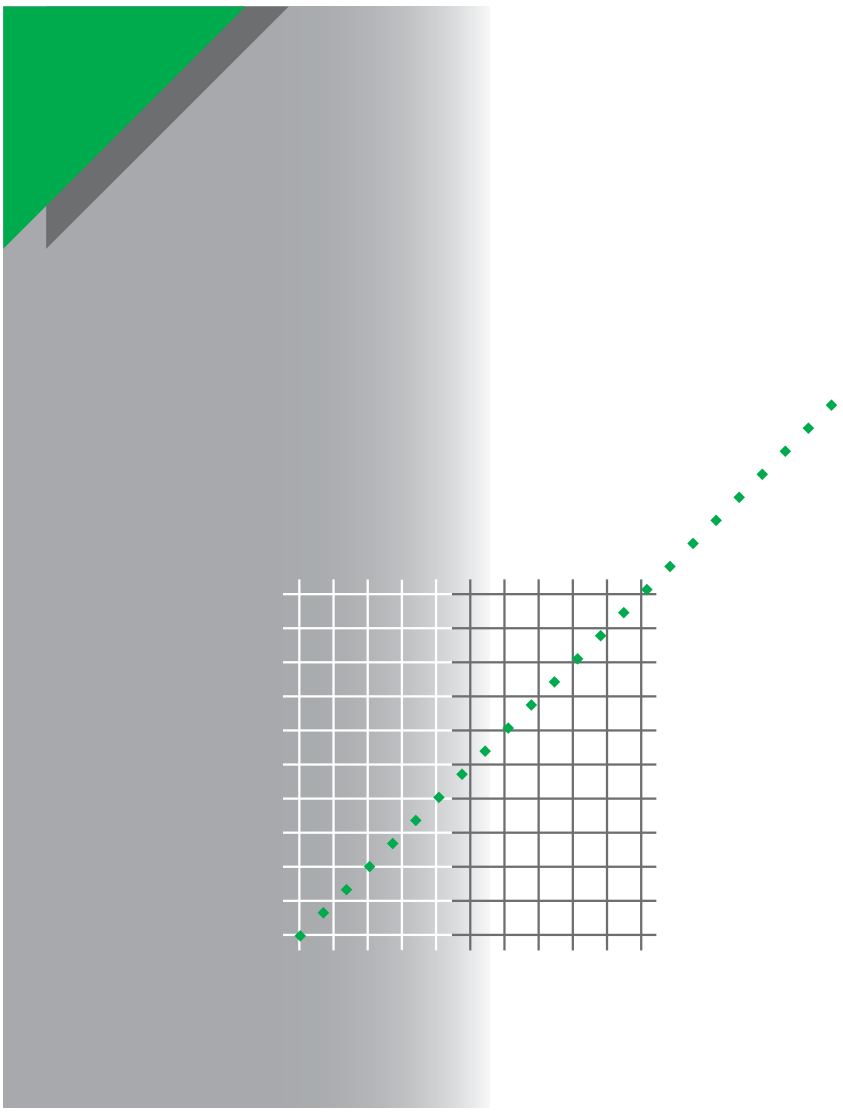
Техническая коллекция Schneider Electric

Выпуск № 36

Защита систем от кибер-атак



Schneider Electric

Компания Schneider Electric приступила к выпуску ***«Технической коллекции Schneider Electric»*** *на русском языке.*

Техническая коллекция *представляет собой серию отдельных выпусков для специалистов, которые хотели бы получить более подробную техническую информацию о продукции Schneider Electric и ее применении, в дополнение к тому, что содержится в каталогах.*

В ***Технической коллекции*** *будут публиковаться материалы, которые позволят лучше понять технические и экономические проблемы и явления, возникающие при использовании электрооборудования и средств автоматизации Schneider Electric.*

Техническая коллекция *предназначена для инженеров и специалистов, работающих в электротехнической промышленности и в проектных организациях, занимающихся разработкой, монтажом и эксплуатацией электроустановок, распределительных электрических сетей, средств и систем автоматизации.*

Техническая коллекция *будет также полезна студентам и преподавателям ВУЗов. В ней они найдут сведения о новых технологиях и современных тенденциях в мире Электричества и Автоматики.*

В каждом выпуске ***Технической коллекции*** *будет углубленно рассматриваться конкретная тема из области электрических сетей, релейной защиты и управления, промышленного контроля и автоматизации технологических процессов.*

Валерий Саженков,
Технический директор
ЗАО «Шнейдер Электрик»,
Кандидат технических наук

Выпуск № 36

Защитита систем от кибер-атак

Выпуск № 36, апрель 2011 г.

Предостережение

Этот документ не является исчерпывающим для всех систем с подобной архитектурой и не освобождает пользователей от их обязанности по соблюдению требований безопасности для оборудования, используемого в их системах или соблюдения национальных и международных норм безопасности, законов и нормативных актов.

Считается, что читатели уже знают, как использовать продукты, описанные в серии руководств с названием Технические Замечания по разработке Систем /System Technical Note (STN).

Документы серии STN не заменяют руководств пользователя.

Коллекция документов STN

Реализация проекта автоматизации включает в себя пять основных этапов: выбор, проектирование, настройка, внедрение и эксплуатация. Для того чтобы помочь в поэтапной разработке целого проекта, компания Шнейдер Электрик разработала серию книг технической концепции: System Technical Guide (STG) /Руководство по Созданию Системы/ и System Technical Note (STN) /Технические Замечания по разработке Систем/.

Руководство по Созданию Системы (STN) представляет собой техническое руководство и рекомендации по применению технологий в соответствии с потребностям пользователей. Это руководство охватывает весь жизненный цикл проекта: от выбора оборудования и методологии проектирования до примеров исходного кода для компонентов системы.

Документы с названием «Технические Замечания по разработке Систем» отличаются более глубоким теоретическим подходом, сосредотачивая внимание на особенностях применяемых технологий. Эти руководства представляют все технологии, которые можно применить для построения решения в рассматриваемой сфере и, следовательно, помогут вам в разработке проекта

Документы STG и STN связаны между собой и дополняют друг друга. Таким образом, вы сможете ознакомится с основами технологий в STN, и изучить соответствующие приложения в одном или нескольких STG.

Среда разработки

Идеология PlantStruxure для систем автоматического управления от Шнейдер Электрик представляет собой целостную разработку, которая предназначена для промышленных и инфраструктурных предприятий и позволяет удовлетворить свои потребности в автоматизации с соблюдением растущих требований к рациональному использованию энергии.

Содержание

1. Обзор безопасности

1.1. Цель

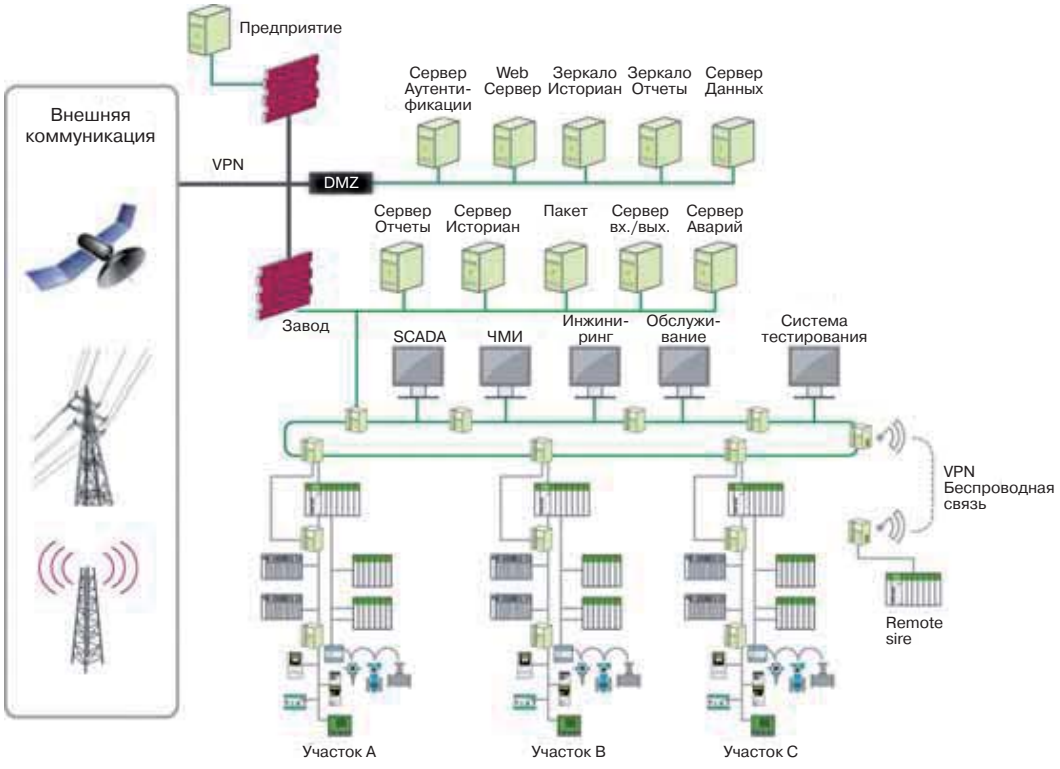
Целью Технических Замечаний по разработке Систем (STN) является описание совместимости различных решений, предлагаемых Шнейдер Электрик, с существующими в промышленности технологиями. В данном документе рассматриваются решения безопасности для критически важных сетевых приложений и, следовательно, общее повышение безопасности структуры на основе сети Ethernet. В нем содержится общее описание, которое понятно для конечных пользователей, системных интеграторов, производителей оборудования, коммерсантов и других специалистов.

1.2. Вступление

Технология PlantStruxure характеризуется открытостью и прозрачностью, обеспечивая плавную связь системы управления предприятием, сетью системы управления и Интернетом. Однако такая прозрачность не должна быть использована для негативного воздействия на производство, оборудование, а так же оказывать воздействие на безопасность персонала и окружающей среды.

В настоящее время безопасность уже не вторична, а является обязательным требованием, и рассматривается как важное условие обеспечения высокой готовности оборудования. Для решения проблем безопасности, Шнейдер Электрик использует самый современный и наиболее надежный подход:

- в партнерстве с Hirschman Шнейдер Электрик предлагает брандмауэры для сети управления с высоким уровнем безопасности связи, такие как VPN и DMZ. Межсетевой экран / маршрутизатор разделяет управляющие сети;
- обеспечивает возможность сегментирования сети с помощью коммутаторов ConneXium через сети VLAN для ограничения доступа к внутренним ресурсам, повышая ответственность персонала и предотвращая проблемы брандмауэра;
- предлагает устанавливать устройства PAC для модулей Ethernet с обеспечением защиты при помощи пароля и контролем доступа с возможность отключения ненужных сервисов;
- обеспечивает безопасную связь через VPN и усиленную аутентификацию для RTU.



Целью данного документа является описание важности темы сетевой безопасности, представление вопросов кибер-безопасности, кибер-уязвимости и методов проникновения в сети, а также рекомендации Schneider Electric по уменьшению рисков. Помните: нет ни одного продукта, который может полностью защитить сети.

1.3. Почему безопасность является важной темой сегодня?

Системы промышленного управления находятся вокруг нас в течение многих десятилетий. Ранее системы управления разрабатывались на основе запатентованных технологий, которые изолировали системы от внешнего мира и, следовательно, безопасность не являлась первостепенной. Сегодня, чтобы сократить расходы и повысить производительность, системы управления переходят в разряд открытых систем с использованием стандартных технологий, таких как операционные системы Microsoft и сеть Ethernet TCP/IP. Сеть Ethernet предоставляет новые возможности, которые были недостижимы при использовании устаревших сегодня сетей. Она позволяет:

- интегрировать приложения автоматизации;
- встраивать WEB-сервера;
- беспроводную связь;
- удаленный доступ для обслуживания;
- обслуживание автоматизированных систем;
- распределенная обработка;
- мгновенный доступ к информации из бизнес-процессов, инвентаризация, производство, доставка и приобретение …

Сегодня имеются другие силы, которые требуют обеспечения безопасности:

- стандарты кибернетической безопасности NERC;
- правила PUC;
- давление со стороны общественности и правительства;
- законодательство;
- профессионализм и ответственность;
- вопросы страхования;
- потеря сервиса;
- безопасность правообладателя.

При использовании стандартных технологий, таких как Ethernet, системы управления уязвимы для кибер-атак, как снаружи, так и изнутри сети системы управления предприятия.

Развертывание системы безопасности для автоматизированной системы управления может сталкиваться с некоторыми проблемами, например:

- физические и логические границы могут меняться;
- системы могут быть установлены на огромных географических регионах с несколькими сайтами;
- реализация безопасности может неблагоприятно сказаться на процессе управления.

2. Что такое кибер-безопасность?

Кибер-безопасность является частью безопасности компьютерных систем и информационных технологий. Целью кибер-безопасности является защита информации и интеллектуальной собственности от воровства, коррупции, или стихийного бедствия, при этом информацию остается доступной и может быть использована авторизованными пользователями. Кибер-безопасность состоит из процедур, политик, программ и оборудования. Она представляет собой непрерывный процесс.

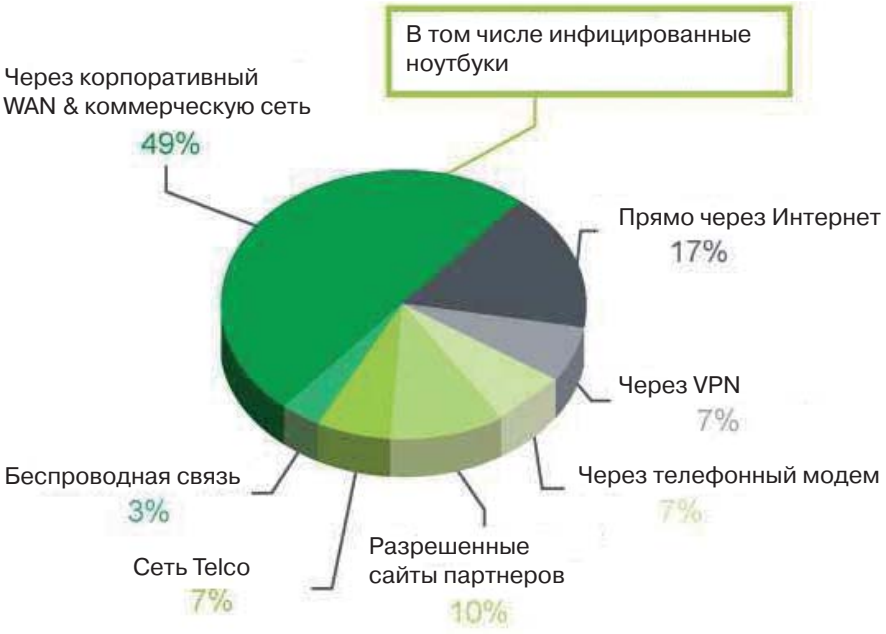
2.1. Профиль кибер-атак

Кибер-атаки на системы управления могут поступать из различных источников:

- Внутренних (сотрудников, поставщиков и подрядчиков):
  - случайного характера;
  - ненадлежащее поведение работников/подрядчиков;
  - недовольные сотрудники/подрядчики.
- Внешних случайных (ненаправленных):
  - детские шалости;
  - развлечения хакеров;
  - авторы вирусов.
- Внешних умышленных (направленных):
  - криминальные группы;
  - активисты;
  - террористы;
  - разведывательные органы иностранных государств.
- Целью кибер-атак на системы управления является:
  - срыв производственного процесса путем блокирования или замены информационных потоков;
  - повреждение, блокировка или отключение оборудования, что может привести к остановке производства, угрозе жизни человека или негативному воздействию на окружающую среду;
  - использование маскировки, отправка операторам ошибочной информации, стимулирующей их произвести ошибочные действия, которые могут иметь негативные последствия;
  - рекомендации изменить конфигурацию программного обеспечения или настройки оборудования для вывода системы из строя;
  - передача системе вредоносных программ (программное обеспечение, разработанное, чтобы проникнуть в компьютер без осознанного согласия его собственника);
  - изменение настроек систем безопасности, что потенциально может угрожать жизни человека.

Большинство кибер-атак в системы управления приходят через информационные сети предприятия, подключенные к Интернет.

Атаки на системы управления



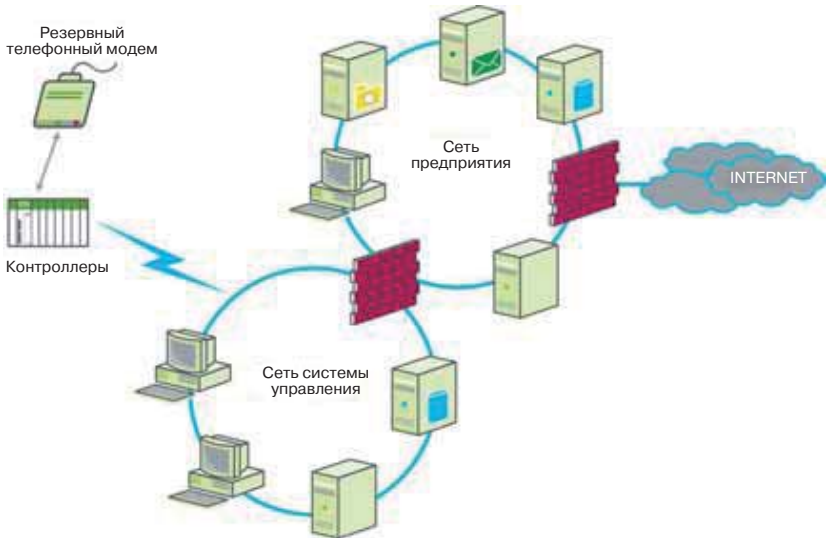
2.2. Как злоумышленники могут получить доступ к системе управления

Для того, чтобы атаковать систему управления, построенную на основе промышленных сетей, злоумышленник должен обойти защиты. Наиболее распространенные методы получения доступа:

- телефонный доступ к устройствам RTU;
- доступ через поставщика услуг (техническая поддержка);
- сетевые IT- продукты;
- корпоративный VPN;
- связь с базой данных;
- плохо настроенные брандмауэры;
- услуги передачи данных.

2.2.1. Доступ через телефонный модем к устройству RTU

Большинство систем управления имеют резервный модем для доступа в случае, если основная сеть не доступна. Злоумышленник должен знать протокол RTU для того, чтобы получить доступ.

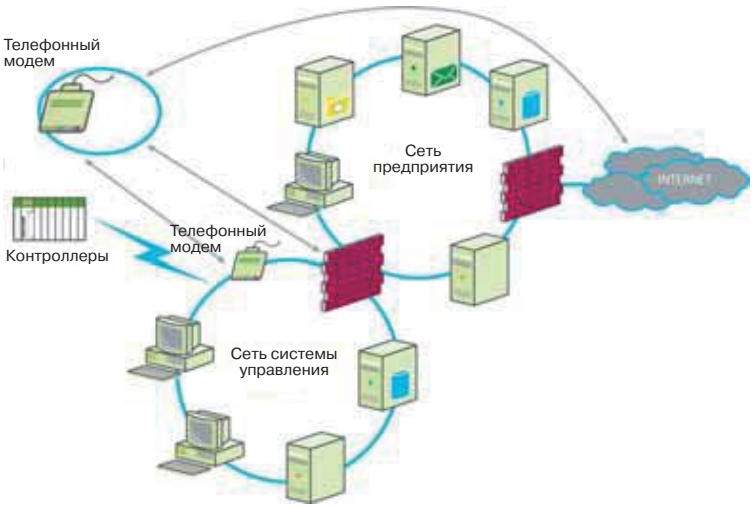


Ниже представлен типичный сценарий атаки:

Фаза	Описание
1	Атака злоумышленника начинается с набора разных телефонных номеров в городе в поисках модема, включая любое добавочные номера в рамках телефонной системы компании.
2	Большинство RTU систем автоматически идентифицируют себя и сообщают производителя модема.
3	Устройства RTU, как правило, не используют аутентификацию.
4	В некоторых случаях пароль RTU, заданный по умолчанию, не был изменен разработчиком системы при настройке.

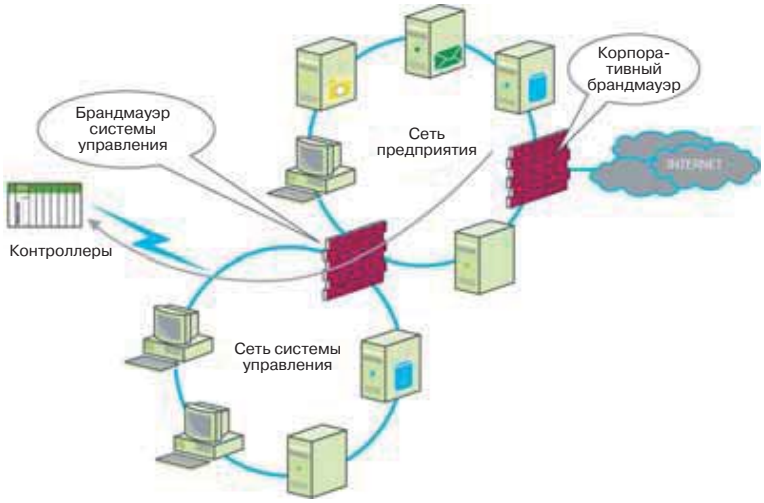
2.2.2. Поставщик услуги доступа

В целях минимизации простоев, поставщики коммуникационных услуг часто открывают доступ через VPN для удаленного обслуживания. Порты после обслуживания часто остаются открытыми, предоставляя злоумышленнику доступ к ресурсам поставщика и позволяя удаленное подключение к сети системы управления.



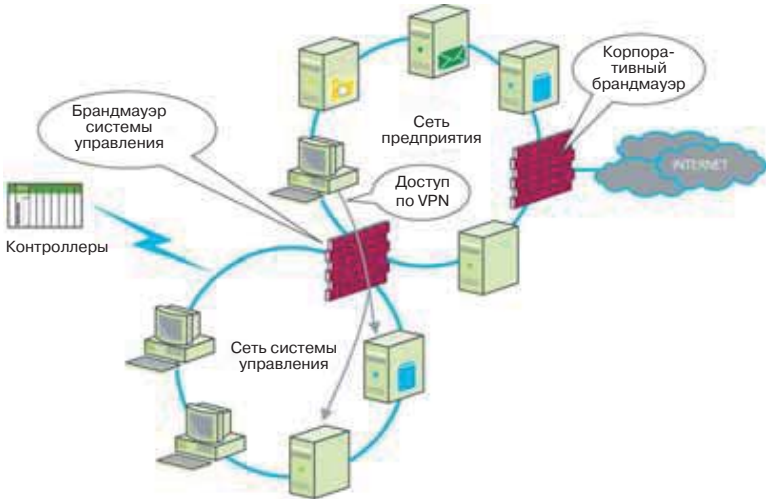
2.2.3. Коммуникационное оборудование, управляемое специалистами ИТ

Обычно специалисты отделов информационных технологий (ИТ) ограничивают доступ пользователей систем управления к оборудованию внутри объекта. ИТ-отдел принимает на себя ответственность за организацию удаленной связи, которая, как правило, контролируется и обслуживается специалистами отдела продаж. Опытный хакер может получить доступ коммуникационному оборудованию и перенастроить или отключить передачу данных внутри объекта.



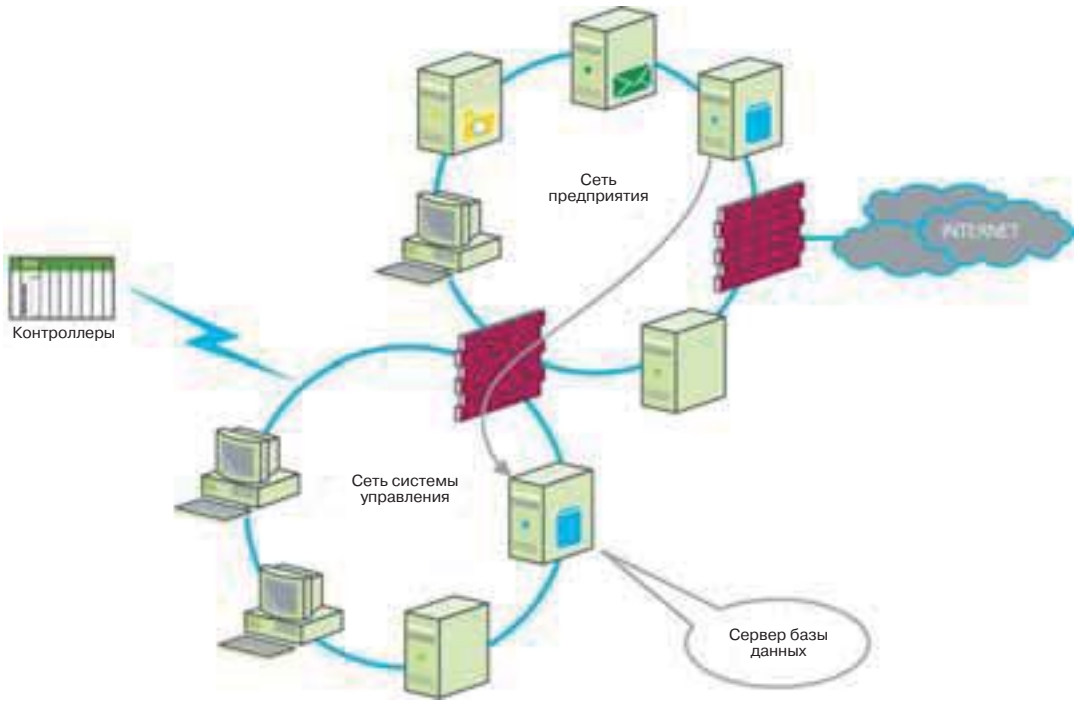
2.2.4. Корпоративная сеть VPN

Инженеры часто находятся в корпоративном офисе используют VPN бизнес-центров, чтобы получить доступ к сетям систем управления. Злоумышленник ждет пока обычный пользователь VPN будет подключаться к сети системы управления и после этого перехватывает связь.



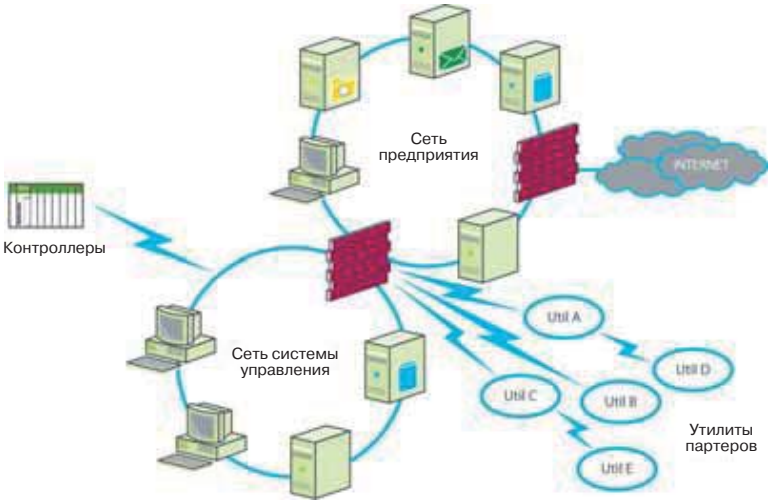
2.2.5. Подключения к базам данных

Большинство систем управления используют базы данных, базы конфигураций, а также разнообразные базы данных истории в режиме реального времени. Если брандмауэр или система безопасности в базе данных не настроены должным образом, то опытный хакер может получить доступ к базе данных из бизнес-центра и генерировать SQL запросы, взяв под свой контроль сервер базы данных и сеть системы управления.



2.2.6. Утилиты связи для сетей партнеров

Партнеры и коллеги получают доступ к информации, находящейся в коммерческой сети или сети системы управления. С учетом ‘того, безопасность системы соответствует безопасности их самого слабого звена.



2.3. Как атакуют хакеры

В зависимости от мотивов и сложности процесса, злоумышленник может знать или не знать детали работы процесса. Например, если мотивом является простое нарушение работы процесса, при этом достаточно иметь поверхностные знания о процессе. Однако, если, злоумышленник хочет целенаправленно атаковать конкретный процесс, то ему необходима точная информации о работе всей системы.

Два наиболее уязвимых процесса:

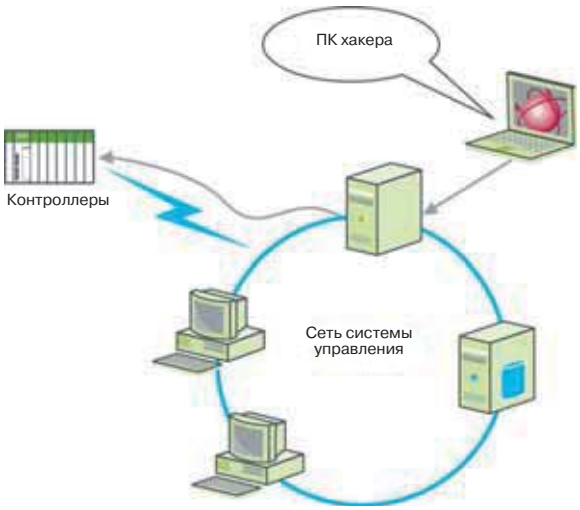
- сбор информации для базы данных;
- экраны ЧМИ/SCADA.

Название базы данных обычно различаются, но большинство пользователей используют общие принципы именования записей, различающихся, например, уникальным номером (т.е. pump1, breaker1,...). На уровне протокола обмена передается ссылка на номер (физический адрес). Для того чтобы осуществить атаку, злоумышленнику необходимо выяснить принцип формирования номеров.

Получение доступа к экранам ЧМИ является простейшим способом для получения этой информации. Экраны ЧМИ позволяют злоумышленнику перевести номера, передаваемые по сети, в значимую информацию.

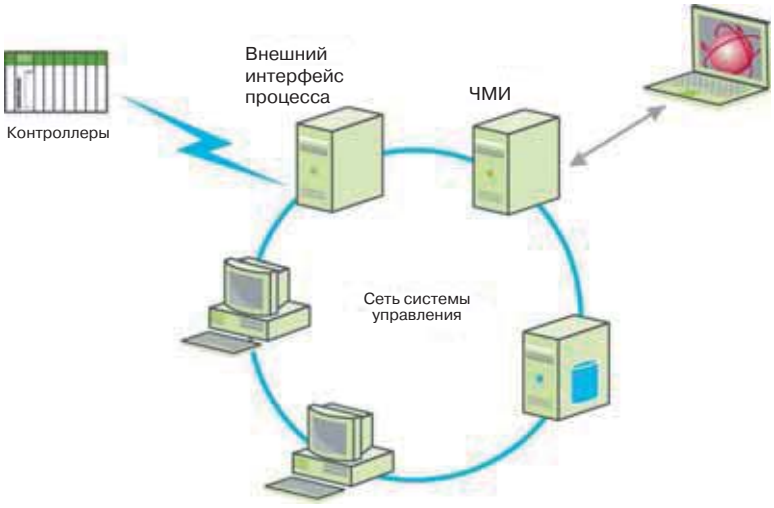
2.3.1. Управление процессом

Как только злоумышленник собирает достаточно информации о процессе, следующим его шагом является попытка управления процессом. Самым простым способом получения контроля над процессом для злоумышленника является подключение к устройству сбора данных, например к РАС (ЭВМ автоматизи-рованного управления технологическим процессом). Большинство ППК, шлюзов и серверов сбора данных не имеют в базовой конфигурации аутентификации и, поэтому обработают любые команды, отправленные в корректном формате.



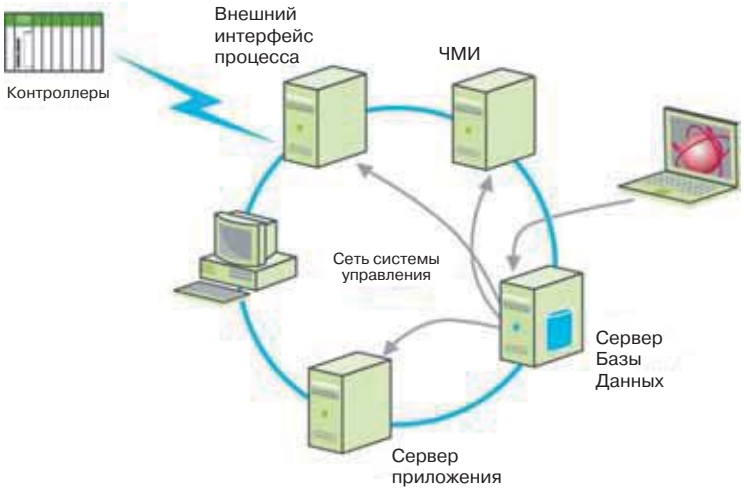
2.3.2. Экспорт экранов ЧМИ

Еще одним способом атаки является экспорт экранов ЧМИ к злоумышленнику для того, чтобы он мог получить контроль над системой. Опытные злоумышленники могут изменить экраны оператора с целью скрыть атаку. Злоумышленник, как правило, ограничивается набором команд, доступных для оператора, подключенного к системе.



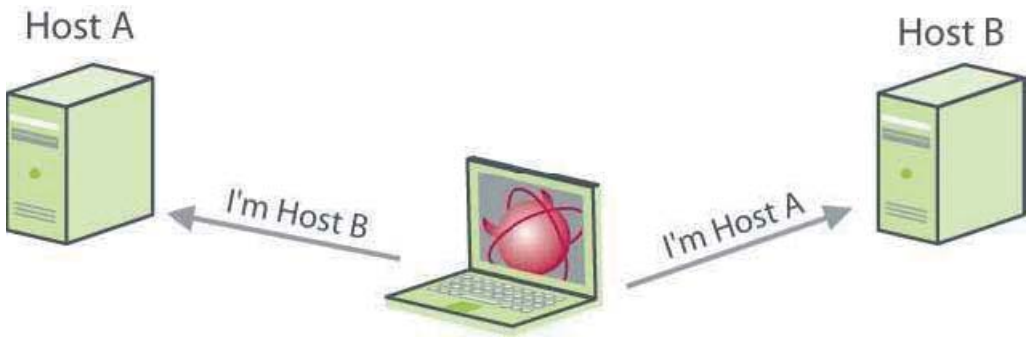
2.3.3. Изменение базы данных

Злоумышленник получает доступ к базе данных и модифицирует данные в ней с целью нарушить нормальное функционирование системы управления.

