ПРОДУКТОВ

Управление сетью

- Cisco Adaptive Security Device Manager (ASDM)
- Cisco IPS Device Manager (IDM)
- Интерфейс командной строки платформы Cisco Identity Services Engine

Обеспечение безопасности

- Cisco ASA 5525-X с IPS

Дополнительная информация

Для получения дополнительной информации о межсетевых экранах нового поколения Cisco ASA серии 5500-X с IPS перейдите по ссылке cisco.com/go/ips.




Главный офис в Америке
Cisco Systems, Inc.
Сан-Хосе, Калифорния

Главный офис в Азиатско-Тихоокеанском регионе
Cisco Systems (USA) Pte. Ltd.
Сингапур

Главный офис в Европе
Cisco Systems International BV Amsterdam.
Нидерланды

У Cisco имеется более 200 офисов по всему земному шару. Адреса, номера телефонов и номера факсов перечислены на веб-сайте Cisco Website по адресу www.cisco.com/go/offices.

 Cisco и логотип Cisco являются товарными знаками или зарегистрированными товарными знаками Cisco и/или аффилированных компаний в США и других странах. Для просмотра списка товарных знаков Cisco перейдите по следующему URL-адресу: www.cisco.com/go/trademarks. Товарные знаки третьих сторон являются собственностью соответствующих владельцев. Использование слова «партнер» не подразумевает партнерских отношений между Cisco и любой иной компанией. (1110R)

Напечатано в США

C36-728974-00 07/13