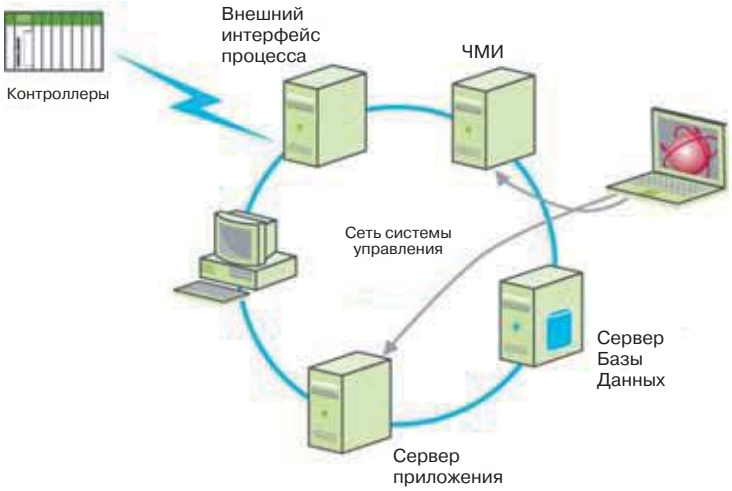


2.3.4. «Человек в цепи передачи данных»

«Человек в цепи передачи данных» является еще одним видом атаки, когда злоумышленник перехватывает сообщения с одного компьютера (хоста 1), изменяет данные до передачи на компьютер приемник (хост 2), а затем наоборот. Оба компьютера, как им кажется, говорят друг с другом и не знают о злоумышленнике.



Для того, чтобы злоумышленник преуспел в манипулировании пакетов протокола, он должен знать эти протоколы. «человек в цепи передачи данных» позволяет атакующему подделать экраны оператора ЧМИ и получить полный контроль над системой управления.



Ниже приводится детальное описание «человек в цепи передачи данных» из публикаций организации US-CERT (www.us-cert.gov):

Фаза	**Описание**
1	Изучение протокола передачи данных.
2	Используя протокол ARP, злоумышленник получает доступ к сети обмена информацией, сканируя кэш ARP, он получает адреса контроллеров и рабочих станций.
3	Используя зараженный компьютер в сети злоумышленник изменяет ARP таблицы на каждом компьютере и сообщает им, что они должны направить все свои сообщения на определенный физический адрес (например, адрес машины злоумышленника).
4	Изменяя ARP таблицы, злоумышленник может вставить свою машину между двумя абонентами и / или устройствами.
5	«Человек в цепи передачи данных» работает путем генерации фальшивых ARP таблиц на каждом узле (отравленные ARP). Эти таблицы ARP вынуждают передающие узлы использовать фальшивые физические адреса устройств в сети MAC– адреса /Media Access Control (управление доступом к среде)/. злоумышленника в качестве адреса получателя.
6	При успешной атаке в режиме «человек в цепи передачи данных», пользователи с каждой стороны не знают, что данные в сети передачи данных проходят по другому маршруту: через компьютер злоумышленника. При этом компьютер злоумышленника должен находиться в режиме синхронизации и не обрабатывать тайм-ауты.
7	После искажения таблиц ARP на обоих устройствах пакеты передаются в обоих направлениях по фальшивому пути. Это гарантирует, что все существующие приложения будут продолжать работать должным образом. При этом любой пакет в любое время может быть искажен на машине злоумышленника, для того чтобы передать определенные команды для каждого компьютера.
8	После того как злоумышленник успешно включил свой компьютер в информационный поток, он имеет полный контроль над передачей данных и может предпринять несколько типов атак.

Фаза	Описание
9	Как отмечалось ранее, одной атаки достаточно для нанесения вреда системе управления. В своей простейшей форме, перехваченные данные из системы управления или / ЧМИ могут быть использованы для создания вида деятельности или управления процессом со стороны злоумышленника для изготовления любой продукции от доброкачественной до вредоносной.
10	При проведении нападения злоумышленник пытается остаться незамеченным и удаляет все следы нападения, где это возможно. Принимая во внимание, что кибер-атаки на системы управления являются уникальными необходимо учитывать, что для их успешного осуществления требуется предоставлять оператору информацию, которую он ожидает увидеть.
11	Управление информацией, которая доступна оператору необходимо для того, чтобы скрыть атаку. На стадии подготовки атаки производится сбор данных отражающих нормальную работу системы управления, эти данные могут быть воспроизведены оператору по мере необходимости. Это гарантирует, что пульт оператора будет отражать нормальное состояние системы, и нападение пойдет незаметно.
12	Во время воспроизведения записи злоумышленник может продолжать разрушительную деятельность, посылая команды на контроллеры для того, чтобы вызвать нежелательные события, а оператор не заметит истинное состояние системы.
13	Еще одно нападение, которое может осуществляться по типу «Человек в цепи передачи данных» - это передача ложных сообщений оператору для того, чтобы стимулировать ложную управляющую команду от оператора. Этот режим может применяться, когда злоумышленнику сложно создать желаемое управляющее воздействие самостоятельно. Злоумышленник просто отправляет информацию о проблемах на пульт, а когда оператор пытается решить проблему, он сам посылает команды в систему управления и его действия приводят к нежелательным событием. Обычно существует множество параметров, изменение которых может повлиять на функционирование системы.

2.4. Насколько уязвимыми являются системы управления

«Североамериканская корпорация надежности энергосистем» /North American Electric Reliability Corporation/ (NERC) провела исследование по выявлению 10 наиболее часто встречающихся уязвимостей систем управления:

1. Исторически сложившаяся неадекватная политика по регулированию безопасности в системах управления:

- различие подходов к построению систем автоматизации с современными методами ИТ-безопасности;
- представители отделов ИТ часто не имеют понимания оперативных потребностей систем управления;
- отсутствие общей информированности и понимания риска, связанного с распространением сетевых технологий системах управления;
- отсутствие политики информационной безопасности систем управления;
- отсутствие аудита и применение требований по политикам информационной безопасности в системах управления;
- отсутствие адекватной оценки рисков.

2. Некорректно разработанные сети систем управления, в которых отсутствуют механизмы противодействия атакам злоумышленников:

- сетевая безопасность приборов систем управления ранее должным образом не учитывалась. Эти системы были разработаны с учетом высокой надежности и готовности, но не безопасности;
- системы управления не в состоянии обеспечить необходимый уровень безопасной работы в Интернет / Интранет без значительных инвестиций в технологии и инжиниринга.

3. Удаленный доступ к системе управления без надлежащего контроля доступа:

- ненадлежащее использование телефонных модемов;
- использование элементарного пароля или неиспользование паролей;
- осуществление незащищенного подключения сети системы управления к корпоративной локальной сети (LAN);
- практика открытия неконтролируемого доступа к сети продавца системы для осуществления поддержки.

4. Используемые в системах управления механизмы системного администрирования и программное обеспечение не исследуются или не обслуживаются достаточно тщательно:

- недостаточно качественное управление внесением исправлений (установка обновлений) в программное обеспечение;
- недостаточность действующей оперативной противовирусной защиты;
- недостатки управления учетными записями;
- недостаточный контроль изменений;
- недостатки ведения учета используемого программного обеспечения.

5. Использование для управления недостаточно защищенной беспроводной связи:

- применение широкораспространенных продуктов COTS (Commercial Off-The-Shelf) и устройств беспроводной связи массового потребления для управления сетевыми данными;
- использование устаревших или плохо зарекомендовавших себя методов обеспечения безопасности и кодирования информации.

6. Использование неспециализированного канала связи для управления и контроля и/или нецелесообразное использования полосы пропускания коммуникационной сети системы управления в целях, несвязанных с управлением:

- системы супервизорного управления и сбора данных, основанные на Интернет (Supervisory Control And Data Acquisition - SCADA).
- возможность подключения к Интернет/Интранет, инициируемая из сетей системы управления:
- совместное использование файлов;
- средства оперативной пересылки сообщений.

7. Недостаточно качественное применение инструментария для обнаружения и оповещения об аномальной или неуместной деятельности:

- недостаточно эффективное использование систем обнаружения вторжений;
- недостаточное управление системой безопасности сети;
- применение недостаточно отработанных систем предотвращения вторжений (Intrusion Prevention Systems - IPS).

8. Неавторизованные или несоответствующие приложения или устройства, подключаемые к сетям системы управления:

- неавторизованная установка дополнительного программного обеспечения на устройства системы управления;
- периферийные устройства, имеющие интерфейсы отличные от интерфейсов системы управления, например, многофункциональные или мультисетевые принтеры;
- незащищенные веб-интерфейсы для устройств системы управления;
- портативные компьютеры;
- карты памяти USB;
- другие портативные устройства, например персональный цифровой секретарь PDA (Personal Digital Assistant - PDA).

9. В системах управления нет подтверждения подлинности команд и контрольных данных:

- не реализована проверка подлинности команд передаваемых по локальным сетям;
- новые, недоработанные технологии подтверждения подлинности последовательной коммуникации с полевыми устройствами;
- недостаточность реализации безопасности, применяемой на объекте, если управление в системе производится с панелей управления.

10. Ненадлежащая организация, управление или работа инфраструктур поддержки в критических ситуациях:

- использование в системах ненадлежащих источников бесперебойного питания (UPS) или других источников питания;
- ненадлежащая работа или неисправность в системах теплоснабжения / вентиляции / кондиционирования воздуха (HVAC);
- слабое описание пограничной инфраструктуры;
- недостаточная защита телекоммуникационной инфраструктуры;
- ненадлежащая работа или неисправность в системах пожаротушения;
- отсутствие или недостатки плана восстановления работоспособности;
- недостаточное тестирование или обслуживание резервной инфраструктуры.

2.4.1. Типы уязвимостей

Национальный институт стандартов и технологий NIST (National Institute of Standards and Technology) опубликовал «Руководство по безопасности промышленных систем управления» (ПСУ), в котором приведено подробное описание уязвимых мест систем управления. Уязвимости распределены на три класса:

- уязвимость системной политики и процедур безопасности;
- уязвимость платформ;
- уязвимость сетей.

Приведенные далее разделы извлечены из «Руководства по безопасности промышленных систем управления».

Уязвимость системной политики и процедур безопасности

Кибер-безопасность – это комплекс процессов, который включает в себя системные политики, технические средства и программное обеспечение. Часто в применяемой системе безопасности системная политика не учитывается вообще или учитывается недостаточным образом, что может привести к уязвимости системы.

В таблице ниже приведено описание уязвимых мест системы, когда системные политики и процедуры безопасности не проработаны должным образом:

Уязвимость	Описание
Ненадлежащая политика безопасности для ПСУ	В ПСУ уязвимые места часто возникают по причине ненадлежащей политики или отсутствия специальной политики для защиты системы управления.
Отсутствие официальных мер обучения и информирования персонала по вопросам безопасности ПСУ	Официальные обучающие мероприятия по вопросам безопасности помогают информировать персонал о современных принципах построения политики безопасности и процедурах поддержания безопасности, а также о стандартах промышленной кибер-безопасности и о рекомендуемых правилах. Без таких обучающих мероприятий нельзя ожидать, что персонал сможет поддерживать безопасные условия работы ПСУ.
Недостаточная безопасность архитектуры и проекта	Исторически специалисты по системам управления имели минимальную подготовку по вопросам безопасности, до тех пор, пока в недавнее время производители не включили функции безопасности в свои продукты.
Нет специального или подтвержденного документами порядка действий по обеспечению безопасности, разработанного на основе системной политики для ПСУ	Для ПСУ необходимо разрабатывать специальный закрепленный в документации порядок действий по обеспечению безопасности, который должен быть изучен всем обслуживающим персоналом.
Отсутствие или недостаточность руководств по применению оборудования ПСУ	Руководства по применению оборудования должны соответствовать современным требованиям и быть легкодоступными. Принципы, изложенные в данных руководствах, являются неотъемлемой частью порядка действий персонала по обеспечению безопасности в случаях нарушения работоспособности ПСУ.
Недостаточность административных механизмов для обеспечения исполнения правил безопасности	Персонал, ответственный за выполнение правил безопасности, должен быть ответственным за выполнение документально подтвержденных системной политики и процедур по обеспечению безопасности.
Недостаточность или отсутствие аудита средств безопасности ПСУ	Независимая ревизия средств безопасности тщательно анализирует системные журналы и записи. На основании этого анализа подтверждается адекватность управления системой и соответствие установленной политики безопасности ПСУ и порядка действий персонала. Аудит также помогает обнаружить нарушения в организации служб безопасности ПСУ, и выдают рекомендации по изменениям в системе безопасности, которые помогут усилить существующую систему безопасности и/или добавить в нее новые аспекты безопасности.
Отсутствие специальной последовательности операций или плана восстановления после аварии DRP (Disaster Recovery Plan)	План восстановления DRP должен быть предварительно подготовлен и протестирован, а также он должен находиться в доступном месте в случае возникновения серьезной неисправности технических средств, сбой программного обеспечения или выход оборудования из строя. Отсутствие специального плана восстановления ПСУ может привести к увеличению времени простоя и потере продукции.
Отсутствие контроля изменений конфигурации ПСУ	Процесс внесения изменений в состав технических средств, программного обеспечения, встроенного программного обеспечения и документации должен производиться под контролем. Это необходимо для того, чтобы обеспечить защиту ПСУ от ненадлежащих или ошибочных изменений, которые могут быть произведены до ввода в эксплуатацию, в ходе внедрения или в процессе эксплуатации. Недостаточный контроль или его отсутствие может привести к появлению упущений, незащищенности или угроз в системе безопасности.

Уязвимости платформ

Современные промышленные системы управления часто состоят из сотен интеллектуальных устройств и должны работать круглосуточно все 365 дней в году. Многие конечные пользователи откладывают или избегают обновления систем в связи с неизбежными потерями, связанными с простоем, и потенциальным риском неудачного обновления. Большинство систем с человеко-машинным интерфейсом (ЧМИ) не имеет защитного антивирусного программного обеспечения, поскольку его базу необходимо часто обновлять, иначе оно неспособно оставаться современным и эффективным. Ранее платформы использовали собственные сетевые протоколы, которые должны были обеспечить безопасность и защитить от нападения, поскольку встроенные функции безопасности отсутствуют или незаконфигурированы.

Уязвимые места платформ можно разделить на следующие категории:

- уязвимость конфигурации платформы;
- уязвимость технических средств платформы;
- уязвимость программного обеспечения платформы;
- уязвимость защиты платформы от вредоносного ПО.

Уязвимость конфигурации платформы

Уязвимость	**Описание**
Обновления для операционных систем (ОС) или другого программного обеспечения не выпускаются до тех пор, пока не обнаруживается серьезное уязвимое место	По причине сложности ПО ПСУ и возможных модификаций основной ОС все изменения должны быть подвергнуты тщательному и всестороннему регрессивному тестированию. Время проведения подобного тестирования и последующего распространения обновленного программного обеспечения образует промежуток времени уязвимости системы.
Обновления для ОС и приложений безопасности не выпускаются	Устаревшие ОС и приложения могут иметь недавно обнаруженные уязвимые места. Необходимо разработать закрепленный документами порядок действий по поддержке обновлений функций безопасности. Если в ПСУ используются устаревшие ОС, то может отсутствовать возможность обновления функций безопасности.
Обновления функций безопасности ОС или приложения применяются без всестороннего тестирования	Применение обновлений для функций безопасности ОС или приложения без тестирования может повредить нормальной работе ПСУ. Необходимо разработать закрепленный документами порядок действий для тестирования свежих обновлений функций безопасности.
Применение конфигураций по умолчанию	Применение конфигураций по умолчанию часто приводит к небезопасным или ненужным действиям: открытию портов, запуску сервисных программ и приложений на хостах.
Необходимые конфигурации не сохраняются и не дублируются	Для того чтобы обеспечить работоспособность системы и предупредить потерю данных в случае нечаянного или злонамеренного изменения конфигурации, необходимо произвести ряд действий по восстановлению настроек конфигурации ПСУ. Должен быть разработан закрепленный документами порядок действий по поддержке настроек конфигурации ПСУ.

Уязвимость	Описание
Незащищенные данные на портативных устройствах	Если секретные данные (например, пароли, телефонные номера) хранятся в незашифрованном виде на портативных устройствах, например, портативных компьютерах и т.п., то в случае потери или кражи таких устройств безопасность системы может оказаться под угрозой. Политики, документация и оборудование нуждается в защите.
Отсутствие компетентной политики паролей	Если применяются пароли, то необходимо определить политику управления паролями, которая определяет сложность пароля и его обслуживание. Без надлежащей политики паролей в системе невозможно организовать надежный контроль и соответственно повышается вероятность несанкционированного доступа. Политика паролей должна разрабатываться как составная часть системы безопасности ПСУ с учетом технических характеристик ПСУ и способности персонала использовать сложные пароли.
Пароль вообще не применяется	Для предотвращения несанкционированного доступа в ПСУ необходимо применять пароли. Уязвимости в системе безопасности возникают при отсутствии паролей: ● для входа в систему (если в системе используются учетные записи пользователей); ● при включении системы (если в системе нет учетных записей пользователей); ● перехода в режим экранной заставки (если компоненты ПСУ работают без внимания оператора в течение некоторого времени). Процедура проверки пароля не должна затруднять или препятствовать действиям при аварийных ситуациях в ПСУ.
Раскрытие пароля	Для предотвращения несанкционированного доступа пароль должен держаться в секрете. Примеры раскрытия пароля: ● запись и размещение пароля в зоне видимости рядом с системой; ● совместное использование паролей несколькими индивидуальными учетными записями или пользователями; ● получение пароля злоумышленником через «социальный инжиниринг» (взломщик путём "уговоров" обманывает пользователей или администратора (например, представляясь новым сотрудником)); ● пересылка незашифрованных паролей через незащищенную связь.

Уязвимость	Описание
Использование легко угадываемого пароля	Неудачно выбранные пароли могут быть легко разгаданы компьютерным алгоритмом или человеком, стремящимся получить неавторизованный доступ. Примеры ненадежных паролей: ● Короткие и простые пароли (например, все строчные буквы), не отвечающие требованиям надежности. Надежность пароля также зависит от специальных возможностей ПСУ в части поддержания более сложных паролей. ● В качестве паролей используются значения, установленные по умолчанию производителем оборудования. ● Значение пароля не изменяется по истечении определенного интервала времени.
Применение ненадлежащего контроля доступа	Недостаточно продуманный контроль доступа может привести к тому, что пользователям ПСУ будет предоставлено слишком много или мало привилегий. Рассмотрим следующие примеры: ● В системе контроль доступа законфигурирован по умолчанию, при этом оператору предоставлены привилегии администратора. ● Некорректная конфигурация контроля доступа может привести к тому, что оператор не сможет произвести необходимые действия в случае аварийной ситуации. Политика контроля доступа должна разрабатываться как часть комплексной программы безопасности ПСУ.

Уязвимость платформ технических средств

Уязвимость	Описание
Ненадлежащее тестирование изменений в системе безопасности	Многие технические средства ПСУ, особенно небольшие устройства, не имеют собственных возможностей тестирования, поэтому изменения в системе безопасности должны применяться для реальной системы в целом.
Ненадлежащая физическая защита для критических систем	Доступ к центру управления, полевым устройствам, портативным устройствам, среде и другим компонентам ПСУ необходимо контролировать. Часто удаленные производственные участки не имеют обслуживающего персонала, поэтому нет возможности персонального контроля на месте.
Неавторизованный персонал имеет возможность физического доступа к оборудованию	Необходимо обеспечить ограничение физического доступа к оборудованию ПСУ. Только авторизованный обслуживающий персонал должен иметь доступ к оборудованию, учитывая требования безопасности системы, например, аварийное отключение или перезапуск. Некорректный доступ к оборудованию ПСУ может привести к описанным ниже последствиям:

Уязвимость	Описание
	o физическая кража данных и оборудования; o физическое повреждение или уничтожение данных или оборудования; o неавторизованные изменения функционирования системы (например, доступ к данным, неавторизованное использование мобильных средств, добавление/отключение ресурсов); o разъединение физических линий связи; o необнаруженный перехват данных (сочетание клавиш и регистрация входа в систему).
Небезопасный удаленный доступ к компонентам ПСУ	Модемы и другие устройства удаленного доступа, которые обеспечивают возможность управляющего персонала или производителей оборудования получить удаленный доступ к системе, должны использоваться под надлежащим контролем, чтобы предотвратить неавторизованный доступ к ПСУ.
Сдвоенная сетевая интерфейсная карта NIC (Network Interface Card) для подключения к двум сетям одновременно	Если в оборудовании применяются сдвоенные сетевые интерфейсные карты NIC для подключения к разным сетям, то в этом случае возможен неавторизованный доступ или передача данных из одной сети в другую.
Недокументированные ресурсы	Для обеспечения надежной защиты ПСУ, необходимо иметь точный список всех ресурсов системы. Ненадлежащее представление системы управления и ее компонентов оставляет неавторизованные точки доступа для входа в ПСУ.
Радиочастотная помеха и электромагнитный импульс (ЭМИ)	Технические средства систем управления чувствительны к радиочастотным помехам и электромагнитным импульсам (ЭМИ). Тяжесть последствий может изменяться от временного нарушения функций управления и контроля до разрушения электрических цепей печатных плат.
Отсутствие резервного источника питания	Если в системе отсутствует резервный источник питания для критических ресурсов, то при полном обесточивании все оборудование ПСУ будет отключено, что может привести к опасной ситуации. Потеря питания также может привести к возврату параметрам небезопасных значений по умолчанию.
Отсутствие контроля состояния окружающей среды	Отсутствие контроля состояния окружающей среды может привести к перегреву процессоров. При этом в целях самозащиты некоторые модели процессоров отключаются; некоторые могут продолжать работать в режиме минимальной производительности, выдавая ошибки; некоторые в случае перегрева разрушаются.
Отсутствие резервирования критических компонентов	Отсутствие резервирования критических компонентов может привести к выходу системы из строя в случае одиночного отказа.

Уязвимость платформы программного обеспечения

Уязвимость	Описание
Переполнение буфера	Программное обеспечение, используемое в ПСУ, может быть чувствительно к переполнению буфера; злоумышленники могут использовать это уязвимое место для разнообразных атак.
Установленные функции безопасности по умолчанию недоступны	Функции безопасности, установленные вместе с продуктом, являются бесполезными, если они не активизированы или заблокированы.
Отказ в обслуживании (Denial of service - DoS)	Программное обеспечение ПСУ может стать уязвимым в случае отказа в обслуживании (DoS-атаки), что может привести к предотвращению авторизованного доступа к системным ресурсам или задержкам в работе системы.
Неправильное управление в неопределенных, нечетко определенных или «недопустимых» режимах	Приложения некоторых ПСУ чувствительны к содержанию пакетов данных, которые могут быть сформированы с ошибками, а также содержать некорректные или неописанные поля данных.
OPC (OLE для управления процессами (OLE for Process Control – OPC)) базируется на RPC – Удаленном Вызове Процедур (Remote Procedure Call - RPC) и DCOM – Распределенной Модели Компонентных Объектов (Distributed Component Object Model - DCOM)	Без своевременного обновления, у OPC имеются в наличии все известные уязвимости RPC/DCOM.
Использование незащищенных широко применяемых в промышленности протоколов ПСУ	Распределенный Сетевой Протокол DNP 3.0 (Distributed Network Protocol - DNP), Modbus, Profibus и другие протоколы являются открытыми и часто используются в промышленности. Данные протоколы часто имеют ограниченные встроенные функции безопасности, или не имеют их вообще.
Использование незакодированного текста	Многие протоколы ПСУ передают незакодированные данные по среде передачи данных, что значительно упрощает прослушивание сообщений злоумышленниками.
Постоянная работа редко используемых или ненужных сервисных служб	Многие платформы предлагают разнообразные типы процессоров и сетевых сервисов, которые по умолчанию работают. Ненужные сервисные программы редко блокируются и могут быть использованы.
Использование запатентованного программного обеспечения, которое обсуждалось на конференциях и в периодических изданиях	Выход запатентованного программного обеспечения обсуждается на международных IT (Information Technology - информационные технологии) и ПСУ конференциях и форумах хакеров “Black Hat”, а также в технических и периодических изданиях и Интернет-рассылках. Кроме того, руководства по обслуживанию ПСУ можно получить у продавцов. Эта информация может помочь злоумышленникам осуществлять успешные нападения на ПСУ.

Уязвимость	**Описание**
Неадекватная аутентификация и контроль доступа к ПО конфигурирования и программирования	Неавторизованный доступ к ПО конфигурирования и программирования может повредить устройство.
Не установлено программное обеспечение обнаружения/ предотвращения вторжений	Вторжение может привести к потере работоспособности системы, краже, модификации и удалению данных, неправильному выполнению команд управления. Программное обеспечение обнаружения/предотвращения вторжений может остановить или предотвратить различные типы нападений, включая нападения DoS, а также идентифицировать подвергшиеся нападению внутренние хосты, в том числе зараженные саморазмножающимися вирусами. Программное обеспечение обнаружения/предотвращения должно быть проверено до применения, чтобы убедиться, что оно не ставит под угрозу нормальную операцию ПСУ.
Журнал регистрации событий не ведется	Если не ведется тщательной и точной регистрации событий, то может быть очень трудно, а иногда и невозможно определить причину сбоя в системе безопасности.
Не обнаруженные события	Если в системе установлены датчики безопасности и ведется журнал регистрации событий, то состояние датчиков и содержание журнала можно просмотреть в реальном времени и поэтому событие в системе безопасности можно быстро обнаружить и отреагировать.

Уязвимость защиты платформы от вредоносного ПО

Уязвимость	Описание
Программное обеспечение защиты от вредоносного ПО не установлено	Вредоносное ПО может привести к снижению производительности, потере работоспособности системы, краже, модификации или удалению данных. Защитное ПО, например, антивирусные программы, необходимо использовать для предотвращения инфицирования системы вредоносными программами.
Устаревшее программное обеспечение защиты от вредоносного ПО	Устаревшее защитное ПО оставляет систему уязвимой для нового вредоносного ПО.
Защитное ПО применяется без надлежащего тестирования	Использование защитного ПО без надлежащего тестирования может оказать сильное влияние на нормальную работу ПСУ.

Уязвимости в коммуникационных сетях

Уязвимости в коммуникационных сетях обычно возникают вследствие недоработок при проектировании, недостаточного технического обслуживания сетей, а также при недостаточном понимании сетевых требований. Во многих приложениях проектированием коммуникаций по сетям занимаются два отдела: отдел IT и отдел управления процессами. Если каждый из отделов не знаком с требованиями другого, это может привести к уязвимости коммуникационной сети.

Различия между IT и ПСУ:

Категория	**Система IT**	**ПСУ**
Управление рисками	Конфиденциальность и целостность данных очень важна. Отказоустойчивость менее важна – кратковременный простой не является главным риском. Главный риск – это задержка деловых операций.	Важнейшей целью является безопасность человека и защита процесса. Отказоустойчивость тоже очень важна, даже кратковременный простой может быть неприемлем. Главные риски – это потеря управления, воздействия на окружающую среду, человеческие жертвы, утрата оборудования или продукции.
Безопасность архитектуры	Основное внимание уделяется защите ресурсов IT и информации, которая хранится в них или передается между этими ресурсами. Центральному серверу требуется усиленная защита.	Основной целью является защита конечных клиентов (например, полевых устройств, таких как контроллеры управления процессом). Защита центрального сервера очень важна.
Результаты	Решения по безопасности разрабатываются для типовых систем IT.	Средства безопасности должны быть протестированы (например, в отключенном режиме на аналогичной ПСУ) для того, чтобы убедиться, что они не препятствуют нормальной работе ПСУ.
Взаимодействие, критическое по времени	Менее критичное чрезвычайное взаимодействие. Сильно ограниченное управление доступом может быть применено в степени, необходимой для безопасности.	Ответная реакция человека и других чрезвычайных взаимодействий является критической. Доступ к ПСУ должен жестко контролироваться, но не должен вредить или мешать взаимодействию человек-машина.
Функционирование системы	Системы разрабатываются для типовых применений.	Нестандартные и патентованные программные продукты часто не имеют встроенных функций безопасности.

Категория	Система IT	ПСУ
	Обновления осуществляются напрямую, с возможностью применения автоматизированных инструментов ввода в эксплуатацию.	Изменения ПО должны производиться осторожно лучше продавцами ПО, из-за специализированных алгоритмов управления и возможного изменения аппаратных средств и вовлеченного ПО.
Ограниченность ресурсов	Системы обычно спроектированы с достаточным объемом ресурсов, чтобы обеспечить выполнение дополнительного ПО приложений третьих компаний, например, приложений безопасности.	Системы спроектированы, чтобы поддержать намеченный производственный процесс и, возможно, не имеют достаточного объема памяти и вычислительных ресурсов, чтобы поддержать дополнительные функции безопасности.
Коммуникация	Стандартные коммуникационные протоколы. В основном проводные сети, возможно с небольшим количеством беспроводных устройств. Типичные сетевые методы IT.	Множество патентованных и стандартных коммуникационных протоколов. Несколько типов коммуникационных сред, включая проводные и беспроводные (радио и спутниковая связь). Сети являются сложными и иногда требуют экспертизы технических специалистов.
Управление изменениями	Изменения ПО производятся своевременно в сопровождении качественной политики и процедур безопасности. Процедуры часто автоматизируются.	Изменения ПО должны быть полностью проверены и развернуты с приращением ресурсов системы в целом, чтобы гарантировать, что сохранена целостность системы управления. Отключения системы должны быть заранее запланированы на конкретные дни/недели. ПСУ может использовать операционные системы, которые больше не поддерживаются.
Управляемая поддержка	Допускаются разнообразные стили поддержки.	Техническая поддержка осуществляется поставщиком оборудования.
Срок службы компонентов	Срок службы 3-5 лет.	Срок службы 15-20 лет.
Доступность компонентов	Компоненты обычно размещены локально и они легкодоступны.	Компоненты могут быть изолированными, удаленными, и доступ к ним может быть затруднен.

Уязвимости в сетях можно разделить на следующие категории:

- уязвимость сетевой конфигурации;
- уязвимость сетевых аппаратных средств;
- уязвимость сетевого периметра;
- уязвимость сетевого мониторинга и журнала регистрации;
- уязвимость коммуникации;
- уязвимость беспроводного подключения.

Уязвимость сетевой конфигурации

Уязвимость	**Описание**
Недостаточная безопасность сетевой архитектуры	Сетевая инфраструктура в пределах ПСУ часто разрабатывается и изменяется на основе деловые и рабочих требований с некоторым учетом потенциальных угроз безопасности от этих изменений. В течение некоторого времени, в системе безопасности сетевой структуры могут пробелы. Без надлежащих исправлений, эти пробелы могут предоставить злоумышленникам «черный ход» в ПСУ.
Не используется контроль потоков данных	Контроль потоков данных, например, списки контроля доступа ACL (Access Control List), необходим для того, чтобы четко описать какие системы могут получать прямой доступ к другим устройствам сети. Как правило, только назначенные сетевые администраторы могут получить прямой доступ к таким устройствам. Контроль потоков данных должен обеспечить невозможность несанкционированного прямого доступа других систем к сетевым устройствам.
Недостаточным образом законфигурировано оборудование безопасности	Использование в конфигурации значений по умолчанию часто приводит к опасному и ненужному открытию портов и запуску сетевых служб, выполняющихся на хостах, которые могут быть использованы. Ненадлежащим образом законфигурированные брандмауэры и маршрутизаторы ACL могут допустить ненужный трафик.
Не выполняется сохранения или резервного копирования конфигурации сетевых устройств	Чтобы обеспечить работоспособность системы и предотвратить потерю данных в случае нечаянных или злонамеренных изменений в конфигурации, должны быть доступны процедуры восстановления сетевых параметров настройки конфигурации устройств. Необходимо разработать документированные процедуры по поддержке сетевых параметров настройки конфигурации устройств.
Пароли при передаче не шифруются	Если пароли передаются открытым текстом по передающей среде, то они могут быть перехвачены злоумышленниками, которые могут использовать их для получения авторизованного доступа к устройствам сети. Такой доступ позволит злоумышленнику нарушить работу ПСУ или проследить за обменами информацией по сетям ПСУ.

Уязвимость	Описание
Пароль действителен в течение неограниченного времени	Необходимо регулярно изменять пароли для того, чтобы даже если один из них стал известен неавторизованному лицу, то это лицо смогло бы получить доступ к устройству сети только на короткий промежуток времени. Хотя даже такой доступ позволит злоумышленнику нарушить работу ПСУ или проследить за обменами информацией по сетям ПСУ.
Применение ненадлежащего контроля доступа	Неавторизованный доступ к устройствам сети и функциям администратора позволит злоумышленнику нарушить работу ПСУ или проследить за обменами информацией по сетям ПСУ.

Уязвимость сетевых аппаратных средств

Уязвимость	Описание
Ненадлежащая физическая защита сетевого оборудования	Для предотвращения повреждений или разрушения необходимо контролировать доступ к сетевому оборудованию.
Незащищенные физические порты	К незащищенным универсальным последовательным шинам и портам (USB) или PS/2 можно произвести несанкционированное подключение портативного компьютерного жесткого диска, карты памяти данных, регистратора работы клавиатуры и т.д.
Потеря контроля параметров окружающей среды	Потеря контроля параметров окружающей среды может привести к перегреву процессора. При этом в целях самозащиты некоторые модели процессоров отключаются; некоторые могут продолжать работать в режиме минимальной производительности, выдавая ошибки; некоторые в случае перегрева разрушаются.
Доступ к оборудованию и сетевым средствам коммуникации имеет не только персонал, осуществляющий аварийный ремонт и техническое обслуживание	Возможность физического доступа к сетевому оборудованию должна быть крайне ограниченной и предоставляться только специальному персоналу, осуществляющему ремонт и техническое обслуживание. Несанкционированный доступ к сетевому оборудованию может иметь следующие последствия: ● кража данных или оборудования; ● физическое повреждение или разрушение данных или оборудования; ● неавторизованные изменения в системе безопасности (например, изменения в списках ACL, чтобы подготовить проникновение в сеть). ● неавторизованное прослушивание и манипулирование деятельностью сети; ● отключение физических линий связи или подключение неавторизованных линий связи.
Отсутствие резервирования критических сетей	Отсутствие резервирования критических сетей может вызвать выход системы из строя в случае единичного отказа.

Уязвимость сетевого периметра

Уязвимость	Описание
Не определен периметр безопасности	Если сеть системы управления не имеет явно определенного периметра безопасности, то нельзя гарантировать, что необходимые управления безопасности развернуты и конфигурированы должным образом. Это может привести к неправомочному доступу к системам и данным, так же как другим проблемам.
Брандмауэр не применяется или ненадлежащим образом законфигурирован	В случае отсутствия должным образом законфигурированного брандмауэра, в системе может быть допущена передача ненужных данных между сетями, например между сетью управления и корпоративной сетью. Из-за этого могут возникнуть различные проблемы, в том числе предоставление возможности атаки, распространение вредоносного ПО в сетях, отслеживание и прослушивание данных по другим сетям, возможность неавторизованного доступа в системы.
Сети управления используются для трафика, не связанного с управлением	Трафик управления и трафик, несвязанный с управлением, имеют различные требования, например, по детерминизму и достоверности данных. Если по одной сети передаются оба типа трафиков, то значительно затрудняется конфигурирование сети, чтобы она отвечала требованиям трафика управления. Например, трафик, несвязанный с управлением, случайно, может занимать ресурсы, необходимые для трафика управления, вызывая нарушения функционирования ПСУ.
Сетевые сервисы вне сети управления	Когда в системах используются сервисы IT, такие как DNS (Domain Name System - служба имён доменов) и/или DHCP (Dynamic Host Configuration Protocol - протокол динамического конфигурирования хоста), они часто применяются в сети IT. При этом сеть ПСУ зависит от сети IT, которая в свою очередь может не отвечать требованиям надежности и готовности, предъявляемым к ПСУ.

Уязвимость сетевого мониторинга и журнала регистрации

Уязвимость	Описание
Ненадлежащая регистрация событий брандмауэра или маршрутизатора	Без качественной и точной регистрации часто крайне трудно определить причину инцидента в системе безопасности.
Отсутствие мониторинга безопасности в сети ПСУ	Без регулярного мониторинга безопасности, инциденты могут остаться незамеченными, что может привести к дополнительному повреждению и/или разрушению. Регулярный мониторинг безопасности также необходим для идентификации проблем безопасности, таких как ошибки конфигурации и сбои.

Уязвимость коммуникации

Уязвимость	Описание
Не определен мониторинг критических ситуаций и путей управления	Неконтролируемое и/или неизвестное подключение к ПСУ может предоставить для атаки «черный ход» в систему.
Стандартные, хорошо документированные коммуникационные протоколы используются в явном, нешифрованном виде	Злоумышленники могут отслеживать сетевую активность ПСУ, используя анализатор протоколов или другие утилиты декодирования передаваемых данных по протоколам, таким как протокол эмуляции терминала Telnet, протокол передачи файлов FTP (File Transfer Protocol) или система NFS (Network File System - сетевая файловая система). Использование таких протоколов значительно упрощает реализацию атак на ПСУ и манипуляцию сетевой активностью злоумышленниками.
Аутентификация пользователей, данных или устройств нестандартна или не применяется	Многие протоколы ПСУ не применяют процедуру аутентификации. При этом существует опасность повторной передачи, модификации данных, выдача ложной информации от устройств.
Отсутствие проверки достоверности коммуникации	Большинство промышленных протоколов не имеют встроенной проверки достоверности данных. В данном случае злоумышленники могут незаметно манипулировать сетевой активностью. Чтобы обеспечить достоверность данных, в ПСУ можно использовать протоколы нижнего уровня (например, IPsec), которые обеспечивают проверку достоверности данных.

Уязвимость беспроводного подключения

Уязвимость	**Описание**
Неадекватная аутентификация клиента и точек доступа	Строгая взаимная аутентификация беспроводных клиентов и точек доступа необходима для обеспечения того, что клиенты не подключаются через неконтролируемую точку доступа, созданную злоумышленниками, и того, что злоумышленники не соединяются ни с одной из беспроводных сетей ПСУ.
Ненадлежащая защита данных между клиентами и точками доступа	Необходимо обеспечить защиту уязвимых данных в промежутке между беспроводным клиентом и точкой доступа с помощью устойчивого шифрованию, чтобы обеспечить невозможность неавторизованного доступа злоумышленников к незакодированным данным.

3. Реализация принципов кибер-безопасности в оборудовании Schneider Electric

Schneider Electric рекомендует подход "глубокая защита". Глубокая защита использует несколько методов обеспечения безопасности, чтобы помочь снизить риск. Нет единого решения, которое может обеспечить адекватную защиту от компьютерных атак на сети системы управления.

Подход «глубокой защиты» рассматривает шесть слоев обороны в сети PlantStruxure:

1. План безопасности
Создание плана обеспечения безопасности является первым шагом к построению безопасной сети системы управления.
Политики и процедуры должны быть определены, реализованы и, самое главное: должны обновляться и поддерживаться. Процесс планирования включает в себя проведение оценки уязвимости, снижения рисков и создания плана по сокращению или избеганию этих рисков.

2. Разделение сетей
Физическое отделение сети системы управления от других сетей, включая полное разделение сетей на предприятии.

3. Периметр защиты
Периметр защиты обеспечивает защиту сети системы управления от несанкционированного доступа с помощью брандмауэра, проверки подлинности и авторизации, VPN (IPsec) и антивирусного программного обеспечения. Удаленный доступ входит в периметр защиты.

4. Сегментация сети
Сегментация сети VLAN осуществляется с использованием разделителей сети на подсети для обеспечения дополнительной безопасности и поддержания безопасности каждого сегмента.

5. "Повышение защищенности устройств"
"Повышение защищенности устройств" - это процесс повышения безопасности путем конфигурирования устройств. Подразумевается установка паролей и контроля доступа, а так же запрещение всех не используемых протоколов и сервисов.

6. Мониторинг сети
Не существует сети, защищенной на 100%, из-за постоянной эволюции новых угроз. Требуется обеспечить постоянный мониторинг сети системы управления для того, чтобы своевременно блокировать злоумышленников до нанесения повреждения.

3.1. План безопасности

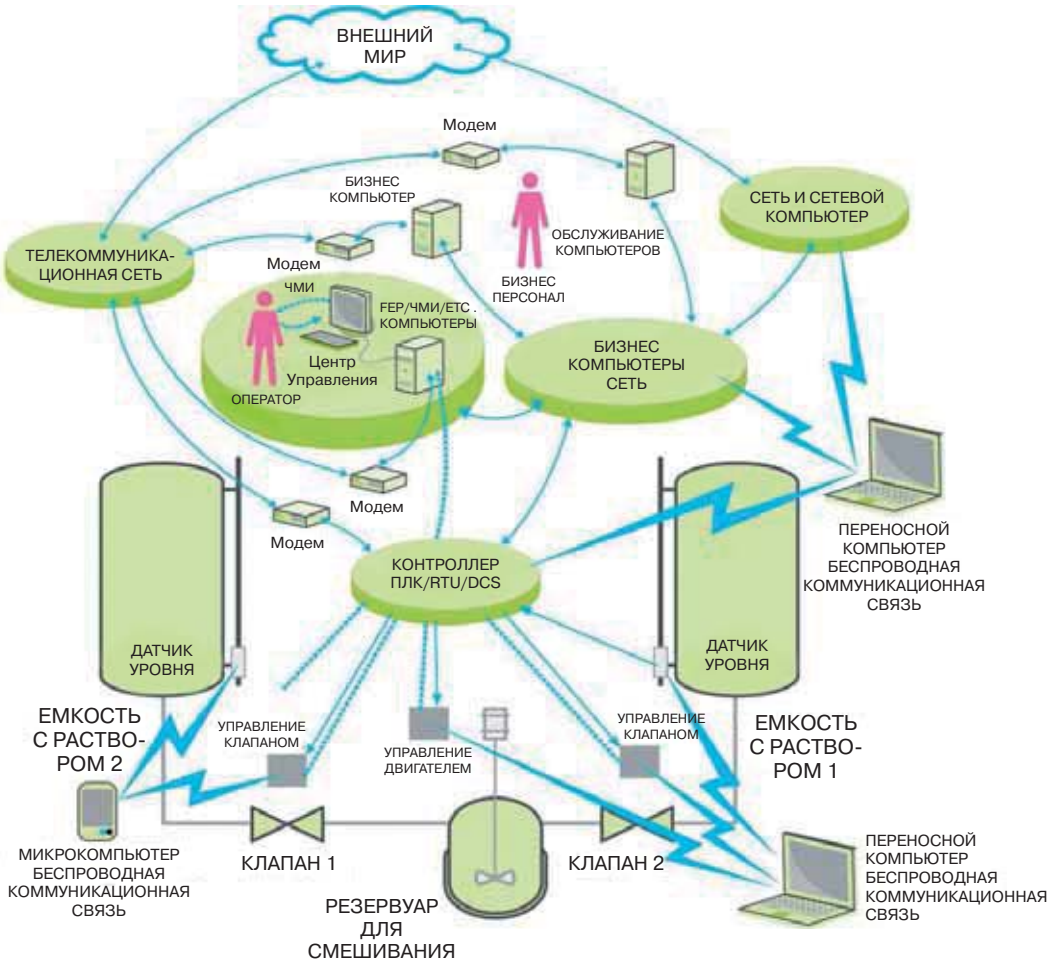
Первый шаг к защищенной сети состоит в создании плана обеспечения безопасности с процедурами и политикой. Для создания всеобъемлющего плана обеспечения безопасности должна быть создана многофункциональная рабочая группа, состоящая из менеджеров, IT-персонала, инженеров систем управления, операторов и экспертов по вопросам безопасности.

План обеспечения безопасности должен четко определять:

- роли и обязанности лиц, которых описывает политика;
- действия и процессы, разрешенные и запрещенные;
- действия при несоблюдении.

Для уже существующих сетей до создания плана по обеспечению безопасности требуется произвести полномерную оценку ситуации:

- определить каналы связи в сеть системы управления и из неё;
- определить каналы связи внутри сети системы управления;
- выполнить полный аудит устройств в сети;
- записать параметры безопасности каждого устройства;
- начертить подробную схему сети.



После разработки структурной схемы системы необходимо провести окончательный анализ уязвимости системы, чтобы выявить слабые места, потенциальные угрозы и происхождение угроз.

Оценивая уязвимость системы, необходимо выявлять:

- наиболее вероятные угрозы;
- наиболее вероятные бизнес-последствия;
- наиболее уязвимые бизнес-процессы;
- оценку ежегодного влияния на бизнес.

Риск = % Вероятность угрозы нападения * % Вероятность использования уязвимого места * Разумно предсказуемые (финансовые) последствия

«Введение в информационную безопасность», Дэйв Нортон, руководитель программы CISSP, «Передача данных и IT-безопасность в энергетике» – Новый Орлеан

План должен состоять из:

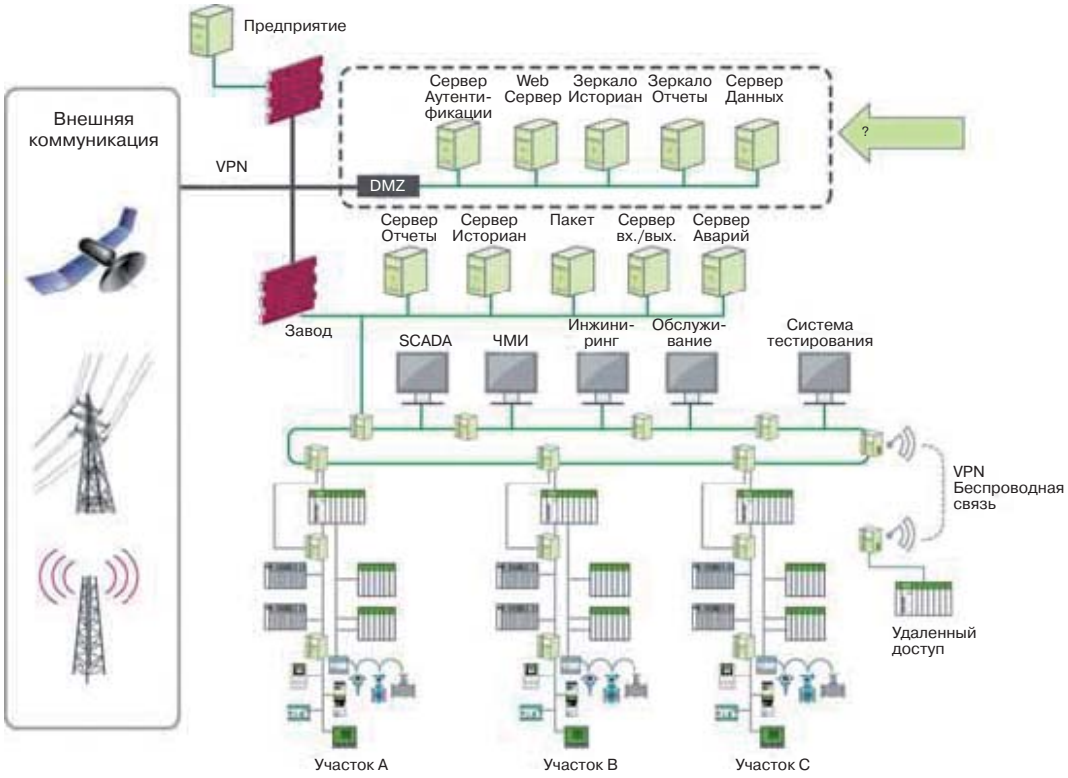
- Политики безопасности - Политики безопасности должны быть разработаны для сети системы управления и ее отдельных компонентов. Политика должны периодически пересматриваться, чтобы учитывать изменения в угрозах, изменения в структурах системы и обеспечение достаточного уровня безопасности.
- Блокирование доступа к ресурсам и услугам - Защита периметра с помощью брандмауэров или прокси-серверы, системы контроля доступа и антивирусное программное обеспечение.
- Обнаружение вредоносной активности - обнаружения вторжений, такие как мониторинг и аудит журналов событий необходимо для выявления проблем в сети.
- Смягчение возможных атак - Более безопасные сети оказывают большие задержки передачи данных. Для того чтобы процесс правильно запустить, может потребоваться знания уровня уязвимости.
- Исправление основных выявленных проблем - Исправление обнаруженных проблем обычно включает в себя обновление, модернизацию или исправление уязвимости или удаление уязвимого приложения.

3.2. Разделение Сетей

Одним из важных элементов проектирования сети системы управления является физическое разделение между управляющей сетью и внешними коммуникациями. Доступ к данным между Интернет, корпоративными системами и сетями управления должен осуществляться на серверах, расположенных в безопасной зоне (DeMilitarized Zone - DMZ). Безопасная зона (DMZ) обеспечивает безопасный и надежный способ обмена данными между устройствами разных зон. Безопасная зона (DMZ) должна содержать:

- серверы данных, например, Citect Historian, которые собирают данные из систем управления и распространяют их внутри предприятия;
- управление обновлениями программного обеспечения;
- сервера антивирусного программного обеспечения;
- сервер веб-доступа;
- точка беспроводного доступа;
- удаленный доступ.

Все коммуникационные линии связи заканчиваются в DMZ. Там не должно быть какого-либо прямого соединения с промышленной сетью управления.



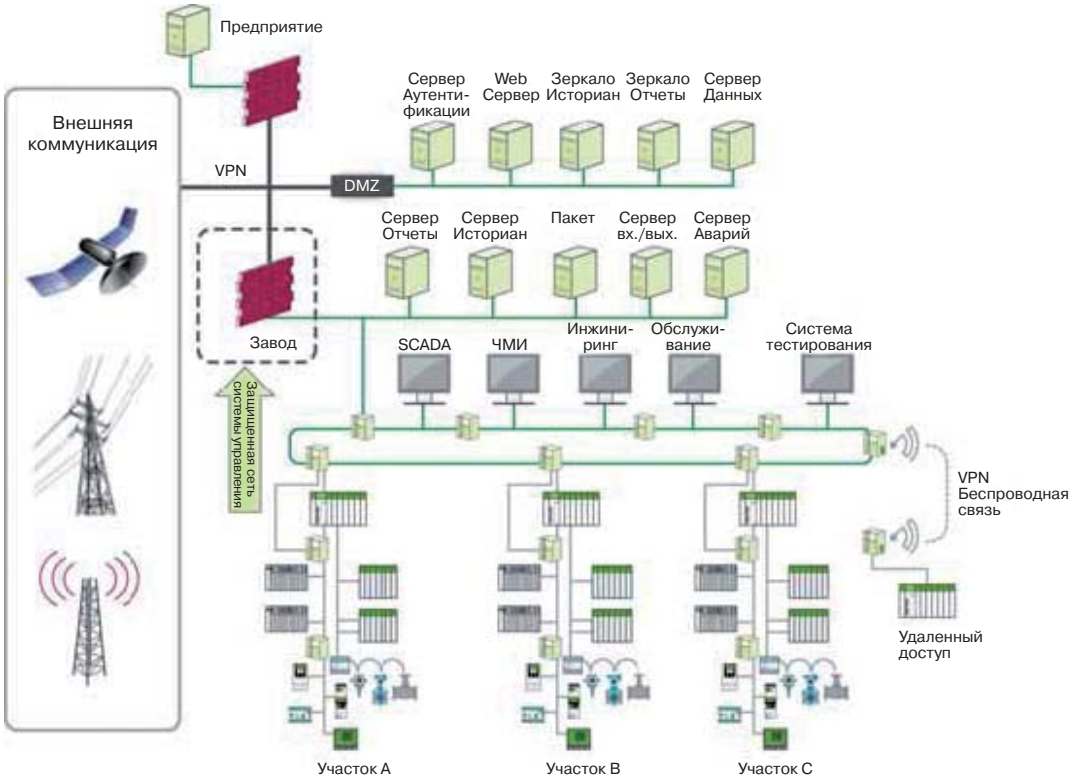
3.2.1. Рекомендации по безопасной зоне (DMZ)

- Все пересылки должны заканчиваться на серверах в DMZ.
- Входящий трафик в систему управления должен быть заблокирован. Доступ к устройствам внутри системы управления должен проводится через DMZ.
- Исходящий трафик через брандмауэр системы управления должен быть ограничен только особо важными пересылками.
- Весь исходящий трафик из сети системы управления в корпоративную сеть должен быть ограничен портом и сервисом источника и приемника.
- Брандмауэр должен быть настроен на фильтрацию исходящего трафика, чтобы остановить фальшивые IP-пакеты при выходе из сети системы управления или DMZ.
- Брандмауэры должны быть настроены на пересылку IP-пакетов, только если эти пакеты имеют корректный IP-адрес источника для сети управления и DMZ сети.
- Настоятельно не рекомендуется открывать доступ в Интернет из устройств систем управления.
- Серверы в зоне DMZ должны иметь жесткую логику. Обновления системы безопасности и антивирусного программного обеспечения должны производится периодически.

3.3. Защита периметра

Межсетевые экраны (брандмауэры) используются для защиты периметра сети, блокируя неавторизованный доступ, разрешая только авторизованные связи. Это устройство (или набор устройств) настроено на разрешение, запрещение, шифрование, дешифрование или пересылку через прокси-сервер всего (входящего и исходящего) трафика между различными доменами безопасности, основанной на наборе правил и других критериев.

Брандмауэры играют важную роль в сети системы управления. Устройства управления процессами требуют быстрой передачи данных и, следовательно, непозволительно вносить задержки, вызванные проверкой стратегии безопасности. Система управления в значительной мере опирается на защиту периметра, позволяющую блокировать все нежелательные и несанкционированные пересылки в сети.



Существует три категории брандмауэров:

- Фильтрация пакетов: основной тип брандмауэров низкой стоимости с минимальным воздействием на производительность сети. Основные данные в каждом пакете, например, IP адреса проверяется до отправления. Не рекомендуются к использованию из-за отсутствия проверки подлинности передаваемых данных, не скрывают архитектуры охраняемых сетей …
- Применение прокси-шлюза – прокси-шлюз анализирует пакеты на уровне приложений и фильтрует трафик на основе определенных правил приложений, таких как специальные программы (например, браузеры) или протоколы (например, FTP). Применение прокси-шлюзы обеспечивает высокий уровень безопасности, но может иметь накладные расходы и задержки, влияющих на производительность сети системы управления, поэтому часто не рекомендуются для применения.
- Брандмауэры Stateful Inspection - Stateful Inspection представляет собой многослойные брандмауэры, сочетающие в себе возможности, указанных выше брандмауэров. Фильтрации пакетов в Stateful Inspection на сетевом уровне, подтверждает, что сессии пакетов и содержимое пакетов на прикладном уровне, являются законными. Применение Stateful Inspection обеспечивает режим работы, при котором все входящие пакеты являются результатом исходящего запроса. И хотя брандмауэры Stateful Inspection дорого стоят и сложны в настройке, они обеспечивают высокий уровень производительности и безопасности.

3.3.1. Рекомендации по брандмауэрам.

Национальный институт стандартов и технологий сформулировал следующие рекомендации:

- основное правило: отвергать все и ничего не разрешать;
- порты и сервисы для обмена данными между сетями сетей управления и корпоративной сетью должен быть открыты и разрешены после рассмотрения каждого конкретного случая по отдельности. Необходимо произвести документальное обоснование, содержащее анализ рисков, и назначить человека ответственного, за каждый разрешенный входящий или исходящий поток данных;
- все "разрешения" должны иметь конкретные IP-адреса и номера портов TCP / UDP;
- все правила должны ограничивать трафик на определенный IP-адрес или диапазон адресов;

- транзитная передача данных из сети системы управления в корпоративную сеть должна быть блокирована. Все пересылки должны заканчиваться в DMZ;
- любой протокол, разрешенный между сетью системы управления и DMZ, не должен быть разрешен между DMZ и корпоративной сетью (и наоборот);
- весь исходящий трафик из сети системы управления в корпоративную сеть должен быть описан по источникам передачи и иметь конкретного получателя с указанием используемого сервиса и сетевого порта;
- исходящие пакеты из сети системы управления или DMZ могут быть разрешены, только если эти пакеты имеют правильный IP-адрес источника, назначенного в сети системы управления или DMZ устройств;
- устройства из сети системы управления не должны иметь разрешенный доступ к Интернет;
- сети систем управления не должны напрямую подключаться к Интернету, даже через канал связи, защищенный с помощью брандмауэра.

3.3.2. Уязвимости брандмауэров.

Отказ в обслуживании или атаки DOS является одним из самых популярных уязвимостей по внешнему периметру.

- Другие общие случаи уязвимостей:
- spoofing (подмена);
- черви и трояны;
- вирусы;
- грабеж;
- подделка идентификационных данных;
- подделка данных/сетей.

Эти атаки на сети систем управления могут привести к:

- сокращение или остановка производства в одном месте или на нескольких объектах одновременно;
- травмы или смерть сотрудников;
- массовые травмы или смерть среди населения;
- повреждение оборудования;
- исчезновение, утечка или кража опасных материалов;
- угроза национальной безопасности;
- экологический ущерб;
- нарушение нормативных требований;
- загрязнения продукта;
- нарушение уголовной или гражданско-правовых обязательств;
- потеря служебной или конфиденциальной информации;
- потеря имиджа бренда или доверия клиентов.

3.3.3. Снижение рисков брандмауэра

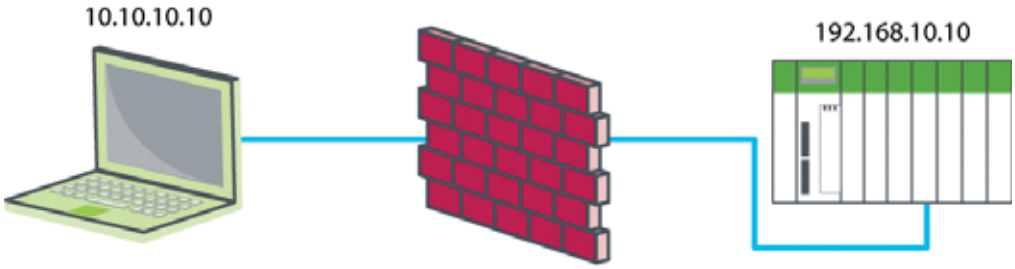
Фильтрация пакетов

Для устройств сети системы управления необходимо организовать систему безопасности, основанную на уникальных приложениях и протоколах. Пакетная фильтрация - это характерная особенность брандмауэров, которые обеспечивают защиту, основываясь на:

- IP-протокол;
- IP-адрес Источника;
- порт источника;

- IP-адреса получателя;
- порт получателя.

С помощью фильтрации пакетов, доступ к устройству может быть разрешен, и в то же время набор протоколов ограничен.

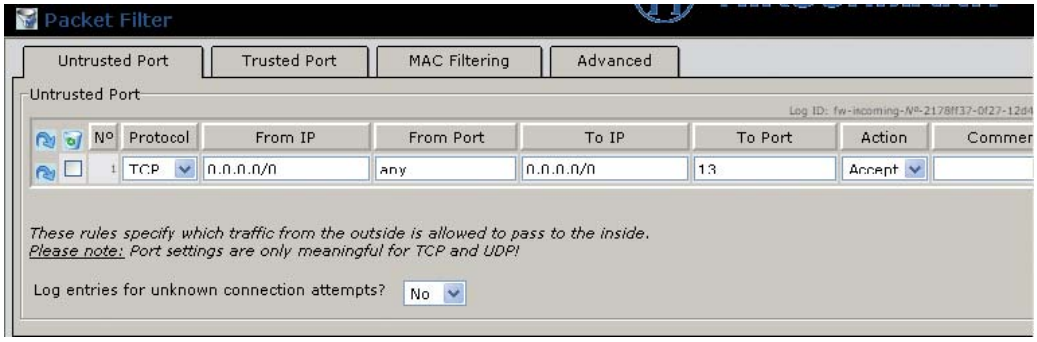


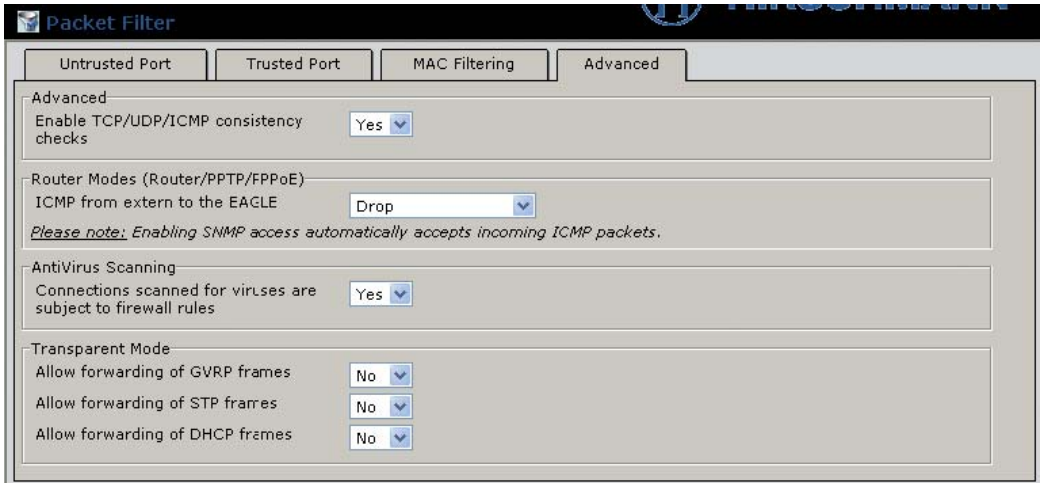
Список доступа				
Система интегратора	Порт	Адрес NOE модуля	Порт	Разрешен
10.10.10.10	Порт 80	192.168.10.10	80	OK
10.10.10.10	Порт 69	192.168.10.10	69	Блокирован

Порты, которые нуждаются в дополнительной защите, в связи с низким уровнем безопасности или отсутствием встроенного контроля безопасности:

Незащищенные протоколы		
IP	**Протокол**	**# порта**
TCP	Telnet	23
TCP/UDP	HTTP	80
TCP/UDP	SNMP v1&v2	161
TCP	FTP	20-Данные 21-Команды
UDP	TFTP	69
TCP/UDP	DNS	53
TCP	POP3	110
TCP/UDP	SMTP	25

Должна быть реализована пакетная фильтрация. Необходимо назначить разрешенные порты для исходящих соединений и разрешенные порты для входящих соединений.





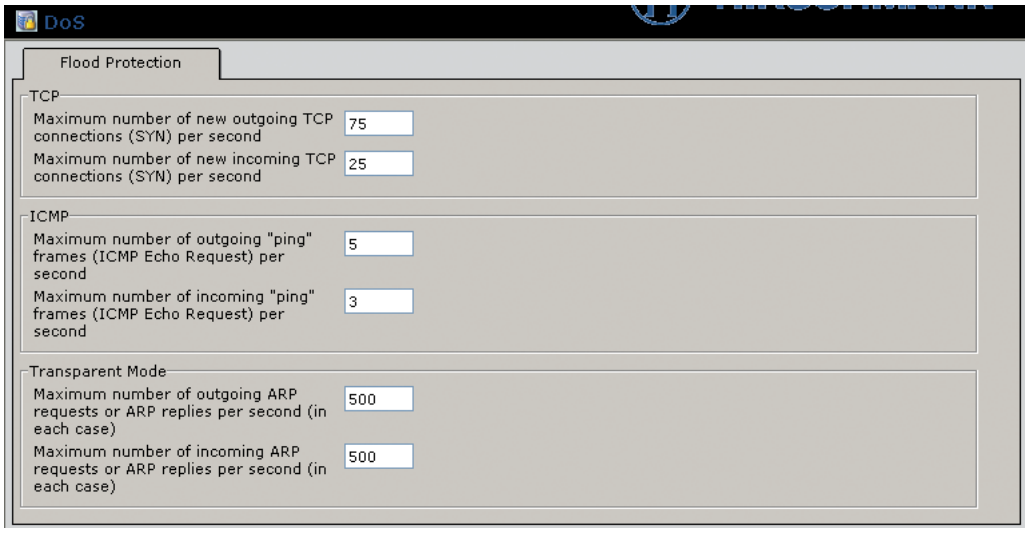
Антивирусное программное обеспечение

Необходимо всегда выполнять антивирусную проверку и постоянно обновлять базы антивирусного программного обновления обеспечения до текущей версии.

Это также применимо к системам SCADA.

Защита от нежелательного трафика (Flood Protection)

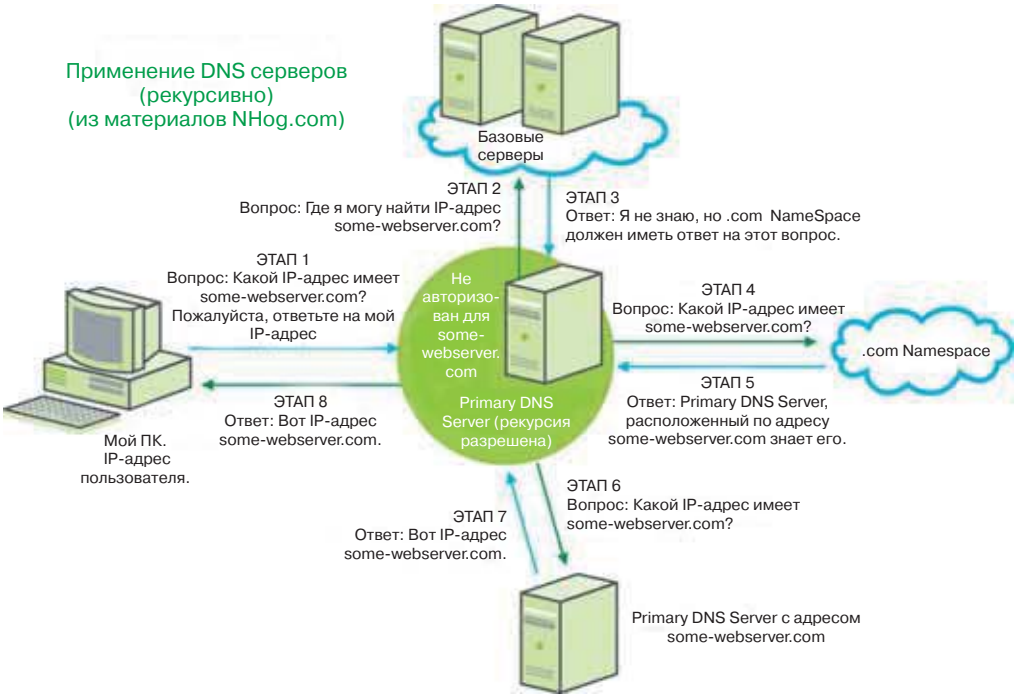
Брандмауэр является важным устройством, обеспечивающим защиту от нежелательного трафика, например такого, как DoS-атаки в сети системы управления. DoS-атаки являются наиболее распространенной формой атак с использованием нежелательного потока данных. Трудно защищать сети системы управления от подобных пересылок по той причине, что возможности брандмауэра ограничены конфигурацией, в то время как новые формы атак постоянно появляются. Если злоумышленник при помощи DoS-атаки успешно проник в сеть системы управления, последствия этого проникновения могут быть сведены к минимуму, при использовании защиты от нежелательного трафика, предусмотренной в брандмауэре.



3.3.4. Правила настройки брандмауэра для специфических сервисов

Сервер доменных имен - Domain Name System (DNS)

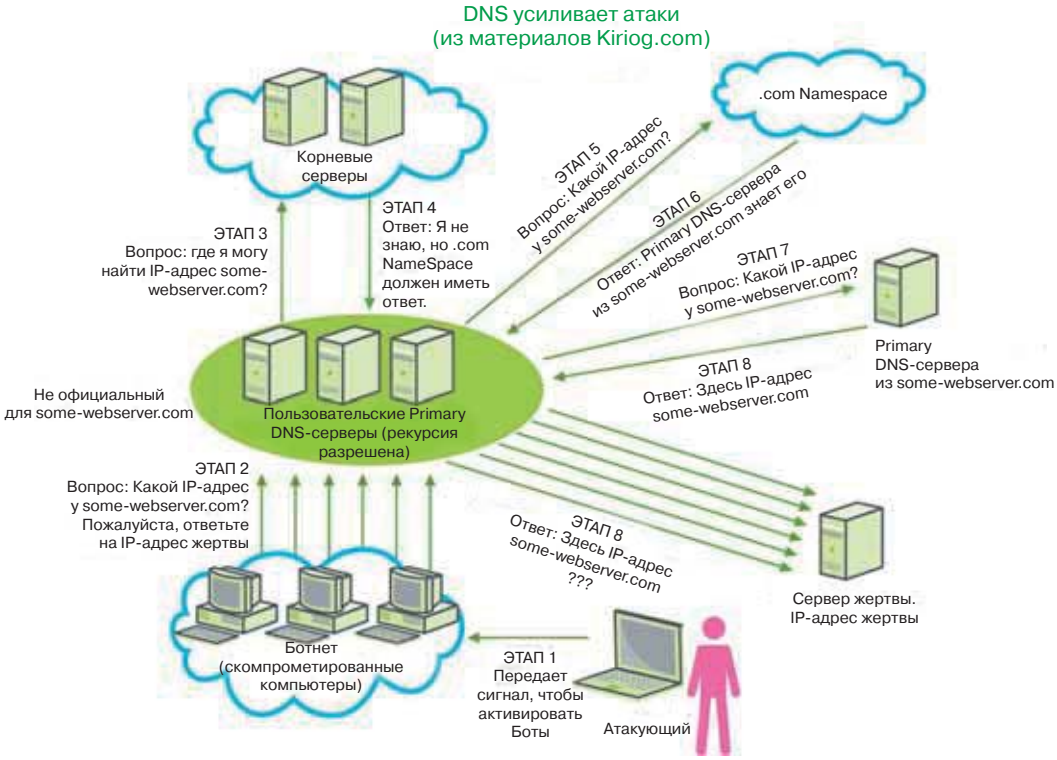
Domain Name System (DNS) представляет собой базу данных имен, используемую для перевода DNS имен в физические IP-адреса устройств. Большинство Интернет-услуг основаны на использовании DNS серверов, но часто в системах управления задаются непосредственно физические IP-адреса. Оборудование Schneider Electric способно работать с устройствами, использующими любой из этих подходов к адресации устройств (IP-адрес ли имя хоста через DNS сервер).



1. Уязвимости DNS.

Существуют многочисленные уязвимости в серверах доменных имен (DNS). Двумя наиболее распространенные из них являются:

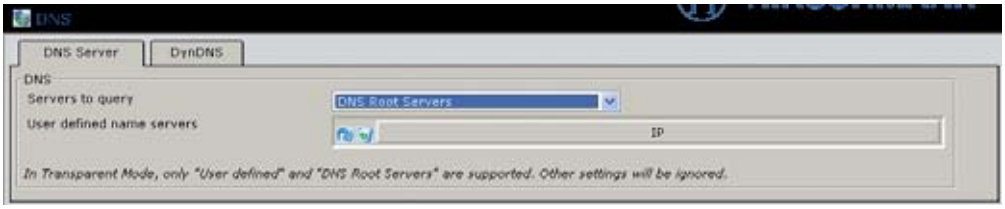
- кэш DNS хранит результаты замены имен на IP-адреса в результате получения специальных запросов от нападающего возможно прочтение истории обновления кэша, веб-трафика, электронной почты, и другие важные данные сети могут быть перенаправлены на внешние системы под контролем атакующего;
- DNS усиливает атаки типа DoS, что генерирует трафик перегрузки сети.



2. Снижение риска DNS

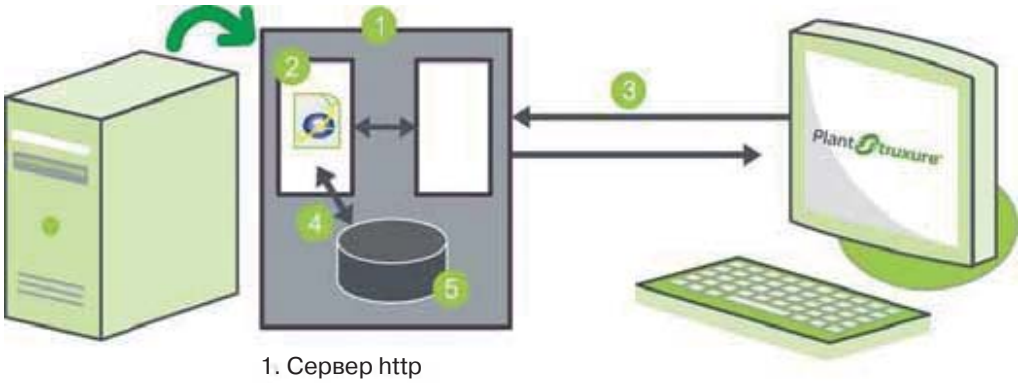
- DNS запросы редко используются в сетях систем управления для доступа к корпоративным сетям, и их следует по возможности избегать.
- Не используйте DNS-запросы в сетях систем управления.
- Рекомендуется задавать конфигурацию DNS на корневых серверах DNS. Запросы будут отправлены на корневой DNS сервер на IP-адрес, хранимый в mGuard.

Эти адреса редко изменяются.



Протокол пересылки гипертекста - Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol является основным протоколом, используемым во «всемирной паутине» World Wide Web и используется во многих приложениях: скачивание файлов, обновления программного обеспечения или для инициализации мультимедийных потоков. Использование HTTP растет в связи с встраиванием веб-серверов в оборудование систем управления. Веб-сервера Schneider Electric используют HTTP протокол для отображения данных и передачи команд через веб-страницы.



1. Сервер http
2. Веб-страница
3. Запрос открытия Веб-страницы
4. Текущее динамическое значение данных помещается в веб-страницу
5. Память устройства

Hypertext Transfer Protocol Secure (HTTPS) представляет собой сочетание Hypertext Transfer Protocol и криптографический протокол. Основные различия между HTTP и HTTPS - это используемые по умолчанию порты (80 для HTTP и 443 для HTTPS). HTTPS работает путем передачи нормальных HTTP страниц с шифрованием. Есть два основных типа шифрования:

- безопасный транспортный уровень -Transport Layer Security (TLS);
- безопасный уровень сокет - Secure Sockets Layer (SSL) – предобработка.

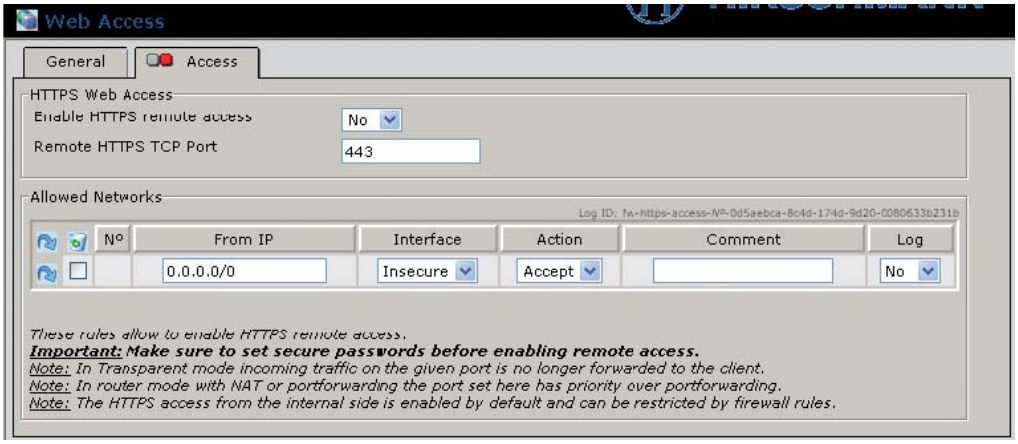
1. Уязвимости HTTP

Протокол HTTP имеет мало механизмов, которые могут быть использованы злоумышленниками, он применим только, в качестве транспортного механизма для атак и червей. Часто применяются атаки «человек в цепи передачи данных» и подслушивание.

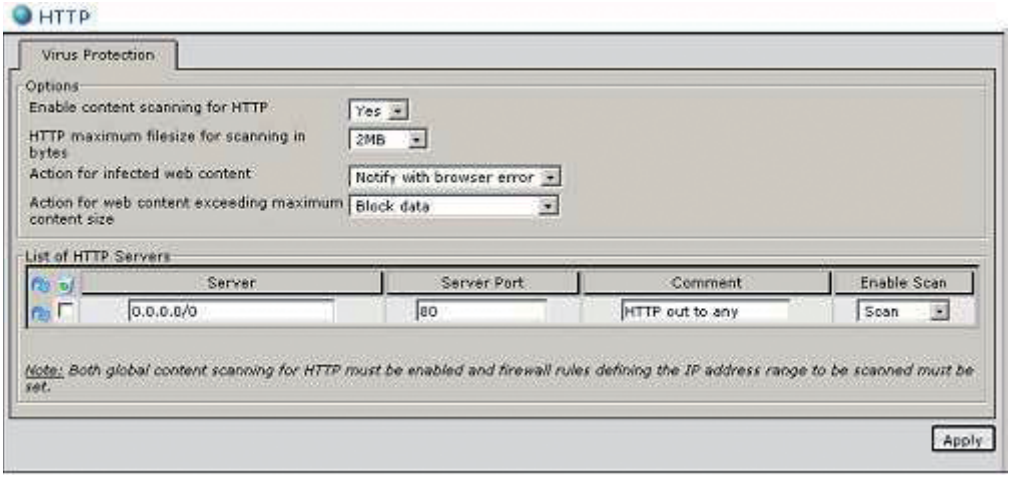
1. Злоумышленник получит доступ к ПК по сети
2. Злоумышленник прослушивает и изменяет передаваемые пакеты

2. Снижение риска HTTP

- Если сервер HTTP не используется, то отключите, а если он необходим, то по возможности используйте HTTPS вместо HTTP, если возможно, и только для конкретного устройства.

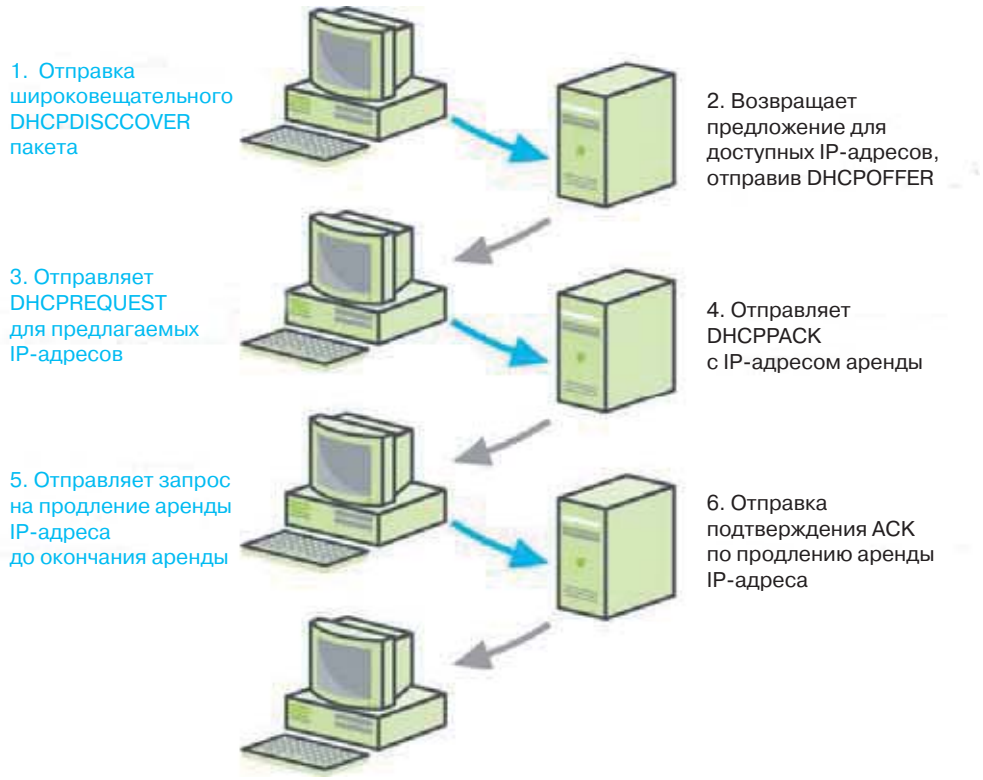


- Если HTTP используется, то применяйте антивирусное программное обеспечение для проверки передаваемой информации.



DHCP

Протокол динамического конфигурирования хостов (компьютеров) - Dynamic Host Configuration Protocol (DHCP) является протоколом сетевого приложения на основе BootP, используется устройствами (DHCP клиентами), которые с его помощью получают информацию о конфигурации для работы в сети Интернет протокола. DHCP является протоколом без аутентификации. Служба DHCP работает с использованием грантов DORA (Discover, Offer, Request and Acknowledgment) (Обнаружение, Предложение, Запрос и подтверждение)



Службы DHCP используют порт 67/UDP в сервере DHCP и 68/UDP для клиентов DHCP.

Schneider Electric использует протокол DHCP для работы механизма замены неисправного оборудования Faulty Device Replacement (FDR).

1. Уязвимость DHCP

Существует два распространенных типа атак на DHCP:

- атака “подвешивания” DHCP - сервер DHCP вводится в затруднее путем подачи на него бесчисленного множества запросов от различных MAC адресов. DHCP-сервер в конечном итоге выводится из строя и не способен выдавать IP-адреса для законных пользователей при запросе о получении или обновлении IP-адреса;
- атака мошенника на DHCP - атакующий маскирует себя, как сервер DHCP, и отвечает на DHCP запросы, указывая ложные IP-адреса, в результате чего достигается атака типа «человек в цепи передачи данных».

2. Снижение риска DHCP

Рекомендации по снижению риска DHCP:

- предотвращение несанкционированного доступа лиц через физическое подключение или беспроводный доступ к компьютеру;
- рекомендуется отключать DHCP в брандмауэре, если он не требуется;
- реализация сервисов в устройствах Schneider Electric. Модули Ethernet NOE или ETY, которые имеют встроенный DHCP-сервер, используют MAC-адрес устройства или имя роли (FDR) для того, чтобы выслать запрашивающему его IP-конфигурацию и файл конфигурации его оборудования.

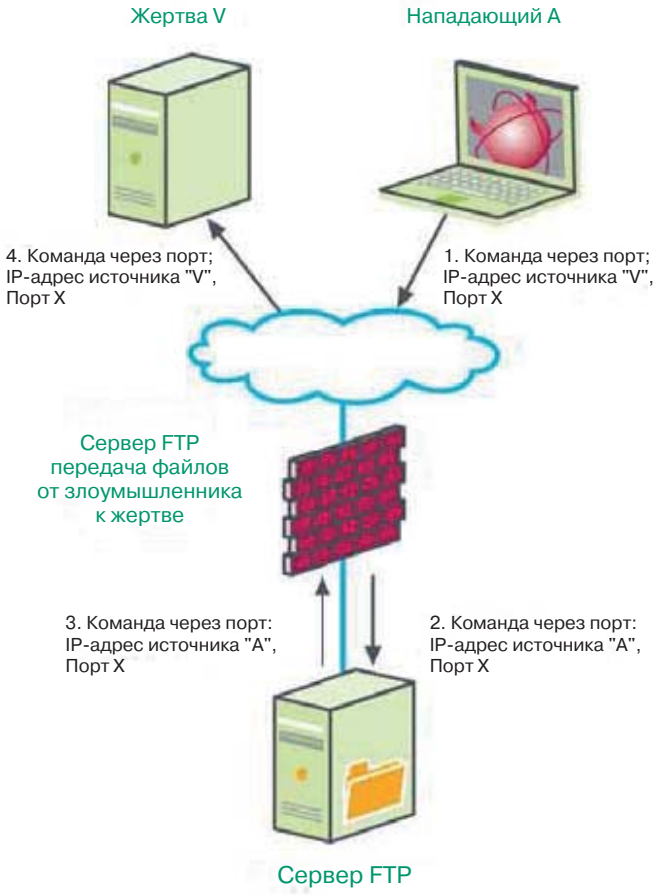
FTP и Тривиальный протокол передачи - Trivial Transfer Protocol (TFTP)

File Transfer Protocol (FTP) и Trivial File Transfer Protocol (TFTP) используются для передачи файлов между устройствами. В устройствах Transparent Ready протокол FTP используется для загрузки прошивки, пользовательских веб-страниц, пересылки журналов аварии и т.д. TFTP используется как основа однонаправленной передачи файлов специального назначения (загрузка прошивок).

1. Уязвимости FTP

При использовании FTP применяют нешифрованные Имя пользователя и Пароль. При использовании TFTP Имя пользователя не требуется.

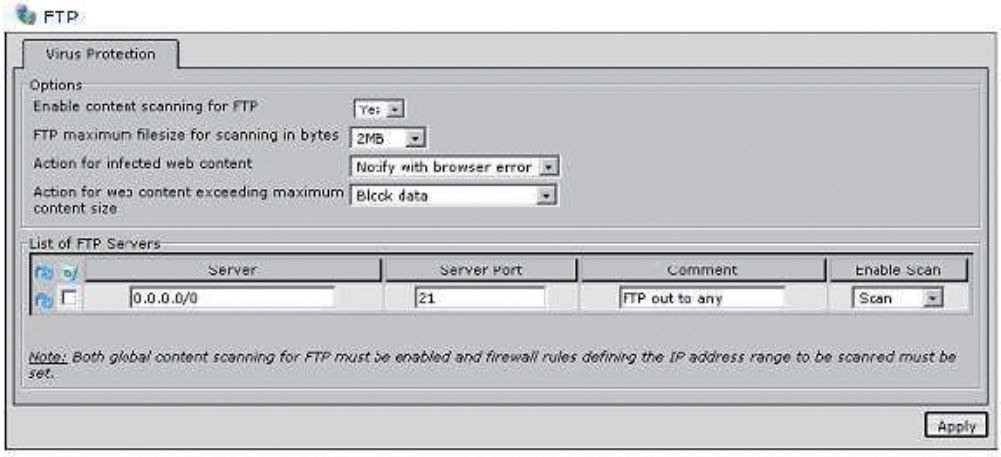
FTP уязвим для переполнения буфера и атак типа дребезга. При нападении типа дребезга злоумышленник использует сервер FTP в пассивном режиме, передавая информацию на любое устройство в сети. Чтобы начать атаку типа дребезга злоумышленник должен войти на сервер FTP, который будет использоваться в качестве "посредника". После подключения к серверу FTP, атакующий посылает команду PORT и направляет все данные, проходящие через этот сервер на шпионский IP-адрес и TCP-порт.



2. Снижение риска FTP

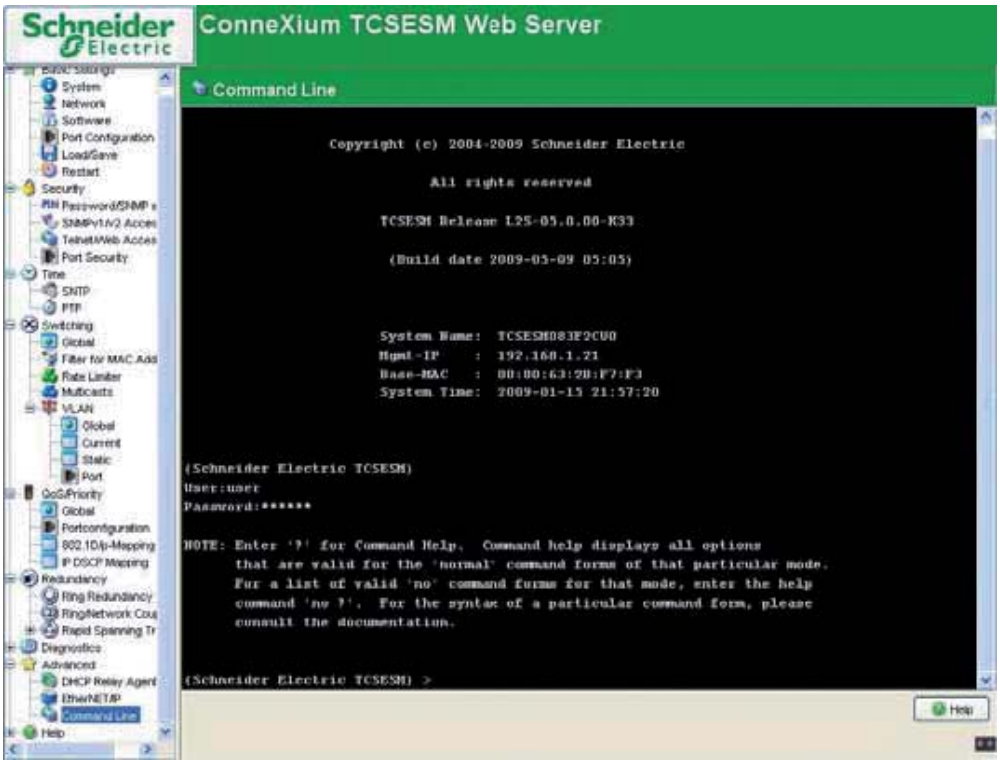
- Передача данных через протокол FTP должна быть разрешена для исходящих сессий только если обеспечены дополнительные режимы проверки подлинности на основе многофакторной аутентификации и используется шифрованный туннель.
- Если возможно, рекомендуется использовать более безопасные протоколы, такие как Secure FTP (SFTP) или Secure Copy (SCP).
- Настройка каждого соединения с сервером производится индивидуально.
- Использование фильтрации пакетов, чтобы разрешать доступ только к FTP-серверу.

● Файлы из FTP-сервера должны быть проверены на наличие вирусов. При определении IP-адреса, как адреса FTP-сервера, необходимо разрешить проверку содержимого на наличие вирусов, если максимальный размер файла не превышает заданного порогового значения. Большие файлы, превышающие заданный максимальный размер файла удаляются.



Telnet

Протокол Telnet предусматривает интерактивный обмен текстовыми сообщениями между клиентом и сервером. Telnet обеспечивает доступ с помощью интерфейса типа командная строка обычно через порт 23. Он, в основном, используется для простого удаленного подключения и использует простые сервисы управления для систем с ограниченными ресурсами или системами с ограниченными требованиями к безопасности.



1. Уязвимости Telnet

Этот протокол представляет серьезный риск для безопасности, потому что все сообщения Telnet, включая пароли, передаются в незашифрованном виде и этот протокол может позволить удаленному устройству обеспечить полный контроль над устройством.

2. Снижение риска Telnet

● Входящие сессии Telnet из корпоративной сети в сеть системы управления должны быть запрещены, если не обеспечена проверка подлинности и туннель с шифрованием.

● Исходящие сессии Telnet должны быть разрешены только по зашифрованным туннелям (например, VPN) для конкретных устройств (описаны в разделе "Удаленный доступ").

Протоколы, используемые для пересылки почтовых сообщений (Simple Mail Transfer Protocol (SMTP) & Post Office Protocol (POP3))

Уведомление по электронной почте в системах автоматизации промышленности становится все более распространенным, так как это позволяет сократить время при использовании удаленных экспертов по поиску и устранению неполадок.

Устройства систем PlantStruxure только отправляют сообщения электронной почты. Тем не менее, существует возможность, что некое стороннее устройство, находящееся в сети, может получать электронную почту. Поэтому настоятельно рекомендуется, чтобы брандмауэр был настроен на сканирование электронной почты на наличие вирусов.

Simple Mail Transport Protocol (SMTP) является стандартным протоколом Интернет, который используют клиенты электронной почты или агенты Mail Transfer Agents (MTA), передающие электронную почту. SMTP-сервер выполняет две функции:

- проверяет корректность конфигурации, и предоставляет разрешение компьютеру на отправку сообщения;
- отправляет исходящие сообщения заранее заданному получателю и проверяет успешность передачи сообщения. Если сообщение не передано успешно, то оно отправляется обратно к отправителю.

Post Office Protocol версии 3 (POP3) или Internet Message Access Protocol (IMAP) используется локальными клиентами электронной почты для скачивания почты с удаленного сервера. POP3 сервер получает сообщение электронной почты и сохраняет его до его считывания локальными клиентами. POP3 использует порт 110.

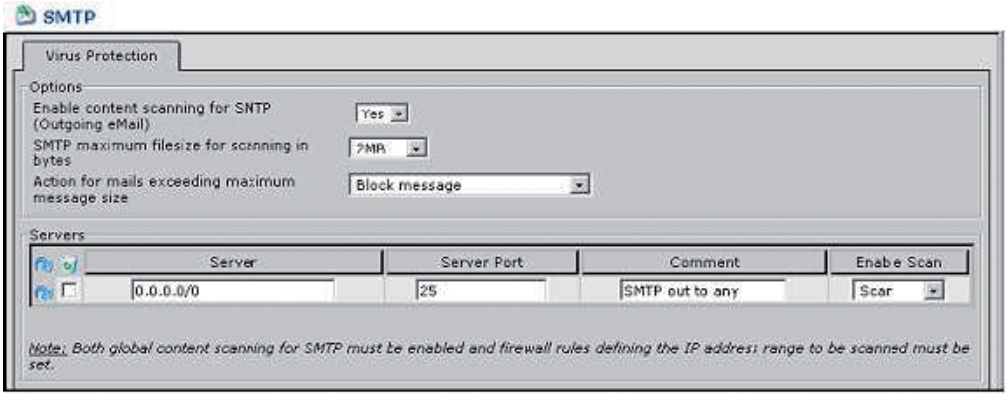
1. Уязвимости SMTP & POP3

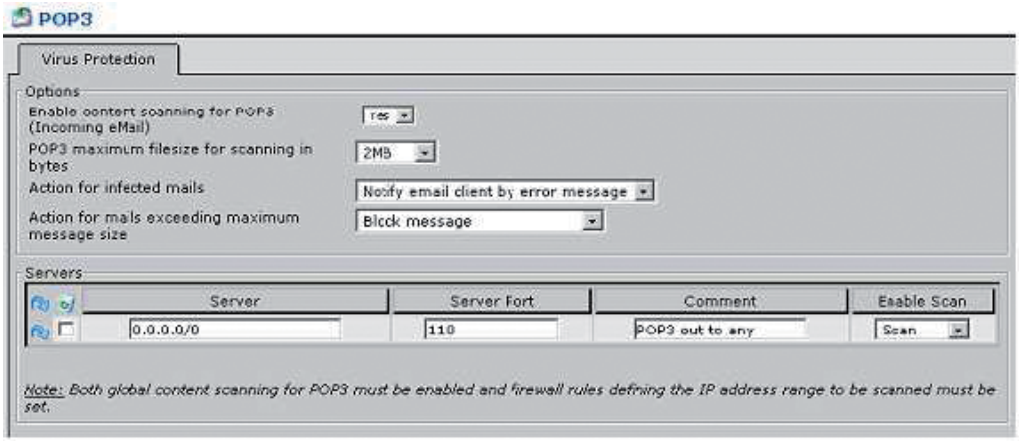
Наиболее распространенной формой атаки является Directory harvesting attack (DHA). Атака основывается на пересылке сообщений с недействительными адресами электронной почты, которые должны быть отклонены системой электронной почты, либо во время обработки на уровне SMTP сервере, либо потом на уровне Delivery Status Notification (DSN) сервера. Когда злоумышленник получает отказ от некорректного адреса электронной почты, адрес электронной почты отправителя отбрасывается. При отсутствии отказа или DSN подтверждает получение, адрес электронной почты считается действительным и добавляется в базу данных спама. Злоумышленник обычно использует два метода:

- грубая сила: подход, при котором отправляются сообщения со всеми возможными буквенно-цифровыми адресами и ожидается правильный ответ;
- селективные: подход, при котором отправляются письма электронной почты с помощью вероятного имени получателя в надежде найти правильное имя пользователя.

1. Уменьшение риска SMTP и POP3

- Входящие адреса электронной почты не должны быть разрешены для любых устройств систем управления.
- Исходящие почтовые сообщения SMTP из сети системы управления в корпоративную сеть могут быть использованы только для отправки предупреждающих сообщений. Устройства PlantStruxure сегодня отправляют только почтовые сообщения.
- Все сообщения должны быть проверены на вирус. Обратите внимание, что некоторые брандмауэры не могут проверить зашифрованные данные на наличие вирусов.
- Определите, какие IP-адреса требуют антивирусной защиты, и разрешите проверку содержимого на вирусы, задайте максимальный размер файла FTP, доступного для проверки.





Простой протокол управления сетью (Simple Network Management Protocol (SNMP))

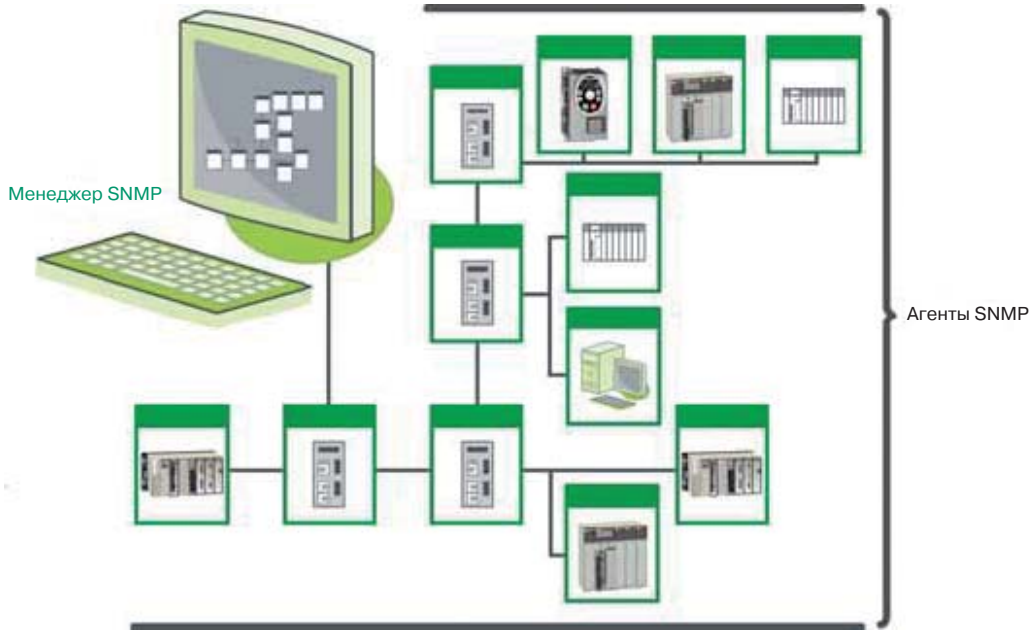
Все устройства PlantStruxure на сети Ethernet имеют активный сервис SNMP для управления сетью. Большинство устройств PlantStruxure используют SNMP v2, который не использует шифрование, поэтому считаются не безопасными. Коммутаторы ConneXium используют SNMP v3, в которых добавлена функция безопасности:

- проверка целостности сообщений;
- аутентификация;
- шифрование.

SNMP состоит из трех частей.

- Менеджер: приложение менеджера, которое управляет SNMP агентами на сети путем выдачи запросов, получения ответов и прислушивания трафика до обнаружения ловушки, выпущенной агентом. Управляемым устройством может быть любой тип устройства: маршрутизаторы, серверы доступа, коммутаторы, мосты, концентраторы, ПКК, преобразователи частоты…
- Агент: программный модуль агента управления сети, который находится в управляемом устройстве. Агенты позволяют менеджерам изменять параметры конфигурации.

● Система управления сетью (Network management system (NMS)): представляет собой терминал, через который администраторы могут выполнять задачи администрирования сети.



1. Уязвимости SMNP

● Протокол SNMP в целом слаб в вопросах безопасности. Версии 1 и 2 протокола SNMP используют незашифрованные пароли для чтения и конфигурирования устройств. Пароли нельзя изменять. Версия 3 является гораздо более безопасной, но её применение все еще ограничено в использовании.

● Часто SNMP автоматически устанавливается вместе с уровнем доступа Public ("открытый") для чтения строк и уровнем доступа Pravite ("закрытый")для записи. Этот тип установки предоставляет злоумышленнику средства для выполнения разведывательных атак и возможности для создания условий по отказу в обслуживании.

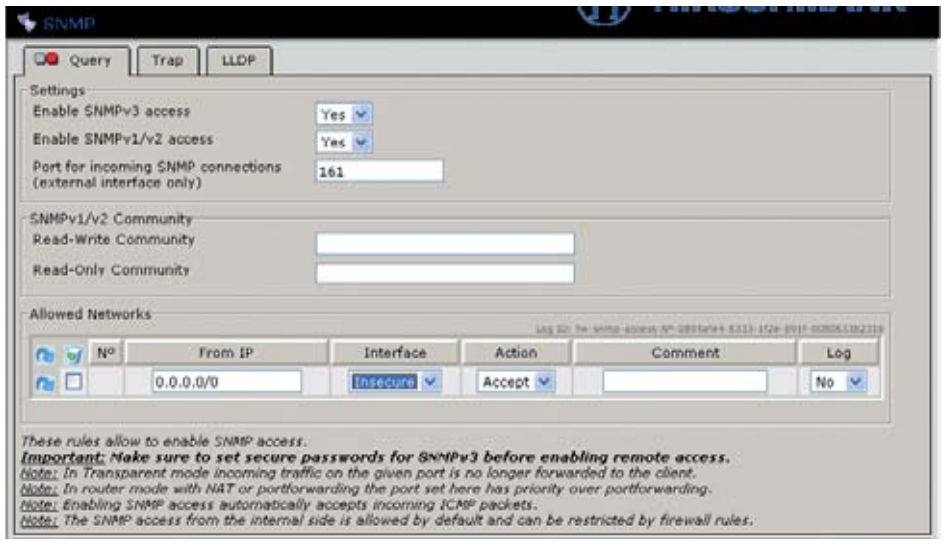
● SNMP также предоставляет информацию о системе, которая может позволить злоумышленнику собрать информацию о конфигурации системы.

2. Снижение рисков SNMP

● Лучшая защита - это переход на SNMP3, который шифрует пароли и сообщения.

● Передача данных по протоколам SNMP V1 и V2 в/из сети систем управления должна быть запрещена, исключением могут быть только случаи использования полностью изолированных каналов передачи данных в пределах систем управления.

● Контроль доступа по списку разрешенных сервисов для конкретных IP-адресов при доступе по протоколу SNMP к устройству.



Трансляция Доступа к Сети (Network Address Translation (NAT))

NAT представляет собой брандмауэр, который не допускает передачу данных от устройств без разрешения. При этом любой IP-адрес не может получить доступ к устройству непосредственно.

NAT подразумевает создание карты всей сети и организацию маршрутизации передачи данных через один IP-адрес. NAT опирается на предположение, что не все внутренние устройства могут активно общаться с внешними устройствами в любой момент времени. Брандмауэр должен отслеживать состояние каждого соединения и, как каждый частный внутренний IP-адрес и порт источника был переназначен.

Если от брандмауэра получено разрешение, IP-адрес назначения заменяется и пакеты направляются надлежащему внутреннему узлу.

Хотя NAT маршрутизаторы технически не являются брандмауэрами, потому что они не умеют фильтровать пакеты, NAT защищает устройства PlantStruxure от внешней сети. NAT обеспечивает высокий уровень безопасности, так как пакеты из Интернет блокируются и закрывается доступ к устройствам напрямую. Только ответы на запросы разрешены для передачи.

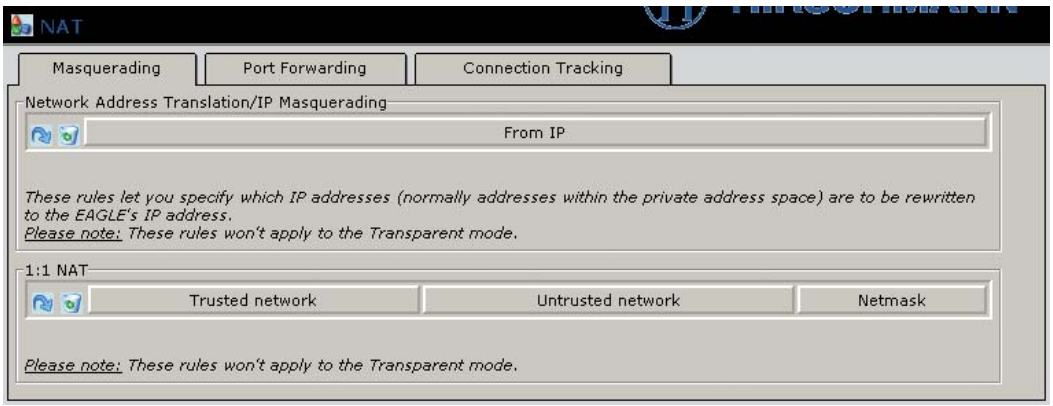
NAT первоначально была разработан для организации сокращения доступных IP-адресов. Это было особенно актуально до IPv6. NAT также упоминается, как маскирование IP-адресов.

1. Уязвимости NAT

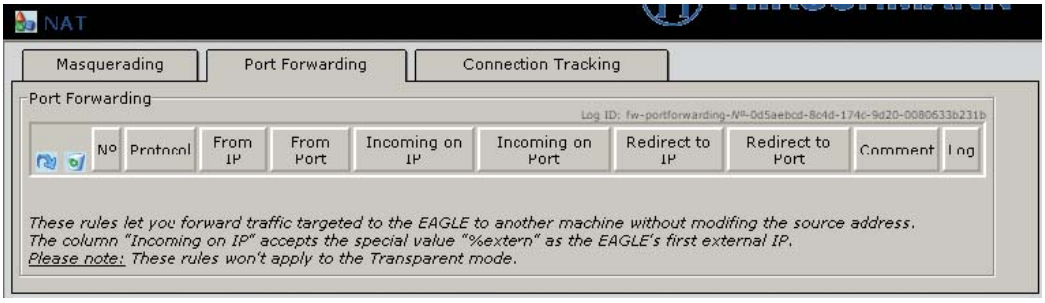
- • Известных уязвимостей нет

2. Рекомендации по конфигурированию NAT

- Используйте NAT, когда это возможно. NAT не поддерживает протоколы производитель-потребитель (EtherNet/IP и полевые шины).

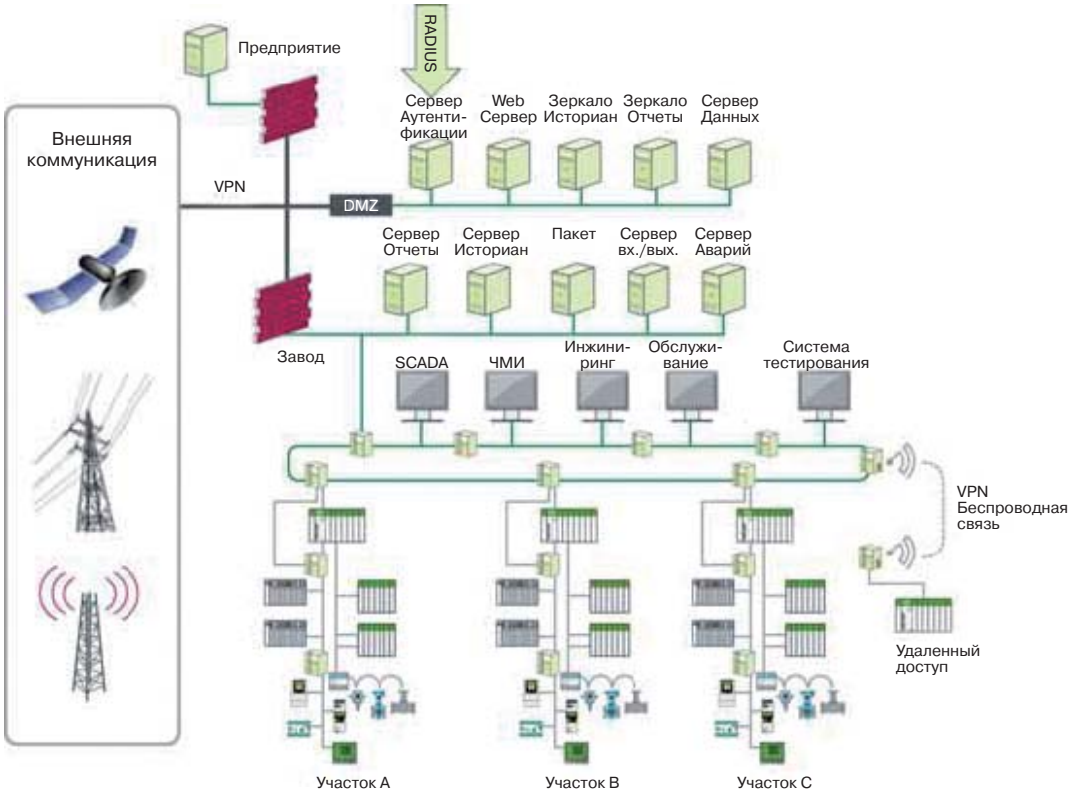


Так как NAT, как правило, используется на маршрутизаторах и сетевых шлюзах, необходимо включать IP-forwarding с тем, чтобы пакеты могли передаваться между сетями:



3.3.5. Внешняя аутентификация

Проверка подлинности - это процесс определения истинного объекта. Есть несколько методов внешней проверки подлинности. Метод удаленной проверки пользователей (Remote Authentication Dial In User Service (RADIUS)) является наиболее популярным сетевым протоколом, используемым в сетях систем управления.

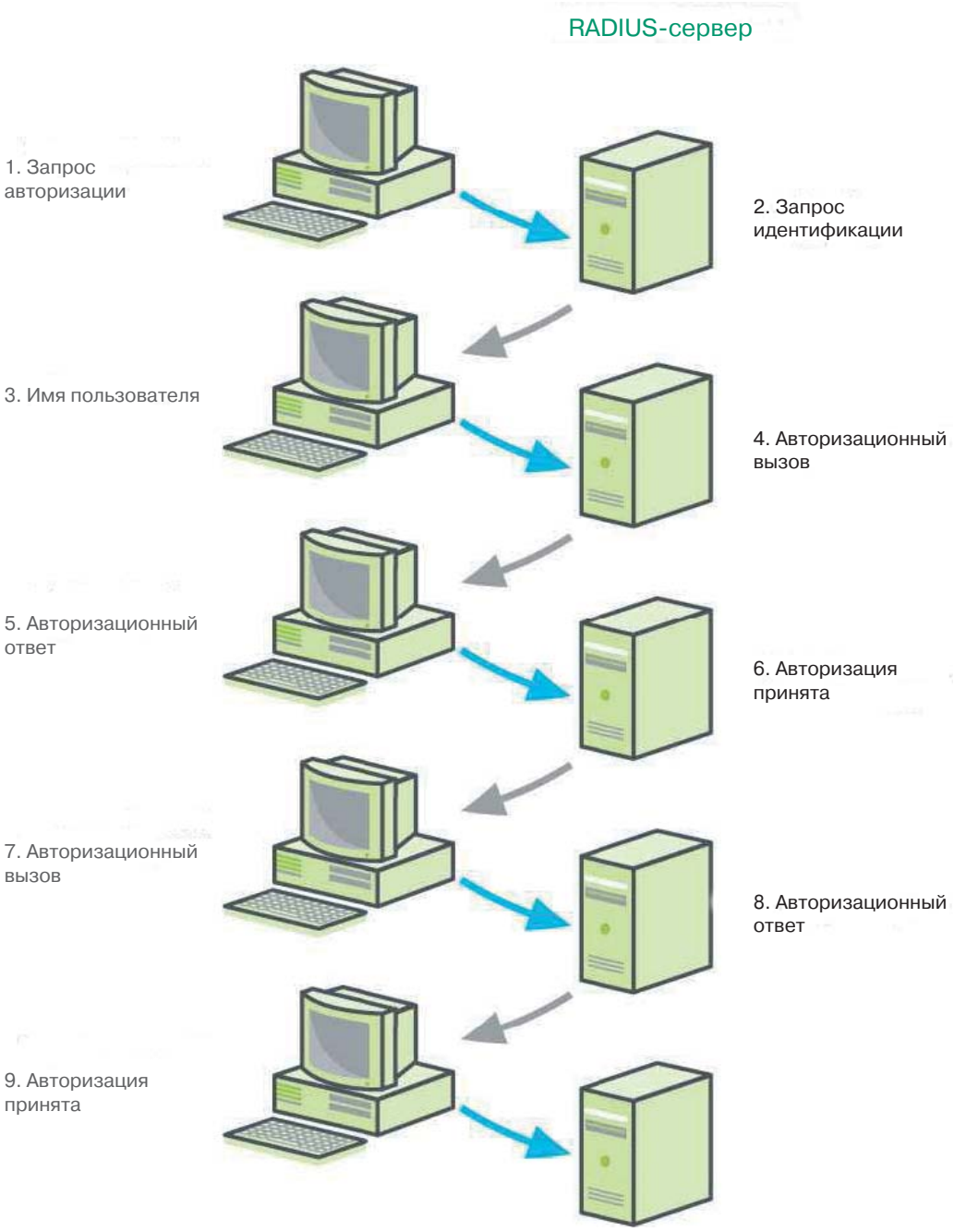


RADIUS имеет три функции:

- аутентификации пользователей и устройств, перед предоставлением им доступа к сети;
- авторизации пользователей и устройств для определенных сетевых услуг;
- ответственность за использование этих услуг.

Передача данных между клиентом и сервером при помощи RADIUS обеспечивается при обеспечении проверки подлинности с использованием специального кода. Этот код шифруется с помощью алгоритма шифрования MD5. Первоначально RADIUS был разработан для коммутируемого удаленного доступа. Сегодня RADIUS поддерживается в серверах виртуальных частных сетей (VPN), беспроводных точек доступа, аутентификации коммутаторов Ethernet, цифровых абонентских линий Digital Subscriber Line (DSL) и других видов доступа к сети.

Подробная информация относительно установления подлинности приводится в секции «Аутентификация при удаленной коммуникации».



Принципы Авторизации

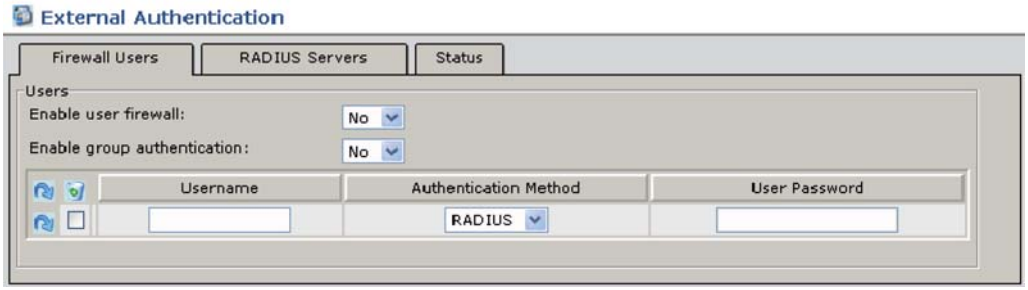
- • Используйте различные методы шифрования для каждой пары клиента и сервера RADIUS.
- • Если возможно, используйте различные пароли и шифры длиной минимумом 16 знаков и состоящие из случайной последовательности прописных и строчных букв, чисел и знаков пунктуации.

Уязвимости аутентификации

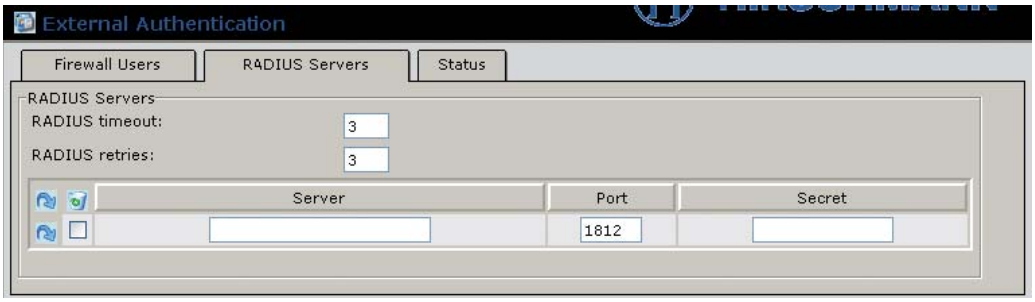
Общие ресурсы в сетях с RADIUS не располагают достаточными средствами защиты от подбора паролей по словарю. Эта уязвимость устраняется с помощью IPsec, рассматриваемой в разделе удаленный доступ.

Снижение риска при аутентификации

Используйте RADIUS аутентификацию на брандмауэре.

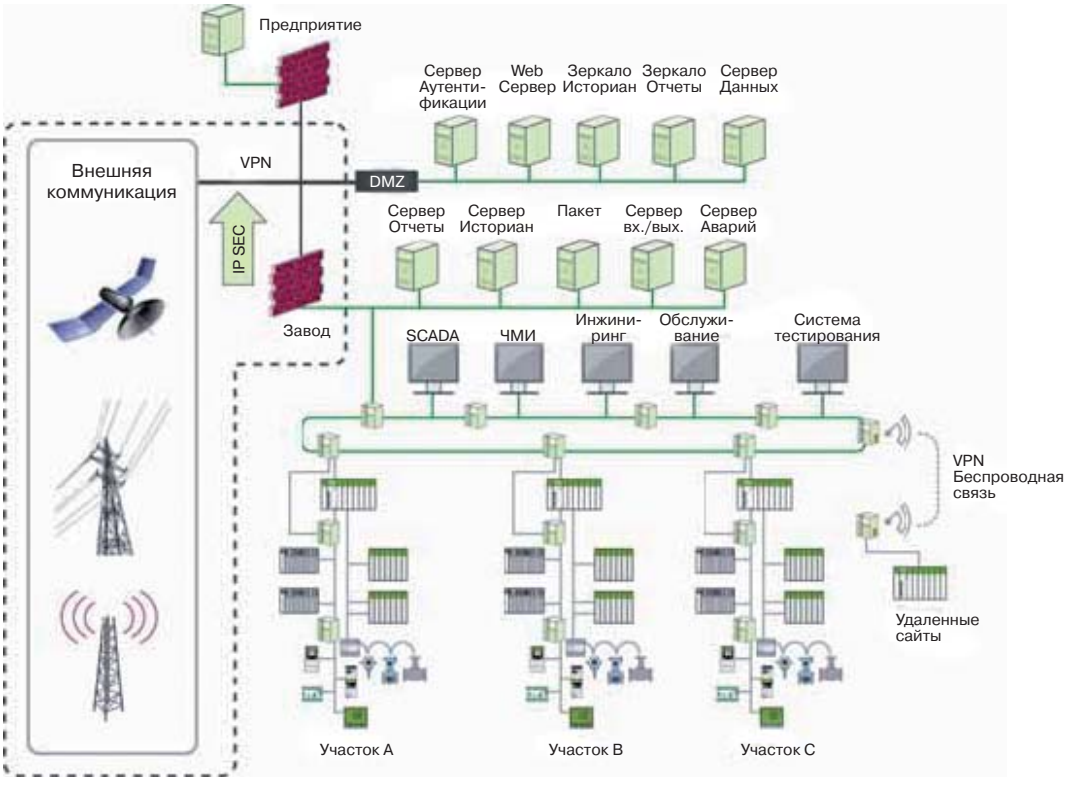


Задайте общий код доступа «секрет» для проверки подлинности связи между RADIUS-сервером и RADIUS- клиентом.



3.3.6. Удаленный доступ

Существует растущий спрос на установку удаленного подключения к системам управления предприятий для того, чтобы позволить инженерам и обслуживающему персоналу проводить мониторинг и управление системой из удаленных мест. Удаленный доступ может быть дорогостоящим и открытым для кибер-атак, если он не настроен правильно. Поэтому компании переходят от телефонных модемов к виртуальным закрытым сетям (Virtual Private Network (VPN)). VPN обеспечивает высочайший уровень безопасности за счет шифрования данных и специальных методов аутентификации, что предотвращает просмотр данных из публичных сетей Интернет.



Существуют две технологии VPN

- Протокол безопасности Интернета (Интернет Protocol Security (IPSec)): IPSec является открытым стандартом передачи данных для приложений, которые способны работать с IP-шифрованием на сетевом уровне и используются для обеспечения безопасной передачи данных по открытым каналам Интернет через IP-сети. IPSec поддерживает:
  - o целостность данных на сетевом уровне;
  - o конфиденциальность данных;
  - o аутентификации при передаче данных;
  - o защита от повторов.

IPsec поддерживает алгоритмы цифровой подписи и секретного ключа с кодом.

- ・Secure Socket Layer (SSL): SSL является общим протоколом, встроенным в большинство браузеров. SSL прост в настройке и не требует специального клиентского программного обеспечения.

Однако, SSL работает только для веб-(TCP) приложений и поддерживает только цифровые подписи.

IPsec

Для организации удаленного доступа настоятельно рекомендуется применение VPN с IP-безопасностью (IPsec). IPSec представляет собой набор стандартов для выполнения шифрования, аутентификации и безопасной установки туннеля.

IPSec открывает частные туннели для подключения безопасного соединения двух устройств, подключаемых через открытые каналы связи в Интернете. IPsec использует следующие компоненты:

- интернет-протокол обмена ключами (Internet Key Exchange (IKE и IKEv2)): протокол, используемый для создания ассоциации безопасности (SA) путем обработки переговоров, протоколов и алгоритмов, передаваемых по сети. Интернет Key Exchange также производит шифрование и проверку подлинности ключей для использования в IPsec. Чтобы настроить общий секретный код используемых криптографических ключей, IKE использует Diffie-Hellman протокол генерации кодов ключей;
- заголовок аутентификации (Authentication Header (AH)): протокол безопасности для проверки подлинности источника IP-пакетов и проверки целостности его содержимого с помощью хеш-алгоритмов, таких как MD% или SHA-1;

0 - 7 бит	8 -15 бит	16-23 бит	24 - 31 бит
Следующий заголовок	Деструктивная длина	РЕЗЕРВ	
Индекс параметров безопасности (Security parameters index (SPI))			
Номер последовательности			
Данные аутентификации (переменная)			

- инкапсуляция безопасной нагрузки (Encapsulating Security Payload (ESP)): протокол, который предоставляет средства для поддержания конфиденциальности с помощью шифрования, аутентификации источника и сохранения целостности (аутентификация). ESP в туннельном режиме инкапсулирует весь IP-пакет (заголовок и полезную нагрузку), а затем добавляет новый IP-заголовок, чтобы зашифровать весь пакет.

Этот новый IP-заголовок содержит адрес назначения, необходимый для маршрутизации защищенных данных при передаче через сеть.

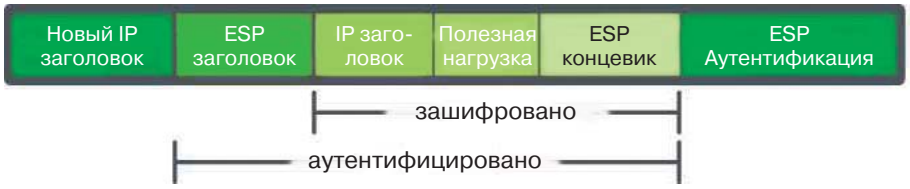
0 - 7 бит	8-15 бит	16 -23 бит	24-31 бит
Индекс параметров безопасности (Security parameters index (SPI))			
Номер последовательности			
Полезные данные (переменные)			
	Заполнение (0-255 байт)		
		Длина поля	Следующий заголовок
Данные аутентификации (переменная)			

IPsec работает в двух режимах соединения.

- Туннельный режим: Соединение установлено между шлюзом и шлюзом, шлюзом и хостом и хостом и хостом. Содержимое IP-пакета инкапсулируется для того, чтобы простроить виртуальный безопасный канал между двумя шлюзами и обеспечивать безопасный туннель через ненадежные каналы связи Интернета.

Транспортный режим ESP

- Транспортный режим: соединение хост-хост. Только полезная нагрузка (передаваемые данные) IP-пакета зашифровываются и/или проводится проверка подлинности.



Транспортный режим ESP

VPN-туннель использует алгоритмы шифрования для зашифровывания и расшифровывания информации. Применяются три общих протокола шифрования:

- расширенный стандарт шифрования (AES (Advanced Encryption Standard)): симметричное 128-битное шифрование данных, которое работает на нескольких слоях сети одновременно. Алгоритм может быть реализован в программном обеспечении, системном программном обеспечении, аппаратно или в комбинации разных методов;
- DES: блочный шифр с 64-разрядным размером блока, который использует 56-битные ключи. В связи с последними достижениями в области компьютерных технологий, некоторые эксперты более не считают DES защиту способной оградить от всех атак;
- Triple-DES (3DES): алгоритм 3DES является вариантом 56-битного DES шифрования. 3DES функционирует аналогично DES, в нем так же данные разбиваются на 64-битные блоки. 3DES обрабатывает каждый блок три раза, каждый раз используется независимый 56-бит ключ. 3DES удваивает эффективность шифрования по сравнению с 56-битным DES.

Проверка подлинности необходима для того, чтобы убедиться, что во время передачи никаких изменений в сообщении не было сделано. Алгоритм случайного хеш-шифрования представляет собой односторонний алгоритм шифрования, использующийся для того, чтобы принять входное сообщение произвольной длины и произвести конвертирование его в сообщение фиксированной длины на выходе. Алгоритм случайного хеш-шифрования используется в IKE, AH и ESP для проверки подлинности данных. Два популярных алгоритмов хеширования представлены ниже.

- Message Digest 5 (MD5): 160-битным ключом.
- Secure Hash Algorithm 1 (SHA-1): создает 160-битный (20 байт) дайджест сообщения. SHA-1 работает медленнее, чем MD5, но обеспечивает более надежную защиту от некоторых видов атак.

Рекомендации по удаленному доступу

- Все возможности удаленного доступа, как аппаратного, так и программного, должны быть организованы в соответствии с выбранной политикой безопасности.
- Удаленный доступ должен быть разрешен только после прохождения идентификации и проверки подлинности.
- Требуется отключение удаленного доступа, если в нем нет потребности.
- Изменить пароль доступа сразу после завершения сеанса удаленного обслуживания.
- Анализ риска для системы управления в случае открытия удаленного доступа.
- Персонал удаленной поддержки, подключаемый через Интернет или с помощью телефонных модемов, должен использовать зашифрованный протокол доступа, такой как IPSec.
- После подключения, должна проводиться процедура повторной проверки подлинности на брандмауэре сети управления с помощью мощного механизма безопасности, такого как многофакторная аутентификация для того, чтобы открыть доступ к сети системы управления.
- Автоматическая блокировка возможности подключения пользователя после нескольких последовательных попыток подключения этого пользователя с некорректным вводом пароля.
- Необходимость менять пароль и не допускать работу с паролем, заданным по умолчанию.
- Изменение пароля должно происходить периодически.
- Для удаленного доступа через модемы:

o изменение параметров по умолчанию в соответствующих случаях:
– отключение автоматического ответа на всех модемах исходящих каналов связи;
– увеличение числа звонков перед ответом;
– использование таймера подсчета бездействия, если таковые имеются.

- Использование режим обратного вызова, если возможно.
- Убедитесь, что VPN-устройства не оказывают негативного влияния на сеть системы управления.
- Для беспроводных коммуникаций рекомендации приведены в соответствующем разделе приложения.

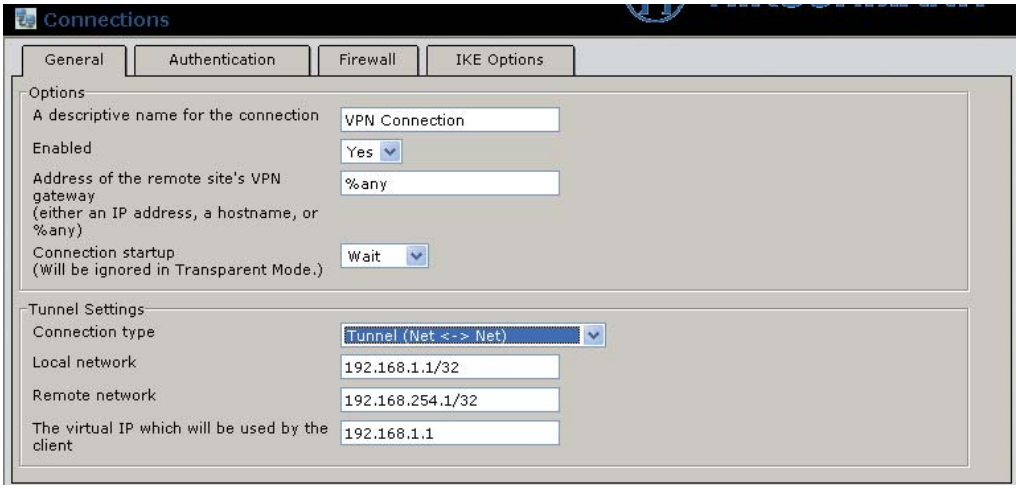
1. Уязвимости удаленного доступа

- Некорректные настройки ограничения доступа является основным источником уязвимости для сетей систем управления.
- Недостатки фильтрации на брандмауэрах.
- Сервисы, разрешенные в сети системы управления.
- Нападение на телефонные модемы (компьютерный набор последовательных телефонных номеров в поисках модема).
- Подключение с паролями, заданными по умолчанию производителем оборудования.
- Доступ через ссылки, которые не имеют защиты с проверкой подлинности и/или шифрования данных.
- Беспроводные каналы связи имеют дополнительные опасности, поскольку радиоволны распространяются за пределы предназначенной для них области:

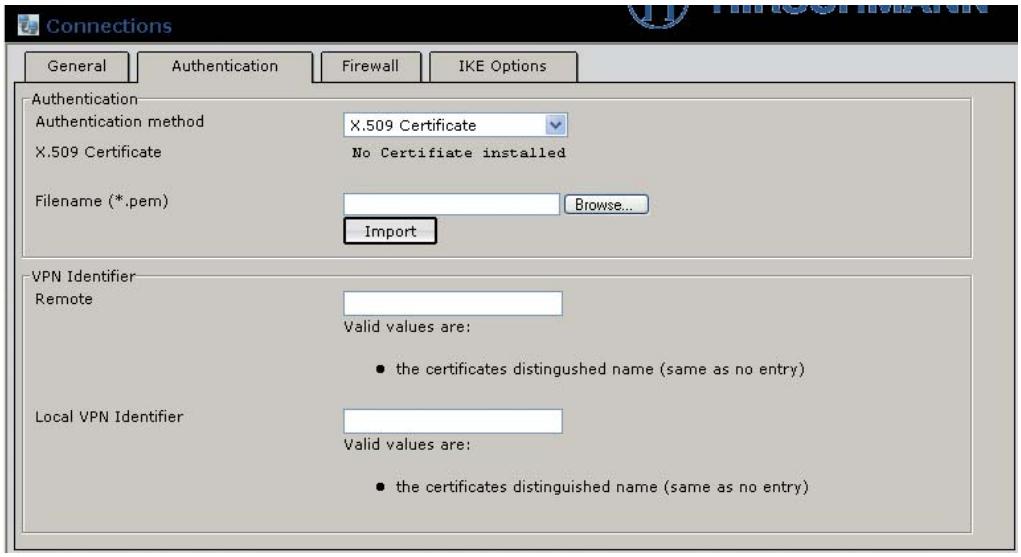
o злоумышленники, которые находятся в диапазоне распространения радиоволн, могут захватить управление или перехватывать незащищенные данные;
o исследование беспроводных сетей является распространенной формой атаки, когда человек ищет мобильное устройство в движущемся транспортном средстве, используя портативный компьютер или КПК.

2. Снижение риска удаленного доступа

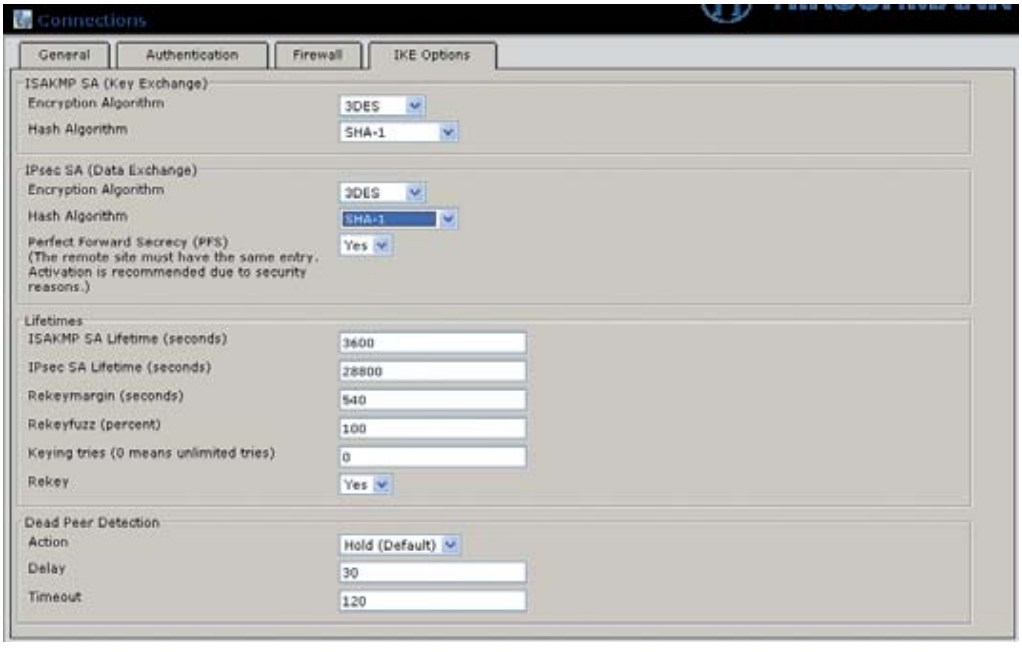
Брандмауэр должен быть настроен на фильтрацию внешних связей и обеспечивать соединения через VPN с помощью тоннеля сети в сеть. Режим передачи из сети и в сеть является наиболее безопасным и будет работать во всех приложениях.



Сертификат ключа X.509 удостоверяет подлинность открытого ключа, который будет использоваться в качестве хеш-значение в IPsec (или S/MIME).



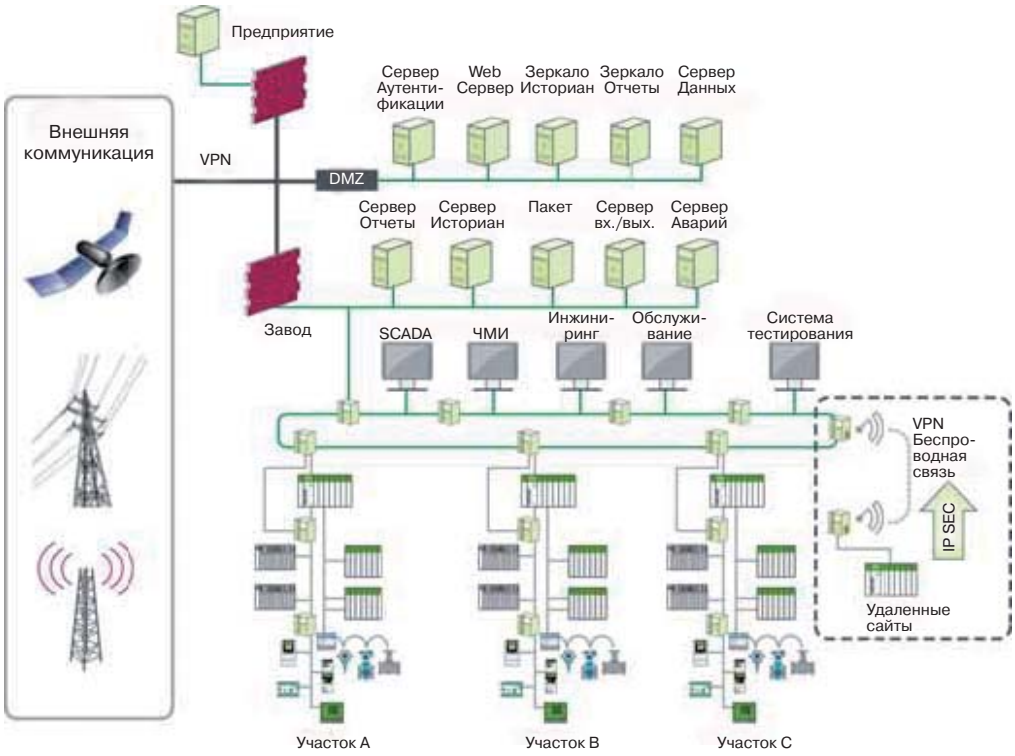
Рекомендуется применять алгоритм SHA-1. Алгоритм хеширования MD5 был взломан.



3.4. Дистанционное управление

Дистанционное управление отличается от удаленного доступа тем, что дистанционное управление часто организуется в обход защиты периметра безопасности в связи с задержками, которые накладывает брандмауэр. Необходимо проведение анализа рисков такого подключения для того, чтобы выявить и сбалансировать влияния рисков.

Дистанционное управление через беспроводный доступ вносит дополнительные проблемы безопасности. Лучшей защитой является использование VPN туннелей с IP Sec (в качестве межсетевого экрана).



3.4.1. Рекомендации по организации дистанционного управления

При использовании беспроводной связи существуют отдельные рекомендации по обеспечению безопасности:

- перед установкой беспроводной линии связи необходимо провести обследование для того, чтобы определить местоположение антенны и незащищённость передаваемых данных, чтобы минимизировать сторонние воздействия на беспроводную сеть. Обследование должно принимать во внимание тот факт, что злоумышленники могут использовать мощные направленные антенны, которые расширяют эффективный диапазон беспроводной сети за пределы ожидаемого стандартного диапазона. Клетки Фарадея и другие методы также доступны, чтобы минимизировать распространение зоны беспроводной сети за пределы отведенных для беспроводной связи мест;
- пользователи сети, использующие беспроводной доступ, должны применять аутентификацию IEEE 802.1x с защищенными протоколами аутентификации (например, Extensible Authentication Protocol [EAP] с TLS [EAP-TLS]), что обеспечивает аутентификацию пользователей с помощью сертификатов или удаленной проверки пользователей через (RADIUS) сервер.
- Беспроводные точки доступа и серверы данных с беспроводным доступом работников должны быть расположены на изолированной сети с описанным количеством подключений и минимальным (одно, если это возможно) подключением к сети ICS.
- Беспроводные точки доступа должны быть настроены на уникальный набор услуг (SSID), отключение трансляции SSID, и настройку MAC-фильтрации на минимум.
- Беспроводные устройства, если они используются в сети Microsoft Windows ICS, должны быть настроены в отдельную организационную единицу-домен Windows.

- Беспроводные устройства должны подключаться с использованием шифрования и защиты целостности при передаче данных. Шифрование не должно ухудшать эксплуатационные характеристики конечного устройства. Шифрование следует рассматривать на уровне 2 модели OSI, а не на уровне 3, что сокращает задержки шифрования. Следует также рассматривать использование аппаратных ускорителей для выполнения криптографических функций.
- Для сетей с ячеистой топологией требуется рассмотреть вопрос об использовании широковещательных ключей доступа вместо открытого доступа через уровень 2 модели OSI, это позволит достигнуть максимальной производительности. Приемы асимметричной криптографии должны использоваться для выполнения административных функций, симметричного шифрования каждого потока данных, а также трафика управления сетью. Протокол адаптивной маршрутизации следует рассматривать, если устройства будут использоваться для беспроводной мобильной связи. Время восстановления сети должно быть максимальным для обеспечения быстрого восстановления работы сети в случае обнаружения ошибок или потери силового питания. Использование сетей с ячеистой топологией может обеспечить отказоустойчивость путем выбора альтернативного маршрута и упреждения сбоя в сетях.

3.4.2. Уязвимости при использовании дистанционного управления для беспроводных серей

- Настройки безопасности, либо не сделаны либо настроен низкий уровень безопасности.
- Радиоволны распространяются за пределы заданной области.
- Легко подслушивать.
- Физическое расположение позволяет получить легкий доступ.
- Не заданы политики безопасности беспроводной сети.
- Злоумышленники, которые находятся в диапазоне доступа или перехвата, могут осуществить неконтролируемое подключение.
- Мобильное проникновение - это распространенная форма атаки, когда человек с портативным компьютером или КПК в движущемся транспортном средстве пытается получить доступ к системе.

Курт Роджерс / «San Francisco Chronicle» Сан-Франциско -2009

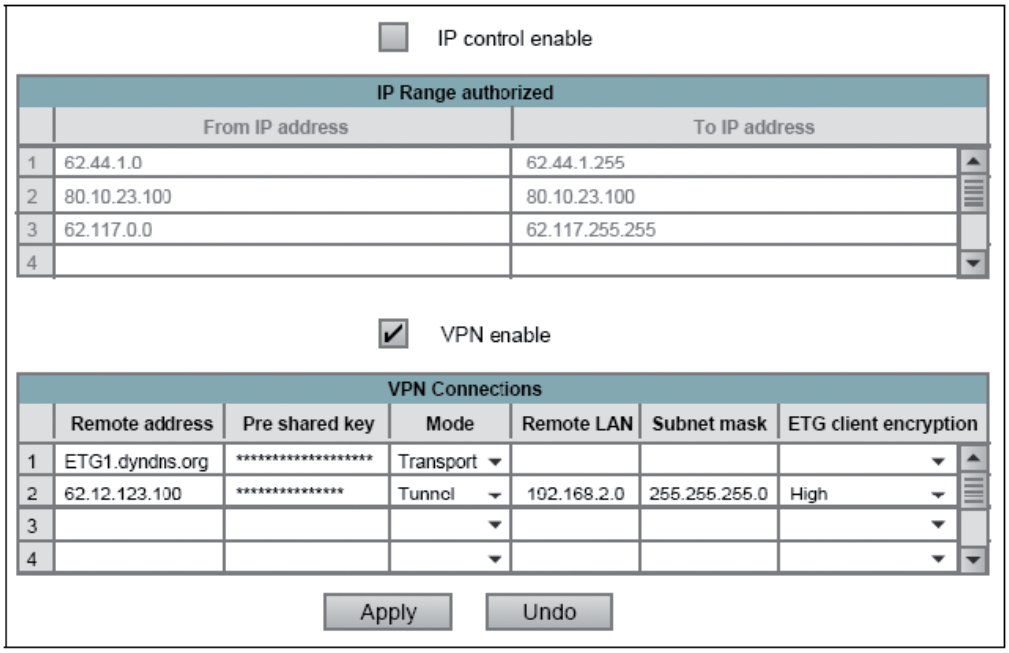
3.4.3. Снижение риска при удаленном управлении.

FactoryCast ETG302x предоставляет возможности подключения через VPN для удаленного управления. Рекомендуется использовать подключение через два ETG для организации доступа к сети управления от станций RTU через беспроводное подключение.

Те же правила, что и для брандмауэра, нужно применять и для ETG302x:

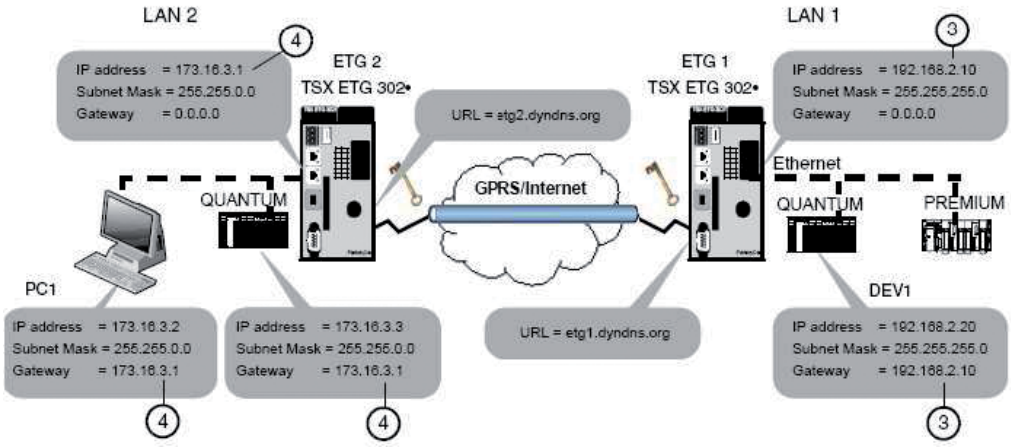
- общий ключ используется для проверки подлинности;
- для устройств PlantStruxure, всегда используйте туннельный режим доступа (обязательно);
- используйте шифрование 3DES с режимом высокий защиты и аутентификацию шифрования SHA-2.

Необходимо включить VPN на обоих ETG302x и настроить удаленный доступ в каждом из них.



После выбора режима VPN на двух ETG, настройте IP-адреса GPRS и режим туннеля.

Legend	Parameter	Settings
1	ETG1 GPRS IP address	etg1.dyndns.org (use dyndns address)
2	ETG2 GPRS IP address	etg2.dyndns.org (use dyndns address)
3	Ethernet address ETG1	192.168.2.10
4	Ethernet address ETG2	173.16.3.1
5	ETG1 & ETG2 VPN authentication	Preshared key
6	ETG1 & 2 VPN mode	Tunnel
7	Remote LAN (ETG1 side)	173.16.*.* or 173.16.0.0 + subnet mask
8	Remote LAN (ETG2 side)	192.168.2.* or 192.168.2.0 + subnet mask



3.5. Сегментация сети

Сегментация сети представляет собой разделения сети на подсети с целью повышения производительности и усиления безопасности. Сегментация может быть выполнена с помощью специальных устройств, таких как брандмауэры, маршрутизаторы и Ethernet-коммутаторы со списками контроля доступа.

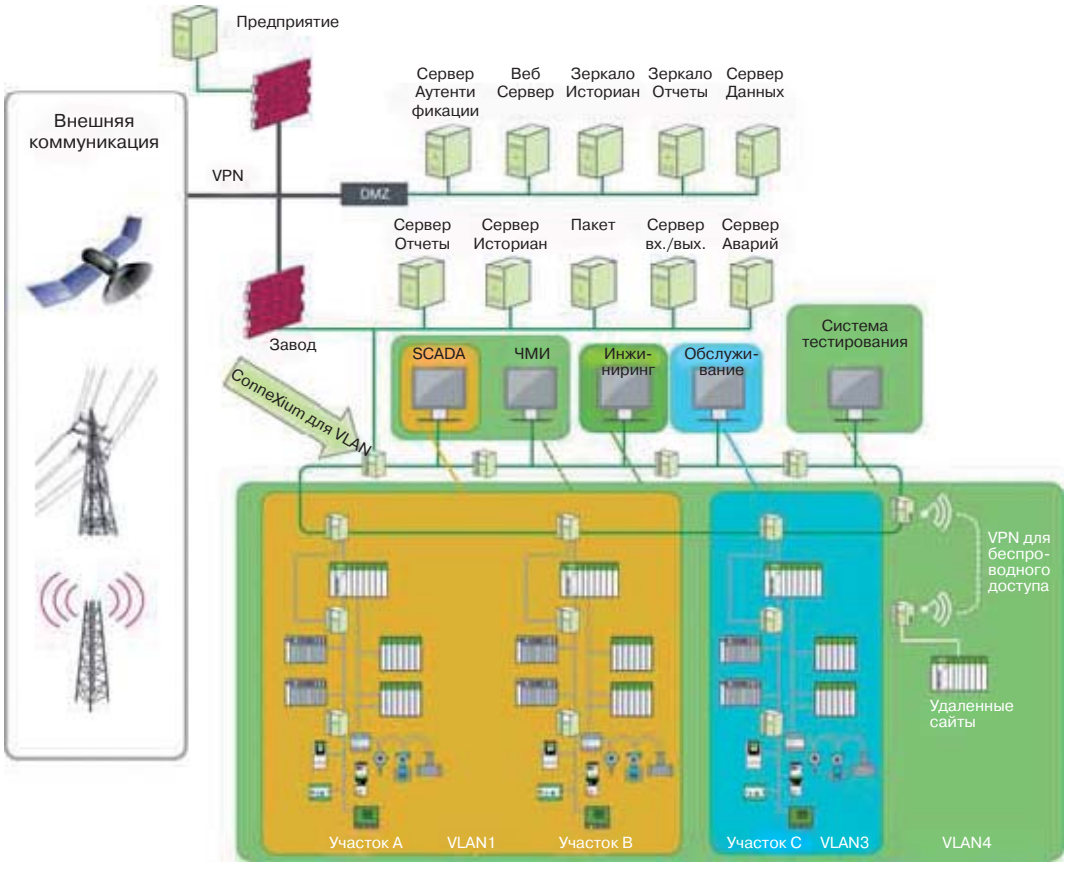
Преимущества сегментации сети:

- вредоносное содержимое трафика (вирусы, черви, трояны, спам, рекламное ПО) проникает только в один сегмент одной сети;
- улучшение безопасности поскольку узлы не видны из несанкционированных для доступа сетей;
- большинство злоумышленников сканируют сети вглубь по иерархии, прежде чем они выберут систему для атаки;
- предотвращение утечки информации, если есть нарушения безопасности в сети.
- передача информации в широковещательном режиме и рассылки нескольким пользователям ограничены только соответствующими сетями VLAN;
- повышение производительности сети и уменьшение нагрузки на сеть.

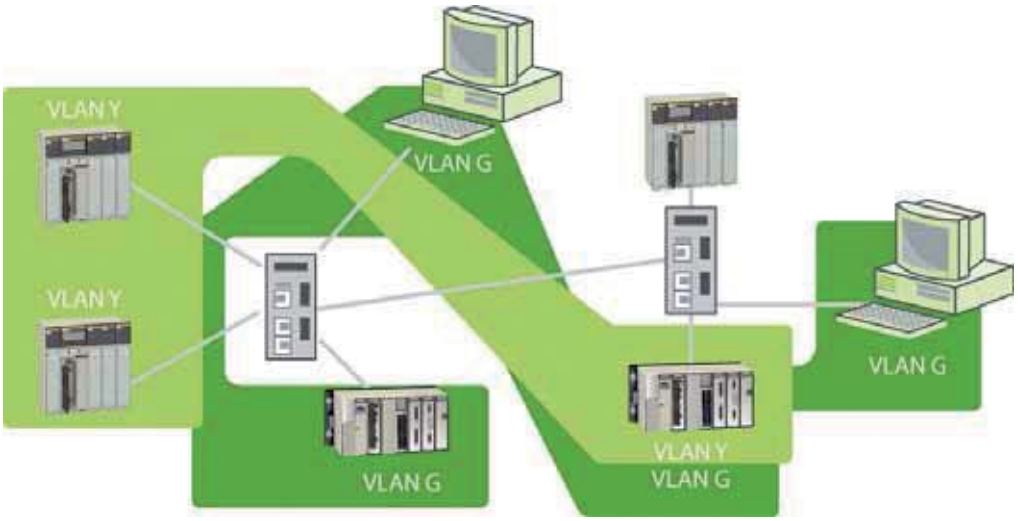
Для сетей системы управления рекомендуется применение коммутаторов Ethernet из-за более высокой производительности и большей, чем маршрутизаторы эффективности. Однако, маршрутизаторы, которые имеют поддержку VLAN, являются более безопасными из-за способности обеспечить контроль прав доступа, но эти устройства привносят задержку при передаче данных, что может быть недостатком. Тестирование производительности всегда должно быть проведено до начала использования.

3.5.1. VLAN

Виртуальные локальные сети (VLAN) обычно используются для сегментации сети. VLAN разделяет физическую сеть на меньшие логические сети для повышения производительности, улучшения управляемости, упрощения проектирования сетей и обеспечения дополнительного уровня безопасности.



VLAN - это широковещательный домен (уровня 2), настроенный при помощи коммутаторов Ethernet, работающий по принципу передачи Порт-в-Порт, которая изолирует трафик от других сетей VLAN. Когда два устройства назначены для работы на той же сети VLAN, коммутатор передает сообщения из одной сети в другую без каких-либо ограничений.



VLAN обычно сгруппированы по следующим принципам:

- функциональность или заданная ячейка: только конкретный трафик для конкретной ячейки, принимается для обработки;
- требования типа доступа: тип доступа различается для различных типов пользователей: операторов, инженеров, поставщиков, бухгалтеров ...;
- трафик: предельной уровень трафика для достижения требуемой производительности.

Рекомендации по сегментации

- • Используйте один VLAN на кольцевой топологии для всех устройств, генерирующих технологический трафик в производственном сегменте.
- • VoIP должны быть на отдельных VLAN.
- • Пакеты, поступающие в DMZ из Интернет, назначены для ограниченного доступа с идентификатором VLAN, который позволяет получить доступ только к устройствам, назначенным для DMZ.
- • Весь ненужный трафик должен быть удален из передачи внутри конкретного VLAN.
- • Применять QoS ACL, чтобы ограничить максимальное количество разрешенного трафика.
- • Предотвращение всех Telnet соединений и разрешение только SSH сессий.
- • Подключение ненадежных устройств к ненадежным портам, а доверенных устройств к доверенным портам.
- • Отключение неиспользуемых портов и назначение их в одну неиспользуемую VLAN.

Уязвимости VLAN

VLAN Hopping - это метод атаки сетевых ресурсов на VLAN. Смысл атаки заключается в том, что злоумышленник может получить доступ к другому устройству в сети не из своего VLAN. При использовании VLAN Hopping злоумышленник может использовать "спуфинг" (подмену) кадров или дважды инкапсулированные кадры для доступа на несанкционированный порт, чтобы получить доступ к другому VLAN.

Наиболее распространенными типами атаки для получение доступа к желаемой VLAN :

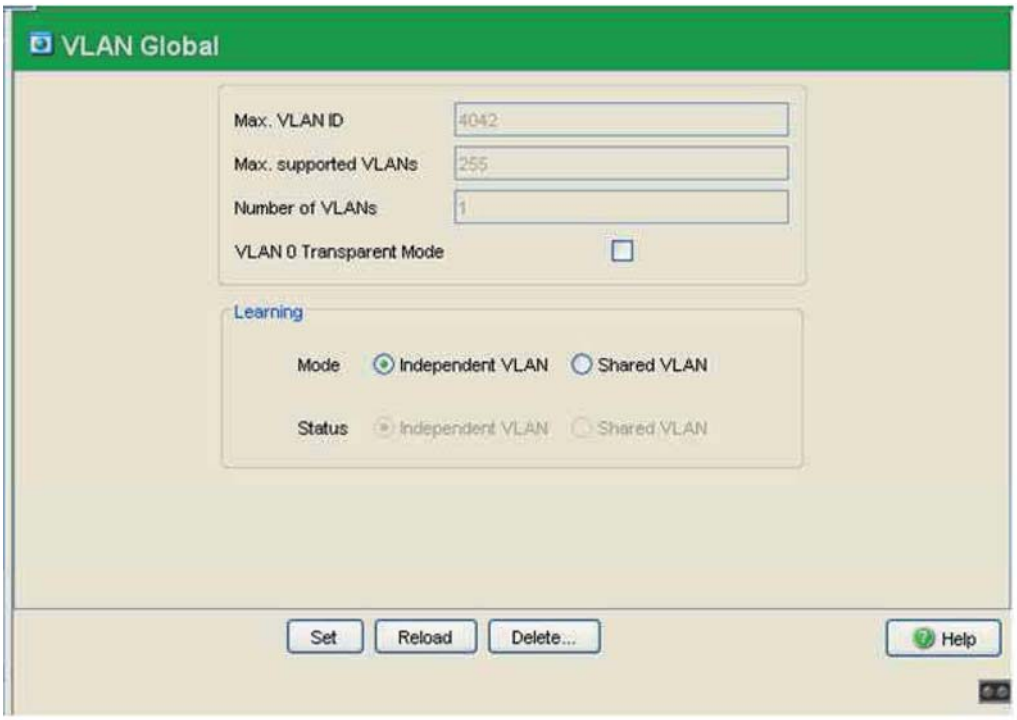
- ・атаки типа MAC flooding (внутри VLAN);
- ・атаки тегирования ISL и 802.1Q;
- ・VLAN атаки типа Double-Encapsulated 802.1Q;
- ・ARP атаки;
- ・атаки закрытых сетей VLAN;
- ・атаки перебором (Multicast Brute Force Attack);
- ・атаки Spanning-Tree;
- ・стресс атака случайными запросами (Random Frame Stress Attack).

Снижение риска VLAN

Возможности ConneXium по организации VLAN позволяют ограничить доступ по областям / зонам ответственности.

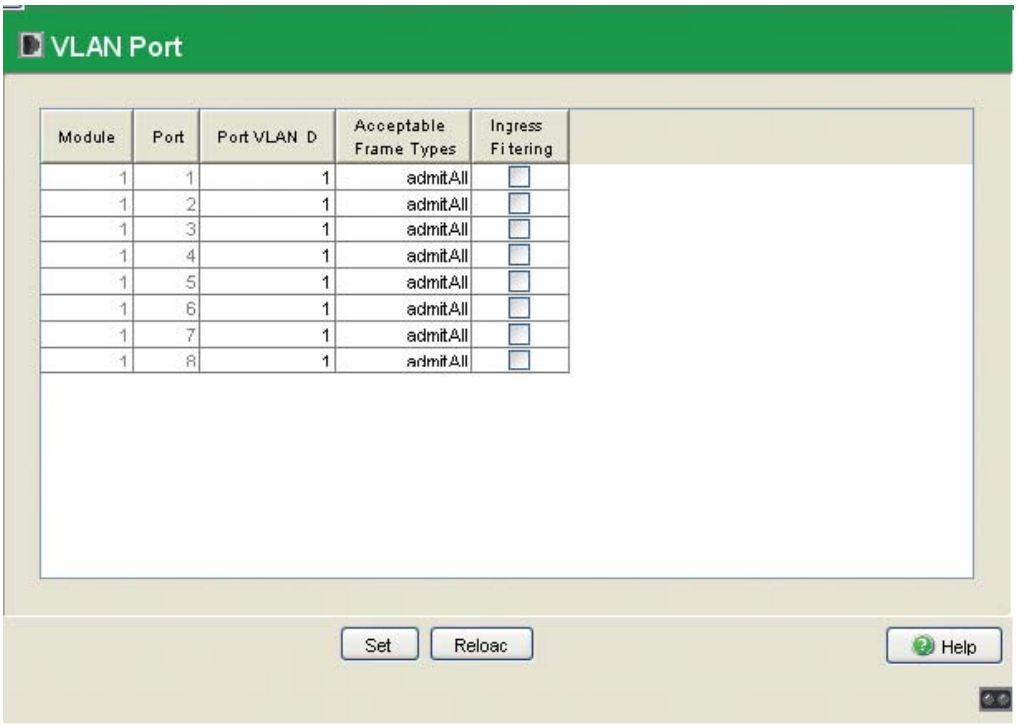
Например, инженер имеет доступ к сети всего завода, но оператор, отвечающий за сайт A & B не должен иметь доступ к сайту C. Обслуживающий персонал сайта C должен иметь доступ только к этому сайту. Это ограничивает области уязвимости.

Будьте осторожны при настройке VLAN 0 с прозрачным режимом доступа. Если отмечен этот режим доступа, то пакеты посылаются без проверки принадлежности VLAN.

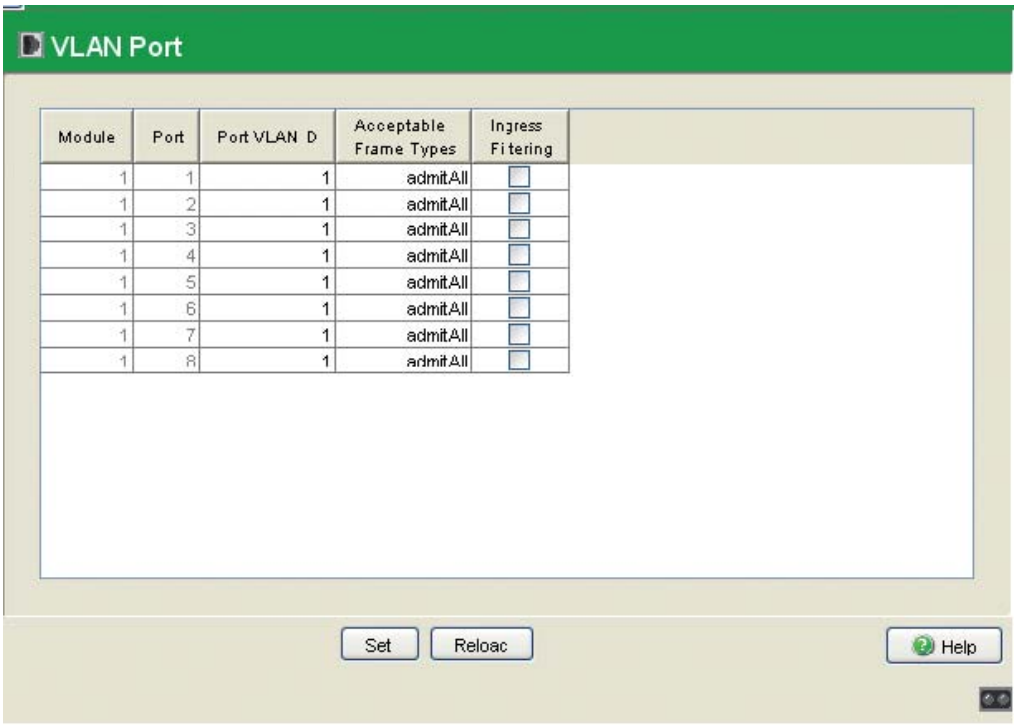


- Настройте порты коммутаторов на прием только маркированных пакетов и игнорирование всех немаркированных пакетов.

Замечание: Неиспользуемые порты должны быть отключены и помещены в неиспользуемую VLAN.

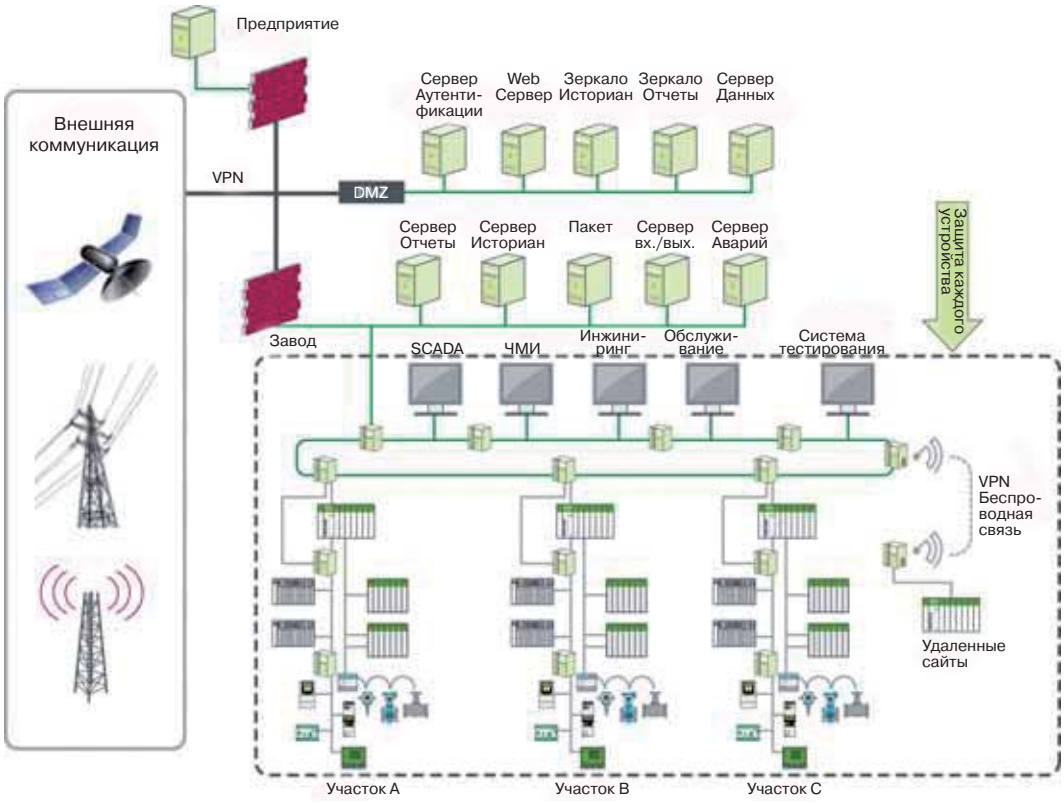


- Используйте фильтрацию на входе для проверки, что входящие пакеты являются законными.



3.6. "Повышение защищенности устройств" (Device Hardening)

Device hardening - это процесс, который позволяет перенастроить устройства из конфигураций по умолчанию в конфигурации с усиленной безопасностью.



Device hardening применяется для усиления защиты маршрутизаторов, межсетевых экранов, коммутаторов и других устройств в сети, таких как SCADA и PAC. Примеры применения усиления защиты:

- управление паролями, включая шифрование;
- отключение неиспользуемых служб;
- контроль доступа;
- сетевая система обнаружения вторжений NIDS (Network intrusion detection systems);
- строгая аутентификация.

В следующем разделе будет продемонстрировать методы упрочнения устройств Schneider Electric.

3.6.1. Пароли

Управление паролями является одним из основных средств Device Hardening, которое можно легко и быстро реализовать, но оно часто игнорируется в сетях систем управления. Политики и процедуры часто не описаны или отсутствует полностью. Необходимо обратить внимание на рассмотрение требований безопасности с оценкой потенциальных последствий (например, производительность, безопасность и надежность должны рассматриваться совместно с учетом их взаимного влияния).

Руководство по конфигурированию паролей

- Пароли, установленные по умолчанию, должны быть изменены сразу после установки ПО:
  - пароли пользователя;
  - прикладные пароли;
  - скрипты & исходный код;
  - оборудование управления сетью.
- Все учетные записи пользователей должны иметь пароли.
- Ограничить срок действия паролей для пользователей, которым необходим доступ.
- Пароли не должны быть легко угадываемыми или общепринятыми.
- Пароль должен содержать не менее 8 символов и содержать:
  - заглавные или строчные буквы английского алфавита (например: A, B, c, d);
  - числа (например: 1, 2, 3);
  - не буквенно-цифровые символы (например: !, $, #, %).
- Пароли должны регулярно меняться.
- Удалить доступ к учетной записи сотрудника, когда его работа прекращена.
- Используйте разные пароли для различных учетных записей, системных служб и приложений.
- Должны быть организованы универсальные пароли для всех служб и пользователей, которые могут быть быстро использованы в случае чрезвычайной ситуации и доступны в каждый момент времени для всех систем на заводе, при этом должна поддерживаться их безопасность.
- Применение паролей должно быть реализовано должным образом, никогда не мешать оператору, оперативно реагировать на ситуацию (например, возможность нажать аварийный выключатель).
- Пароли не должны передаваться в открытом виде по незащищенным каналам Интернет, например по электронной почте.

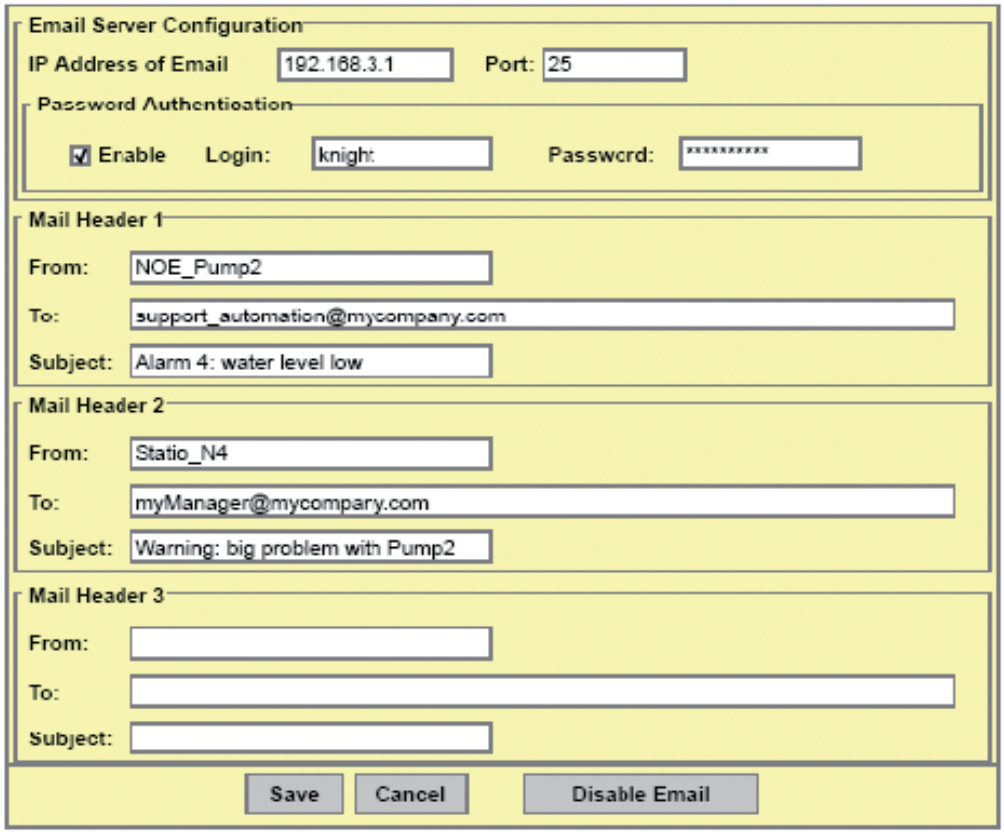
Уязвимости паролей

- Такие данные, как пароли и номера телефонов для удаленного доступа хранятся на незащищенных или портативных устройствах, которые могут быть потеряны или украдены.
- Отсутствие адекватной политики паролей, которая определяет, когда пароли должны быть использованы и степени секретности паролей.
- Нет назначения пароля для предотвращения несанкционированного доступа.
- Пароли не храниться в тайне и часто используются общие пароли или пароль размещается рядом с компьютером.
- Отправка паролей в не шифрованном виде через открытые каналы связи (например, FTP, SMTP …).
- Плохо настроенный пароль позволяет легко его угадать.
- Некорректная настойка привилегий может дать операторам административные привилегии или не позволить оператору запустить корректирующие действий в системе управления в чрезвычайной ситуации.
- Плохо выбранный пароль может быть легко разгадан человеком или компьютером.
- Пароли, назначенные по умолчанию, не были изменены и настройки по умолчанию можно легко найти в руководствах пользователя.

Снижению риска в вопросах задания паролей

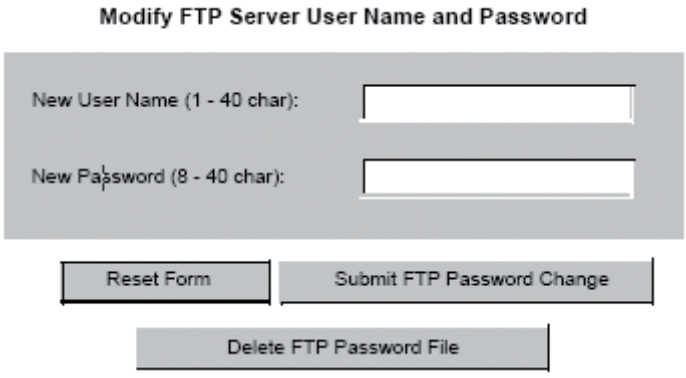
1. SMTP – Email Server

Включите проверку пароля на всех почтовых сервисах: NOE, ETY...



2. FTP

Измените пароль по умолчанию на сервере FTP. Смотрите Приложение A для устройств со службами FTP.



3.6.2. Управление контролем доступа

Один из способов «Повышения защищенности устройства»(Device Hardening) для устройств Schneider Electric является осуществление контроля доступа. Контроль доступа, аналогичен IP-фильтрации пакетов на брандмауэре, только разрешает доступ к адресам, заданным в таблице доступа. Это полезно для предотвращения доступа из одной системы завода одной зоны в другую систему другой зоны.

Руководящие принципы управления доступом

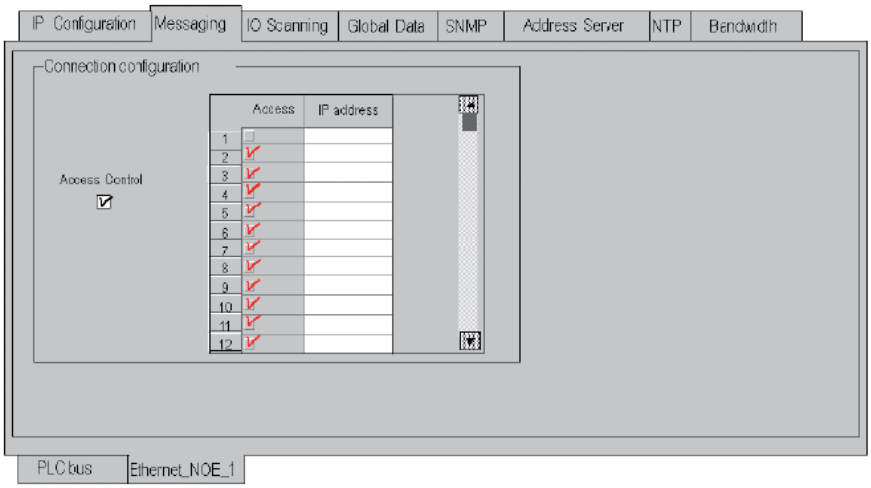
- Контроль доступа должен осуществляться на всех уровнях системы: межсетевой экран, коммутаторы и устройства.

Уязвимости при управлении доступом

- Доступ к логике PAC, что может оказать негативное влияние на производство, оборудование и безопасность персонала.

Снижение риска при контроле доступа

По возможности, настраивайте управление доступом, независимо от того, имеет ли право устройство открывать TCP соединение с модулем или нет:



3.6.3. Коммутаторы Ethernet серии ConneXium

Для упрочнения сети системы управления и для обеспечения дополнительной защиты от несанкционированного доступа необходимо, чтобы были запрограммированы следующие особенности управляемых коммутаторов Ethernet серии ConneXium:

- SNMP;
- доступ через (Telnet/Веб интерфейс);
- программная защита при помощи настроек в разделе Ethernet Switch Configurator;
- контроль доступа портов через IP или MAC-адрес.

SNMP

Станция управления сетью общается с устройствами через простой протокол управления сетью (Simple Network Management Protocol (SNMP)). Пакет SNMP содержит IP-адрес компьютера-отправителя вместе с паролем устройства, необходимым для доступа.

Устройство получает пакет SNMP и сравнивает IP-адрес компьютера-отправителя и пароль с записью в своем MIB файле. Если пароль имеет соответствующие права доступа, и, если IP-адрес компьютера-отправителя тоже разрешен для доступа, то устройство разрешит доступ.

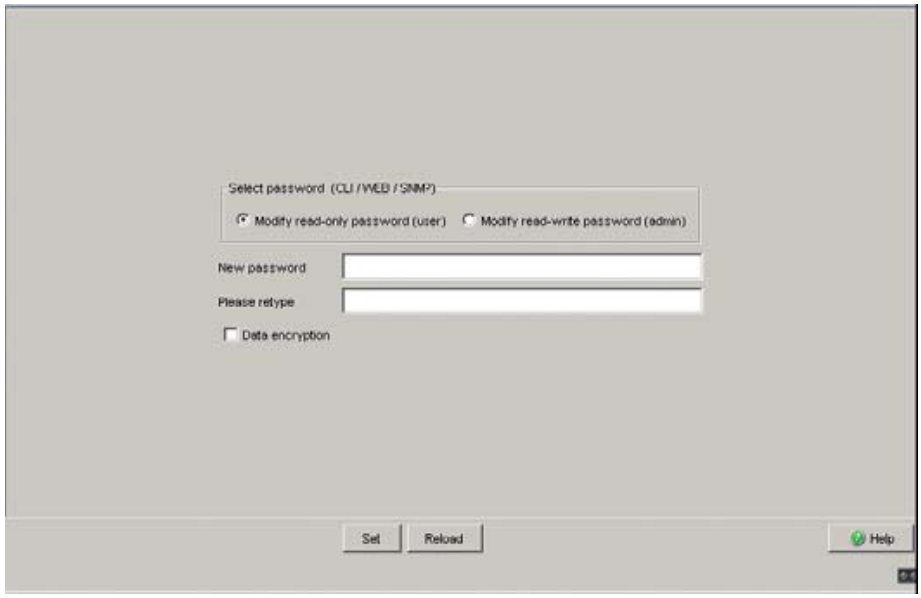
В настройках по умолчанию, устройства разрешают доступ при помощи общего открытого пароля в раздел Public «общий» с доступом (только чтение) и Private «частного» пароля с доступом (чтение и запись) к каждому компьютеру.

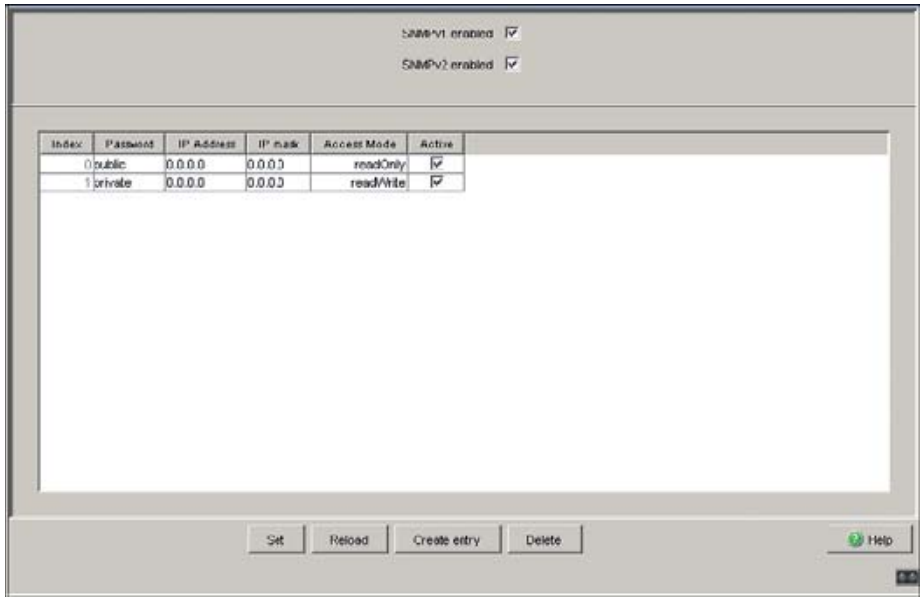
1. Уязвимости SNMP.

Коммутаторы Ethernet восприимчивы к "спуфингу" (подмене) MAC-адресов, переполнению таблиц, и нападениям типа spanning tree protocols, в зависимости от типа устройства и его конфигурации.

2. Снижение риска SNMP

- Использование SNMP v3, если возможно.
- Защита паролями.
- Ограничение срока действия прав доступа на пароли или удаление их устаревших значений.





Доступ через Telnet/Веб-интерфейс

Сервер Telnet, встроенный в устройства, позволяет настроить устройство с помощью интерфейса командной строки (в рамках заданного диапазона).

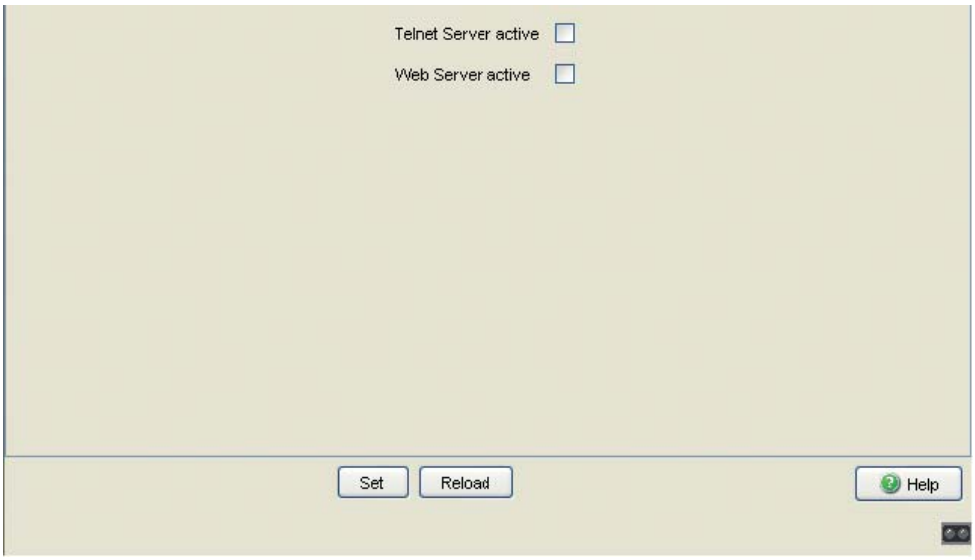
Коммутаторы ConneXium можно настроить при помощи веб-сервера. При поставке оборудования сервер активирован.

1. Уязвимости при доступе через Telnet/Веб интерфейс

Те же уязвимости, что и описанные в разделе о межсетевом экране.

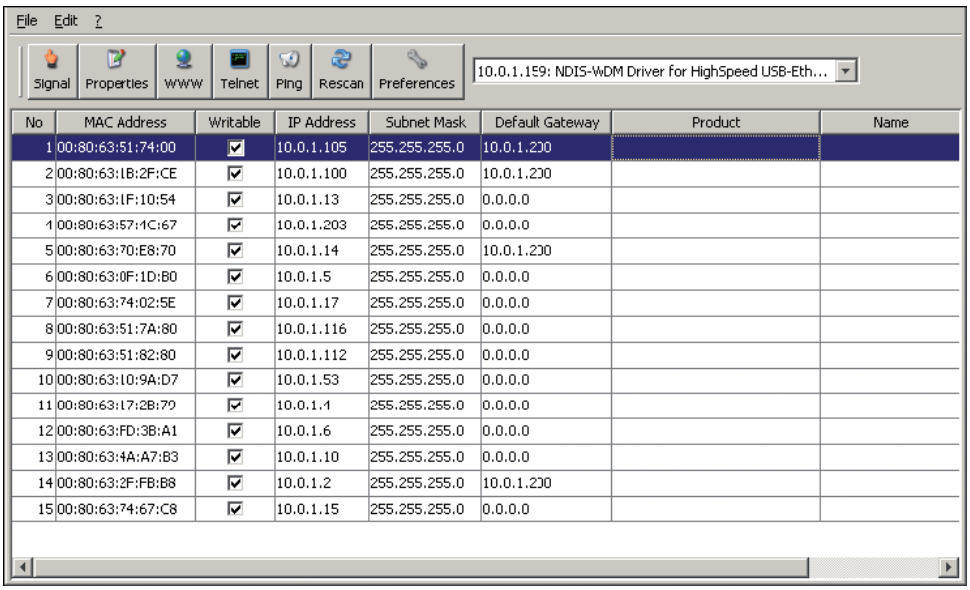
2. Рекомендации по конфигурированию Telnet/Веб интерфейса

- Отключите Telnet и доступ через веб-сервер, если они не используются.



Программная защита с помощью настроек в разделе Ethernet Switch Configurator

Настройки в разделе Ethernet Switch Configurator позволяют назначить устройству IP-адрес на основе его MAC-адреса. ПО Ethernet Switch Configurator работает на уровне 2.



No	MAC Address	Writable	IP Address	Subnet Mask	Default Gateway	Product	Name
1	00:80:63:51:74:00	☑	10.0.1.105	255.255.255.0	10.0.1.200		
2	00:80:63:1B:2F:CE	☑	10.0.1.100	255.255.255.0	10.0.1.200		
3	00:80:63:1F:10:54	☑	10.0.1.13	255.255.255.0	0.0.0.0		
4	00:80:63:57:1C:67	☑	10.0.1.203	255.255.255.0	0.0.0.0		
5	00:80:63:70:E8:70	☑	10.0.1.14	255.255.255.0	10.0.1.200		
6	00:80:63:0F:1D:B0	☑	10.0.1.5	255.255.255.0	0.0.0.0		
7	00:80:63:74:02:5E	☑	10.0.1.17	255.255.255.0	0.0.0.0		
8	00:80:63:51:7A:80	☑	10.0.1.116	255.255.255.0	0.0.0.0		
9	00:80:63:51:82:80	☑	10.0.1.112	255.255.255.0	0.0.0.0		
10	00:80:63:10:9A:D7	☑	10.0.1.53	255.255.255.0	0.0.0.0		
11	00:80:63:17:2B:79	☑	10.0.1.4	255.255.255.0	0.0.0.0		
12	00:80:63:FD:3B:A1	☑	10.0.1.6	255.255.255.0	0.0.0.0		
13	00:80:63:4A:A7:B3	☑	10.0.1.10	255.255.255.0	0.0.0.0		
14	00:80:63:2F:FB:B8	☑	10.0.1.2	255.255.255.0	10.0.1.200		
15	00:80:63:74:67:C8	☑	10.0.1.15	255.255.255.0	0.0.0.0		

1. Уязвимости настройки в разделе Ethernet Switch Configurator

Несанкционированный доступ.

2. Снижение риска настройки в разделе Ethernet Switch Configurator

Рекомендуется запретить работу Ethernet Switch Configurator после назначения IP-адресов устройствам.

- Отключите функционирование Ethernet Switch Configurator в "ПО конфигурирования Ethernet коммутаторов " или, по крайней мере, ограничить доступ до "только для чтения".

Доступ к портам коммутатора Ethernet

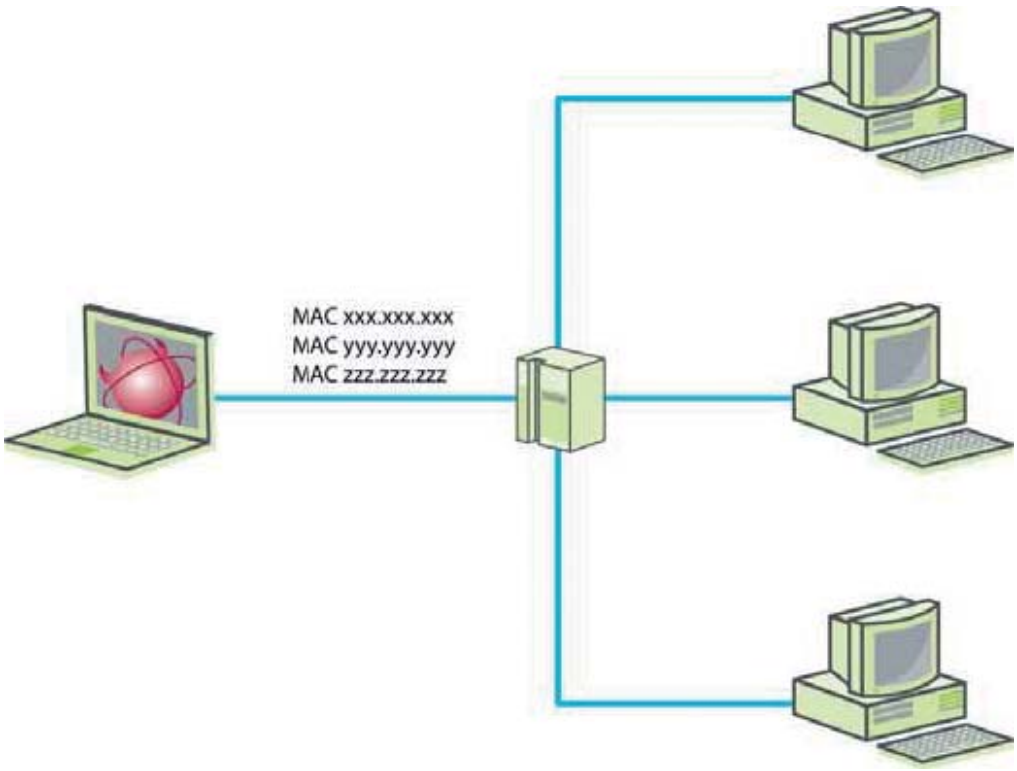
Используйте режимы безопасности портов для предотвращения несанкционированного физического подключения к портам Ethernet. Методы обеспечения безопасности портов:

- отключение открытых портов;
- блокировка MAC-адреса - блокирование конкретных MAC-адресов для доступа к конкретным портам коммутатора Ethernet;
- блокировка IP-адреса – блокирование доступа конкретного IP-адреса к определенному порту коммутатора Ethernet. Часто используется для замены неисправного устройства.

1. Уязвимости портов коммутаторов Ethernet

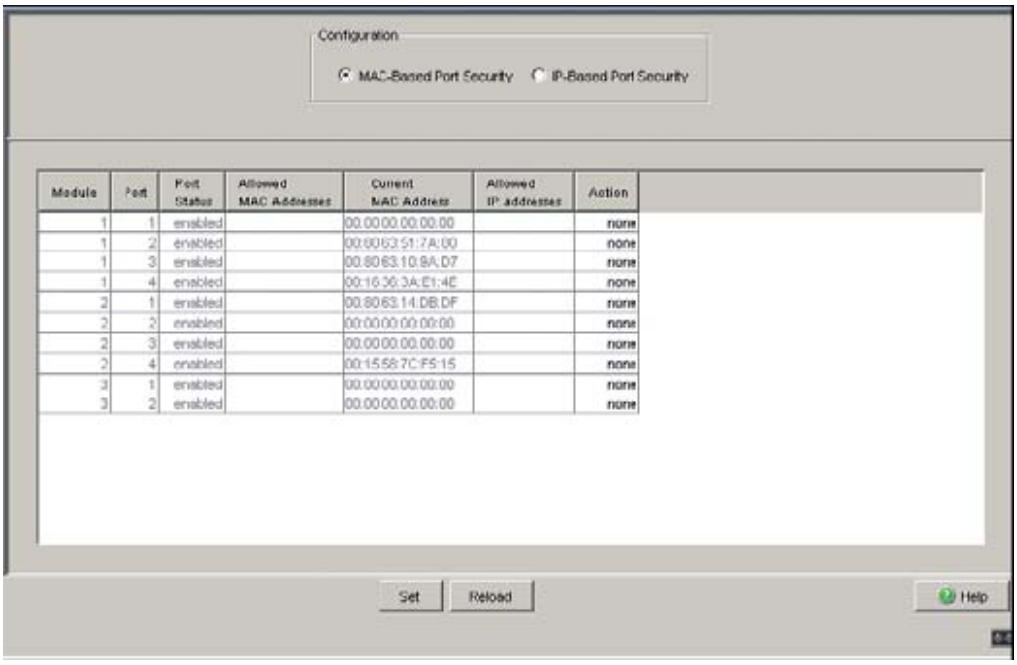
Злоумышленник, имеющий физический доступ к незакрытым портам сетевого коммутатора, может подключиться к сети за брандмауэром для того, чтобы обойти его фильтрацию на входящих каналах защиты.

Коммутаторы Ethernet хранят таблицы Content Address Memory (CAM), которые содержат списки отдельных MAC-адресов в сети, для которых открыт доступ к физическим портам на коммутаторах. В атаке типа MAC flooding злоумышленник посылает на коммутатор большое количество пакетов, каждый из которых содержит разные MAC-адреса источников, что приводит к переполнению таблицы CAM. После переполнения таблиц CAM, коммутатор Ethernet превращается в концентратор Ethernet и позволяет пересылать все входящие пакеты на все свои порты. Атакующий может использовать анализатор пакетов (например, Wireshark), чтобы захватить важные данные от других компьютеров (например, незашифрованные пароли, адреса электронной почты и мгновенные кадры обмена сообщениями в разговорах), пересылаемые в сети, которые не были бы доступны, если бы коммутатор работал в штатном режиме.



2. Рекомендации по конфигурированию доступа к портам

- Отключите неиспользуемые порты и разместите их на используемой VLAN.
- Ограничьте доступ к порту, разрешив только конкретным устройствам работать через него (до 10 устройств на каждый порт).



3.6.4. SCADA

SCADA является одним из наиболее уязвимых устройств в сети системы управления. Шаги, необходимые для упрочнения безопасности системы SCADA:

- ограничите видимые области при помощи настройки ролей;
- использование веб-клиентов вместо клиентов отображения с доступом через Интернет;
- используйте несколько цифровых подписей;
- тщательно настройте привилегии, которые бы не мешали работе процесса;
- используйте аутентификацию MS Windows.

Рекомендации для систем SCADA

- Регулярное отслеживание и контроль работы через аудит, особенно в критических областях для выявления подозрительной активности с целью немедленного устранения подозрительной деятельности.
- Настройка зеркальных серверов, таких как серверы истории в DMZ, предназначенные для внешнего доступа.

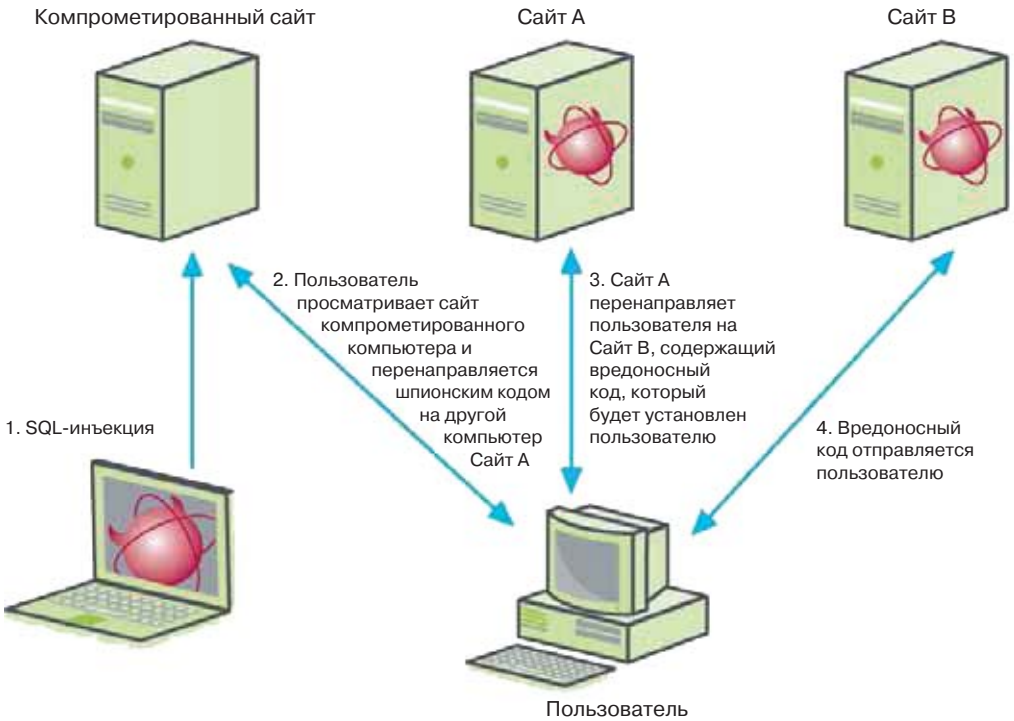
Не допускайте прямого доступа к сети системы управления.

- Периодическая проверка отсутствия сторонних адресов в списке доступа.
- Поддержка постоянной актуальности систем антивирусного программного обеспечения. Это может часто вступать в противоречие с производственными задачами и может потребовать проведения дополнительной оценки рисков.
- Поддержание паролей.
- Отсутствие доступа по электронной почте или веб-доступа.
- Отключение или удаление CD-ROM и дисковод.
- Отсутствие возможности удаленного доступа.
- Размещение системы в закрытых шкафах, если возможно.
- Рекомендуется применение двойных брандмауэров.

Уязвимости для систем SCADA

SQL-инъекция - это метод встраивания кода, помещаемого в базе данных на уровне приложения. Злоумышленник может выполнить несанкционированные команды SQL, воспользовавшись плохой организацией защиты доступа на системах, подключенных к Интернету. Большинство проблем безопасности концентрируются в области ввода строки Логин и адреса URL.

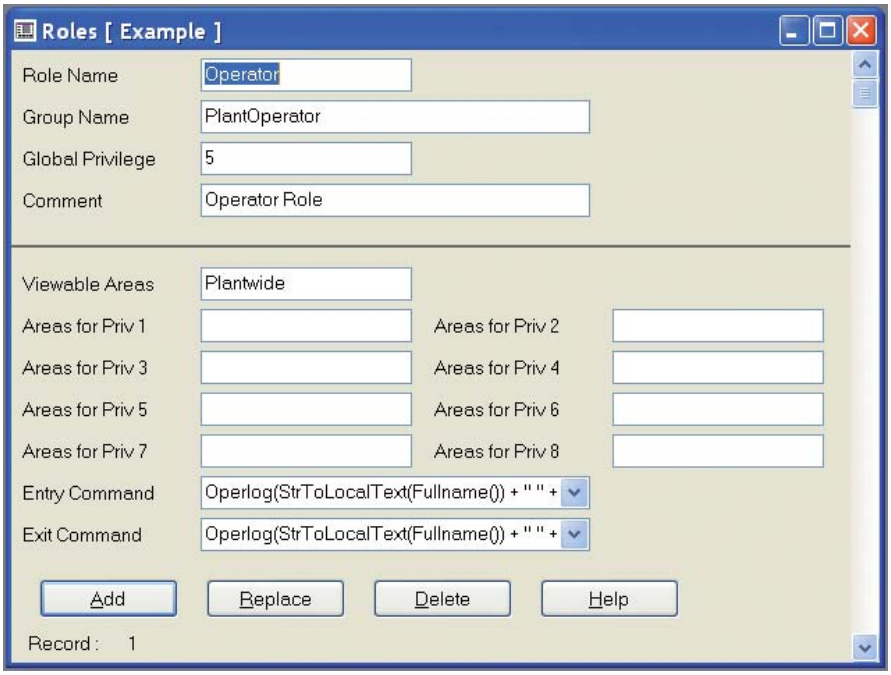
Атаки с SQL-инъекцией используются для кражи информации из баз данных и/или для получения доступа к головному компьютеру организации через компьютер, на котором размещается база данных.



Уменьшение риска для систем SCADA

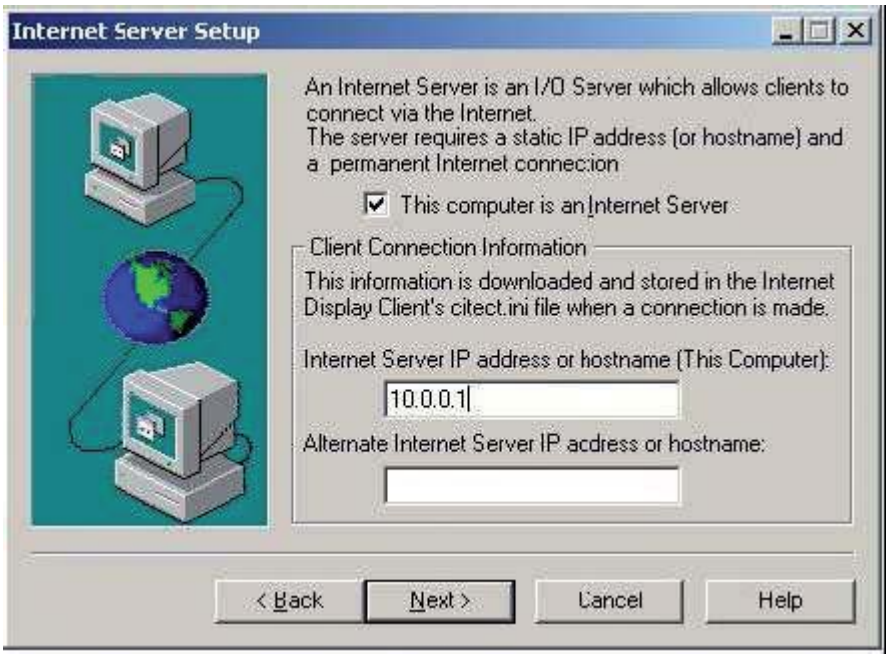
1. Назначение ролей

Ограничьте доступ к конкретному оборудованию завода для всех пользователей с целью предотвращения несанкционированного доступа к другим системам, не входящим в ответственность пользователя. Ограничение доступа обеспечивает дополнительный уровень безопасности. Если злоумышленник сможет проникнуть в систему, то его доступ будет ограничен конкретной областью и безопасен для других систем завода.



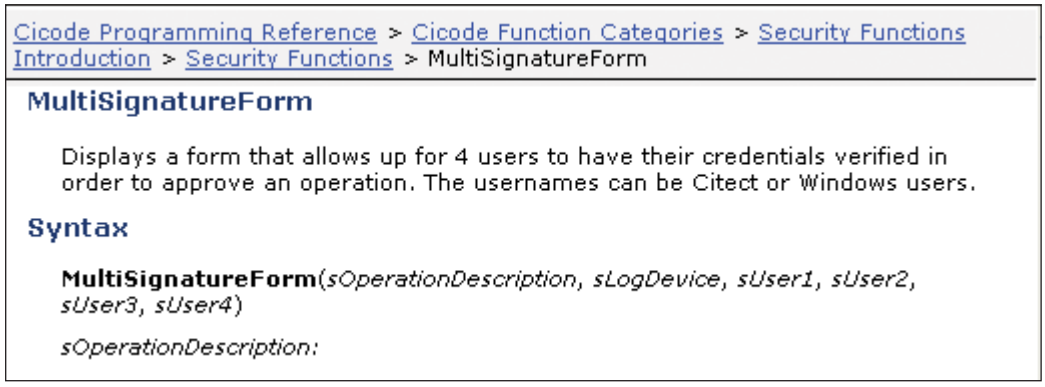
2. Веб-сервера

Интернет-клиенты отображения (Internet Display Client (IDC)) настраиваются с помощью FTP. Как было сказано выше, FTP является ненадежным протоколом, и его следует избегать. Настоятельно рекомендуется использовать веб-клиента CitectSCADA вместо IDC



3. Составная цифровая подпись

Всегда, когда возможно, рекомендуется использовать составные цифровые подписи. Это особенно важно для задач, требующих наивысшего уровня безопасности, например, для изменения порогов.



Cicode Programming Reference > Cicode Function Categories > Security Functions Introduction > Security Functions > MultiSignatureForm

MultiSignatureForm

Displays a form that allows up for 4 users to have their credentials verified in order to approve an operation. The usernames can be Citect or Windows users.

Syntax

MultiSignatureForm(*sOperationDescription, sLogDevice, sUser1, sUser2, sUser3, sUser4*)

sOperationDescription:

4. Мониторинг

В сетях систем управления крайне важен мониторинг безопасности. В мире не существует полностью защищенных систем, поскольку стратегии и методы кибер-атак постоянно совершенствуются. Если ведется мониторинг системы, то в случае попытки вторжения могут быть предприняты немедленные меры, которые могут предотвратить повреждения.

Существует несколько методов мониторинга сети с целью обнаружения подозрительной активности:

- мониторинг файлов регистрации;
- использование перехватов аутентификации;
- использование системы обнаружения вторжений IDS (Intruder Detection System).

Система обнаружения вторжений IDS отслеживает активность сети, например, модель трафика в сети передачи данных, доступ к файлам, изменения статуса порта, ввод неправильного пароля, обнаруженные неисправности оборудования и т.д.

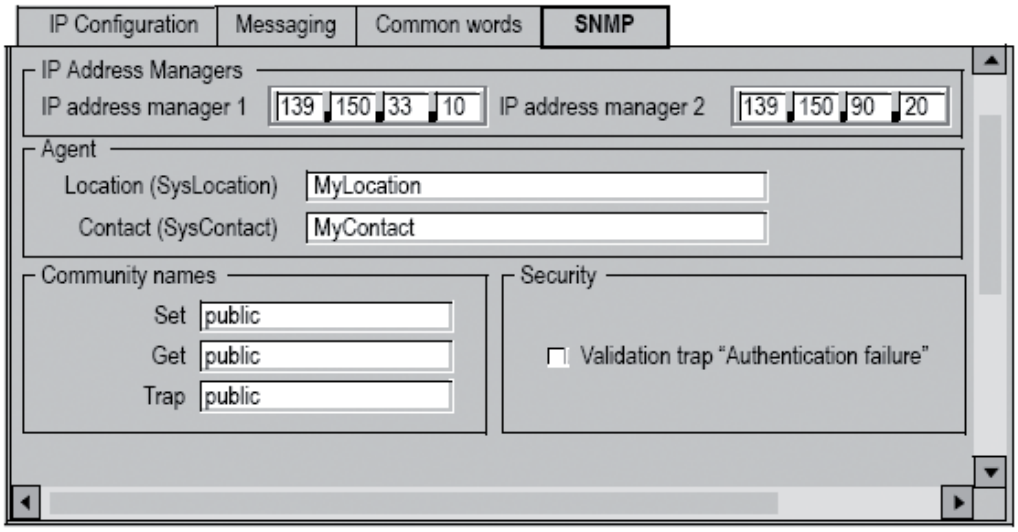
Существуют два типа систем IDS:

- сетевая система обнаружения вторжений NIDS (Network Intruder Detection System) отслеживает трафик от/до всех устройств сети;
- система обнаружения вторжений хоста HIDS (Host Intrusion Detection System) работают на отдельных хостах или устройствах сети.

4.1. Рекомендации по мониторингу

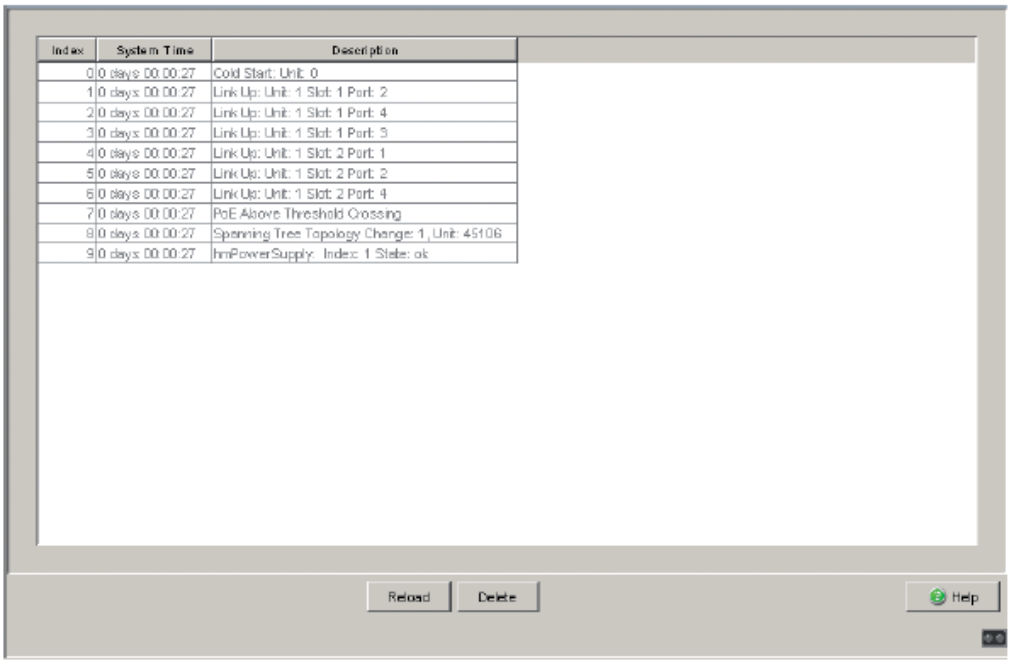
4.1.1. Перехват аутентификации

Разрешение перехвата аутентификации позволяет отслеживать попытки неавторизованной регистрации.

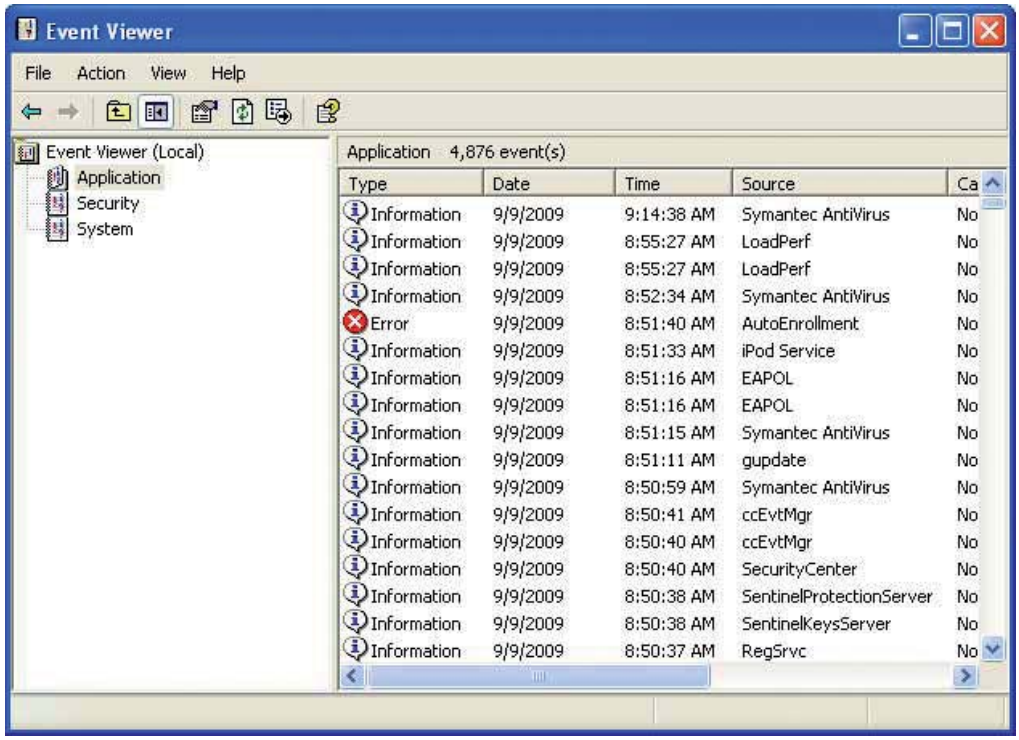


4.1.2. Отслеживание журнала событий

По журналу событий, который ведется на устройстве, можно обнаружить необычную активность.

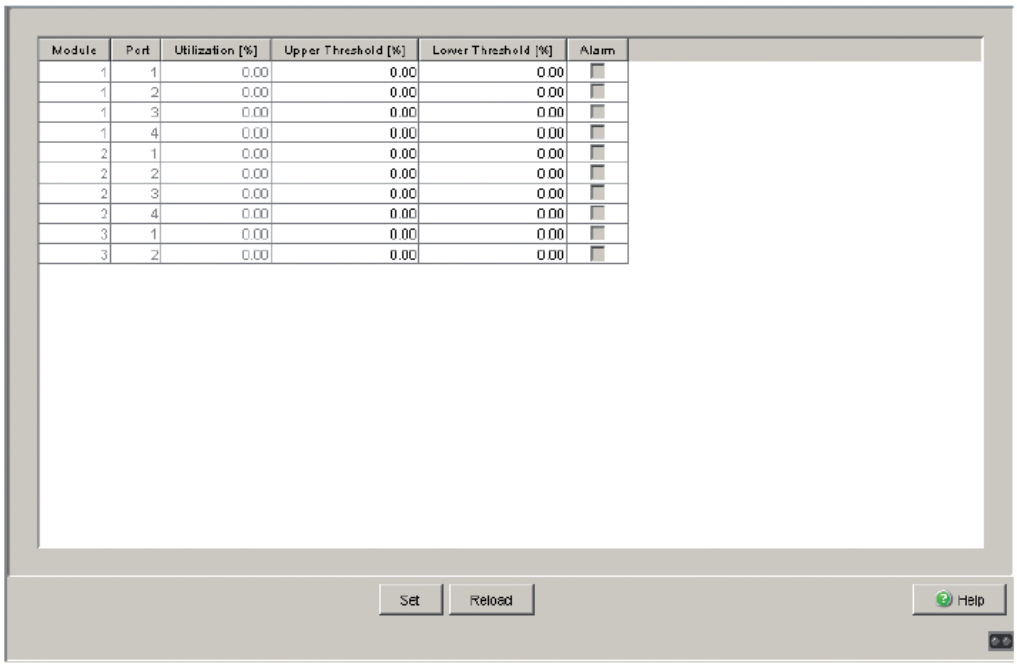


Для просмотра журнала событий с целью обнаружения необычной активности в MS Windows можно использовать программу Event Viewer (Control Panel/Administrative tools/ Event Viewer/Application Log).



4.1.3. Отслеживание нагрузки сети

Отслеживание нагрузки сети позволяет немедленно обнаружить необычный информационный трафик.



4.1.4. Отслеживание файлов регистрации устройства

Отслеживание файлов регистрации, которые ведет устройство. Например:

- файл регистрации отказов (например, Quantum PAC);
- файл регистрации аварийных ситуаций (например, PAC);
- диагностический файл регистрации (например, ConneXium Switch).

5. Приложение

5.1. Сервисы, поддерживаемые на оборудовании

Поддержка разных сетевых сервисов в ПЛК Quantum

SNMP

Устройство	SNMP(v1)	SNMP(v2)	SNMP(v3)	MIB-II	TFprivate-MIB
14OCPU65150	X	-	-	X	X
14OCPU65160	X	-	-	X	X
140CPU65260	X	-	-	X	X
140NOE77101	X	-	-	X	X
140NOE77111	X	-	-	X	X
140NWM10000	X	-	-	X	X

FTP

Устройство	Встроенное ПО	Веб-Файлы	Безопасность	Поддержка FDR
14QCPU65150	X	X	X	X
140CPUE5160	X	X	X	X
140CPU65260	X	X	X	X
140NOE77101	X	X	X	X
140NOE77111	X	X	X	X
140NWM10000	X	X	X	-

TFTP

Устройство	Поддержка FDR
14OCPU65150	X
140CPU65160	X
140CPU65260	X
140NOE77101	X
140NOE77111	X
140NWM10000	X

Telnet

Устройство	Конфигурация	Диагностика[1]	Безопасность	Уровень безопасности
14OCPU65150	-	X	X	X[2]
14OCPU65160	-	X	X	X[2]
140CPU65260	-	X	X	X[2]
140NOE77101	-	X	X	X[2]
140NOE77111	-	X	X	X[2]
140NWM10000	-	X	X	X[2]

[1] Предусмотрено только для использования на заводе изготовителе

[2] Несколько паролей

Поддержка разных сетевых сервисов в ПЛК Premium

SNMP

Устройство	SNMP(v1)	SNMP(v2)	SNMP(v3)	MIB-II	TFprivate-MIB
TSXP571634M	X	-	-	X	X
TSXP572634M	X	-	-	X	X
TSXP573634M	X	-	-	X	X
TSXP574634M	X	-	-	X	X
TSXP575634M	X	-	-	X	X
TSXP576634M	X	-	-	X	X
TSXETY4103	X	-	-	X	X
TSXETY110WS	X	-	-	X	X
TSXETY5103	X	-	-	X	X
TSXWMY100	X	-	-	X	X

FTP

Устройство	Встроенное ПО	Веб-Файлы	Безопасность	Поддержка FDR
TSXP571634M	X	X	X	X
TSXP572634M	X	X	X	X
TSXP573634M	X	X	X	X
TSXP574634M	X	X	X	X
TSXP575634M	X	X	X	X
TSXP576634M	X	X	X	X
TSXETY4103	X	X	X	X
TSXETY110WS	X	X	X	-
TSXETY5103	X	X	X	X
TSXWMY100	X	X	X	-

SNMP

Устройство	SNMP(v1)	SNMP(v2)	SNMP(v3)	MIB-II	TFprivate-MIB
TSXP571634M	X	-	-	X	X
TSXP572634M	X	-	-	X	X
TSXP573634M	X	-	-	X	X
TSXP574634M	X	-	-	X	X
TSXP575634M	X	-	-	X	X
TSXP576634M	X	-	-	X	X
TSXETY4103	X	-	-	X	X
TSXETY110WS	X	-	-	X	X
TSXETY5103	X	-	-	X	X
TSXWMY100	X	-	-	X	X

FTP

Устройство	Встроенное ПО	Веб-Файлы	Безопасность	Поддержка FDR
TSXP571634M	X	X	X	X
TSXP572634M	X	X	X	X
TSXP573634M	X	X	X	X
TSXP574634M	X	X	X	X
TSXP575634M	X	X	X	X
TSXP576634M	X	X	X	X
TSXETY4103	X	X	X	X
TSXETY110WS	X	X	X	-
TSXETY5103	X	X	X	X
TSXWMY100	X	X	X	-

Поддержка разных сетевых сервисов в ПЛК M340

SNMP	SNMP(v1)	SNMP(v2)	SNMP(v3)	MIB-II	TFprivate MIB
BMX NOE 01x0	x			x	x
BMX P34 2030/20302	x			x	x
BMX P34 2020	x			x	x
FTP	Firmware	Веб-Файлы	Безопас-ность	Поддержка FDR	
BMX NOE 0100	x	x		x	
BMX NOE 0110	x	x	x	x	
BMX P342020/2030/20302	x			x	
TFTP	Поддержка FDR				
BMX NOE 01x0	x				
BMX P342020/2030/20302	x				

Сетевые сервисы, поддерживаемые устройствами платформы TSX Micro

FTP

Устройство	Встроенное ПО	Веб-файлы	Безопасность	Поддержка FDR
TSXETZ410	X	X	X	X
TSXETZ510	X	X	X	X

Сетевые сервисы, поддерживаемые устройствами платформы Momentum

SNMP

Устройство	MIB-II	TFprivate-MIB
170ENT11001	X	X

FTP

Устройство	Конфигурация	Веб-файлы	Безопасность
170ENT11001	X	X	X

Telnet

Устройство	Конфигурация	Диагностика	Безопасность
171CCC96020	-	X	X
171CCC96030	-	X	X
171CCC98020	-	X	X
171CCC98030	-	X	X
170ENT11001	X	X	X

Сетевые сервисы, поддерживаемые устройствами платформы Advantys STB

SNMP

Устройство	SNMP(v1)	SNMP(v2)	SNMP(v3)	MIB-II	TFprivate-MIB
STBNIP2212	X	-	-	X	X

FTP

Устройство	Конфигурация	Веб-файлы	Безопасность
STBNIP2212	X	X	X

Сетевые сервисы, поддерживаемые устройствами платформы Advantys STB

SNMP

Устройство	SNMP(v1)	SNMP(v2)	SNMP(v3)	MIB-II	TFprivate-MIB
EGX200	X	-	-	X	-
EGX400	X	-	-	X	-

FTP

Устройство	Конфигурация	Веб-файлы	Безопасность
EGX200	-	X	X
EGX400	X	X	X

Сетевые сервисы, поддерживаемые устройствами платформы ConneXium

SNMP	SNMP(v1)	SNMP(v2)	SNMP(v3)	MIB-II
174CEV20040	x		x	x
TSXETG100	x		x	x
TCSESM*	x	x	x	x
FTP	Встроенное ПО	Веб-файлы	Безопасность	
174CEV20040	x	x	x	
TSXETG100	x	x	x	
TCSESM*		x	x	
TFTP	Поддержка FDR	Встроенное ПО		
174CEV20040	x	x		
TCSESM*	x			
Telnet	Конфигурация	Диагностика	Безопасность	
174CEV20040	x	x	x	
TCSESM*	x	x	x	

5.2. Общее описание методов атак

5.2.1 Подмена IP-адреса или IP "спуфинг" – IP Spoofing

IP "спуфинг" – это разновидность вторжения, при котором взломщик пытается замаскироваться под другую систему, используя ее IP-адрес, с целью выполнения злонамеренных действий, например, блокирование сервиса и человек на пути передачи данных. IP "спуфинг" выполняется путем манипулирования IP-адресом.

Протокол Интернет - IP (Internet Protocol) является основным протоколом, который используется для обменов данными через Интернет. Данные имеют IP-заголовок, который содержит информацию, необходимую для передачи данных отправителя получателю. Заголовок содержит информацию о типе дейтаграммы IP, о том, как долго дейтаграмма остается активной в сети, а также специальные флаги, показывающие специальные типы дейтаграммы и способы ее обслуживания, такие как разрешение фрагментирования данных, адреса отправителя и получателя и другие поля.

Получатель пакета информации может идентифицировать отправителя по его IP-адресу. Протокол IP не проверяет достоверность IP-адреса отправителя. При подмене IP-адреса, злоумышленник подделывает дейтаграмму. Чаще всего злоумышленник создает фальшивый IP-адреса отправителя.

Основными мотивами нападения являются:

- сбор информации об открытых портах, работе систем или приложений на хостах по их ответной реакции. Например: ответ порта 80 может означать, что на хосте работает веб-сервер. Используя протокол эмуляции терминала Telnet, злоумышленник может просмотреть баннер и определить версию и тип веб-сервера. Далее злоумышленник может попытаться использовать известные уязвимые места веб-сервера такого типа;
- обнаружение номера последовательности. Механизм TCP требует применения номера последовательности для каждого передаваемого байта и требует подтверждения от получателя. Злоумышленник посылает несколько пакетов данных жертве с целью раскрыть алгоритм номера последовательности. Когда алгоритм раскрыт, злоумышленник предпринимает попытку нападения на намеченную жертву.
- Получение авторизованной сессии связи, путем мониторинга сеанса связи между двумя хостами и затем запуск трафика, который выглядит, как исходящий от одного из хостов. Выполняя такие действия, злоумышленник похищает сессию одного хоста и прекращает сеанс связи между хостами. Злоумышленник продолжает аналогичный сеанс связи с аналогичными привилегиями доступа с другими легальными хостами.

5.2.2. Атаки типа DoS (отказ от сервиса)

Атаки типа DoS (отказ от сервиса) являются попыткой временно или постоянно предотвратить законным пользователям доступ к сервисным компьютерным программам. Общий метод нападения заключается в переполнении компьютера жертвы внешними запросами коммуникаций и блокировке ответов или сильному замедлению ответов, при этом система становится неэффективной. Злоумышленник достигает этого с помощью:

Шаг	Описание
1	Фатальный сбой системы.
2	Блокировка коммуникации между системами.
3	Вывод из строя системы или сети или значительное снижение скорости работы, влияющей на производительность системы.
4	Зависание системы, которое более опасно, чем фатальный сбой, поскольку нет автоматической перезагрузки. Производительность может быть значительно нарушена.

Существует несколько разновидностей атак типа DoS. Наиболее распространены следующие типы:

- синхронная Flood атака TCP SYN (TCP SYN Flood);
- Land attack;
- ARP Spoofing - ARP «спуфинг» - подмена ARP;
- атака ICMP smurf;
- the PING of Death - "Пинг смерти";
- атака UDP Flood;
- атака Teardrop.

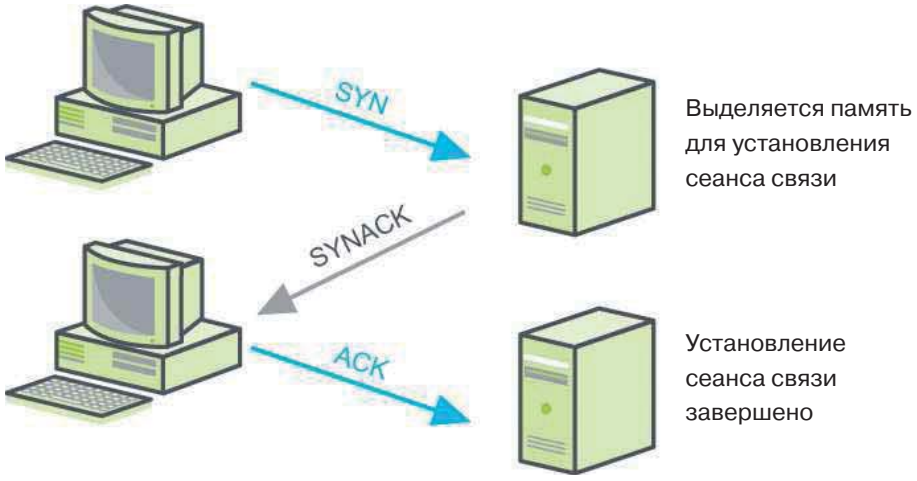
5.2.3. Синхронная Flood атака TCP SYN

Синхронная атака TCP SYN – это форма атаки типа DoS (отказ от сервиса), во время которой нападающий посылает последовательность запросов типа SYN в намеченную для атаки систему.

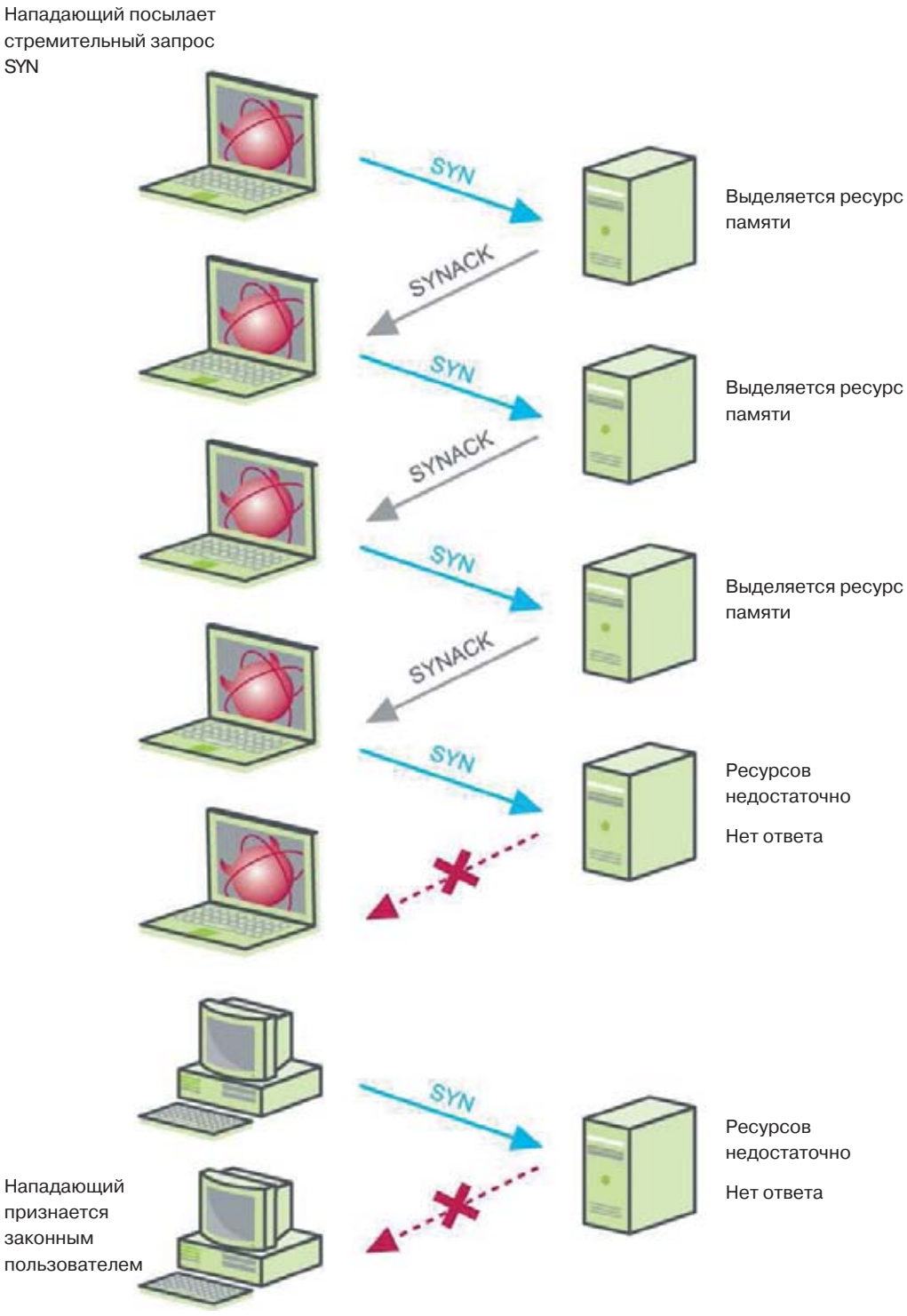
В ходе синхронной атаки TCP SYN, клиент пытается установить TCP-соединение с сервером, клиент и сервер обмениваются информацией в описанной ниже последовательности:

Шаг	Описание
1	Клиент запрашивает соединение, посылая сообщение SYN (синхронизация) серверу.
2	Сервер подтверждает запрос, посылая SYN-ACK клиенту.
3	Клиент отвечает сообщением ACK и соединение устанавливается.

Этот процесс называется трехэтапным установлением сеанса связи TCP.

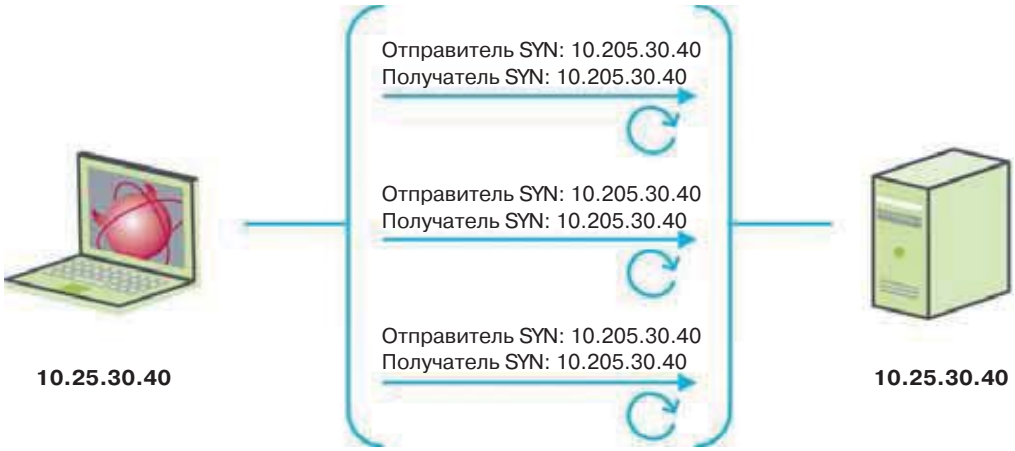


Существует ограничение по имеющимся в наличии ресурсам. Как только доступные ресурсы заканчиваются, все остальные запросы теряются. Устаревшие операционные системы более уязвимы, чем современные операционные системы. В современных операционных системах управление ресурсами организовано лучше, поэтому сложнее достичь переполнения таблиц выделения ресурсов, но, несмотря на это, они все равно остаются уязвимыми.



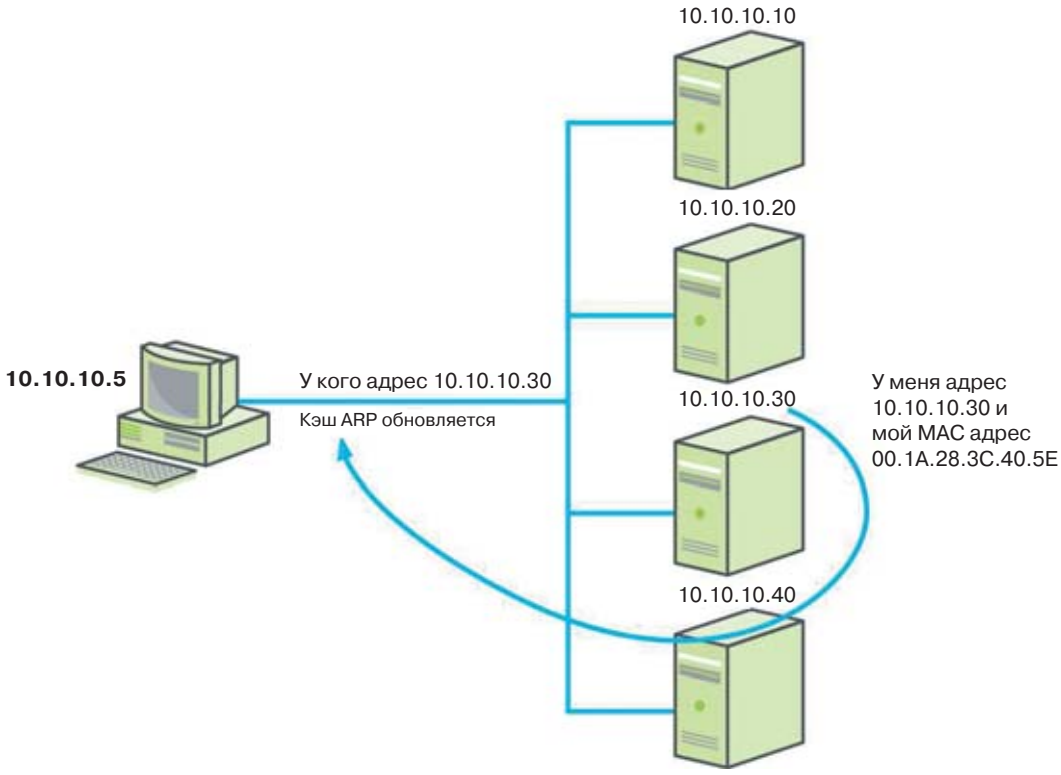
5.2.4. Land Attack

В случае Land Attack в систему посылается поддельный пакет TCP SYN, в котором IP-адрес и номер порта отправителя идентичны IP-адресу и номеру порта получателя. Система-получатель отвечает сама себе в бесконечном цикле до тех пор, пока не будет превышено значение тайм-аута.



5.2.5. ARP Spoofing - ARP «спуфинг» - подмена ARP)

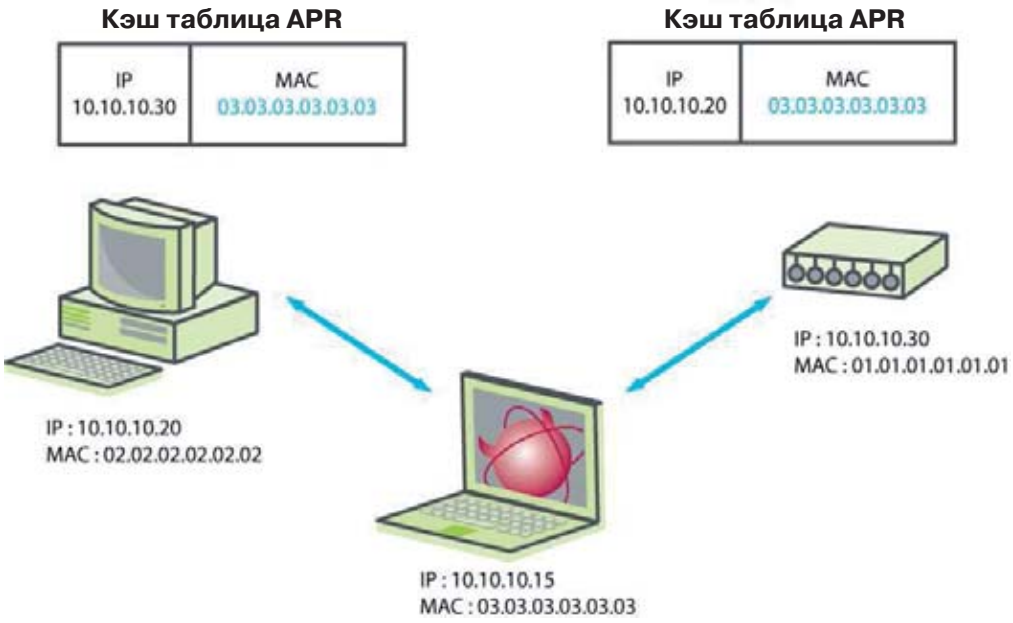
Протокол переопределения адресов ARP (Address Resolution Protocol) – это протокол второго уровня, который обеспечивает динамическое преобразование IP-адреса в аппаратный MAC-адрес, хранящийся в таблице соответствия (кэш-память ARP).



Шаг	Описание
1	Служба ARP проверяет локальный кэш ARP на наличие адреса станции назначения. Если соответствие найдено, то аппаратный адрес станции назначения добавляется в заголовок кадра и кадр отправляется.

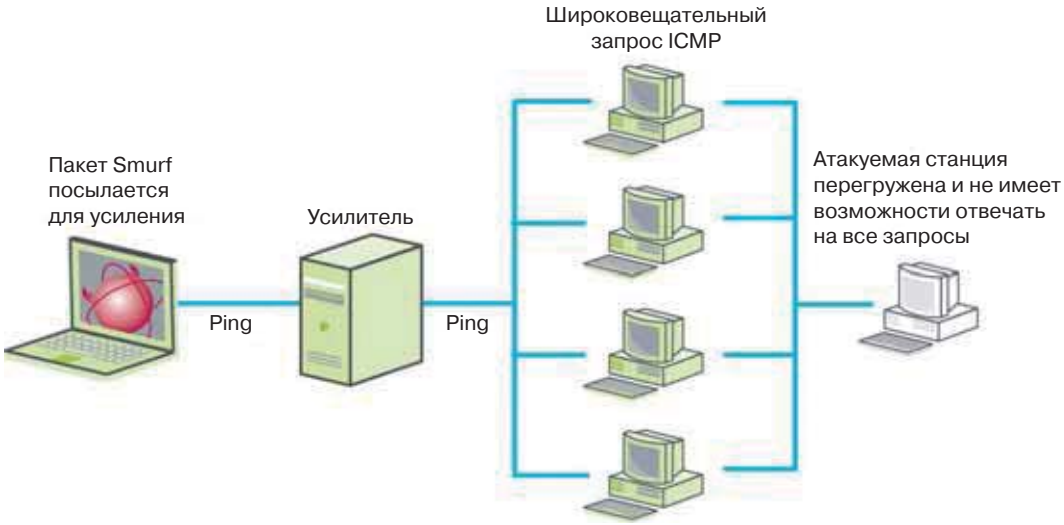
Шаг	Описание
2	Если соответствие не найдено, то служба ARP отправляет широковещательный запрос в локальную сеть (напоминание: служба знает, что разыскивается станция, размещенная на локальной сети, так как ей известен идентификатор сети из IP-адреса и маска подсети). Запрос ARP содержит текущий IP-адрес отправителя и разыскиваемый аппаратный адрес. Такой запрос отправляется на широковещательный адрес 255.255.255.255 (но он будет обработан на всех станциях).
3	Когда хост получателя получает широковещательный запрос, он посылает в ответ на этот ARP запрос свой ARP запрос, содержащий свой аппаратный адрес и свой текущий IP-адрес.
4	Когда источник получает ответ ARP, он обновляет свой ARP кэш, а затем создает кадр запроса и отправляет его получателю.

ARP flood spoofing или переполнение ARP «спуфинга», также известно, как отравление ARP или ARP маршрутизация, при этом посылаются поддельные ARP сообщения в сеть. Целью является ассоциирование MAC-адреса атакующего с другой станцией (например, адресом шлюза) это достигается путем отравления ARP кэш системы, чтобы перехватить трафик.



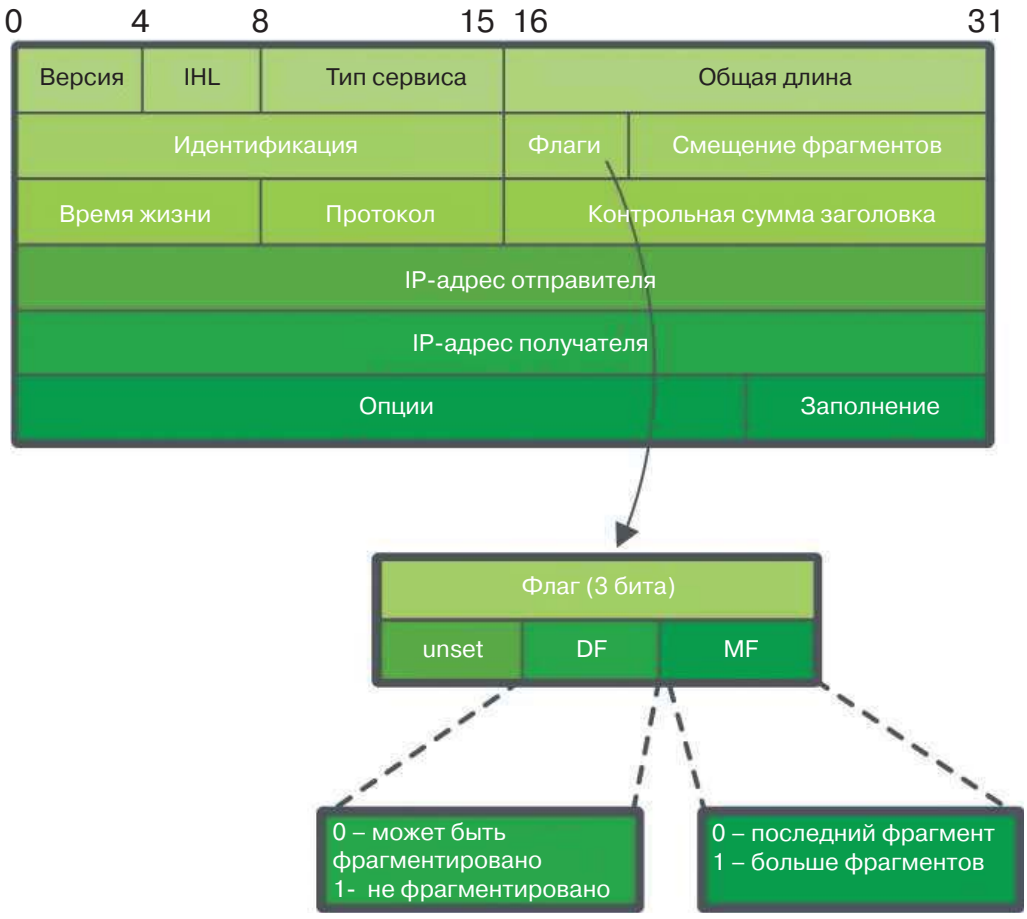
5.2.6. ICMP Smurf

В атаке Smurf злоумышленник подделывает IP-адрес станции назначения, отправляя ICMP эхо-запрос (ping) в широковещательном режиме по посреднической сети. В результате целевой хост будет наполнен ответами, при этом ресурсы будут исчерпаны, и законные пользователи не смогут получить доступ к серверу. Атаки ICMP Smurf аналогичны атакам ICMP Flood, однако Smurf-атаки использует другие сети для умножения количества запросов.



5.2.7. The PING of Death - "Пинг смерти"

Особенностью TCP/IP является обработка фрагментации в виде возможности обработки одного IP-пакета разделенного на более мелкие сегменты. При фрагментации, каждый фрагмент IP должен нести информацию о том, какие части исходного пакета IP в нем содержится. Эта информация хранится в поле «Смещение фрагмента» в заголовке IP.



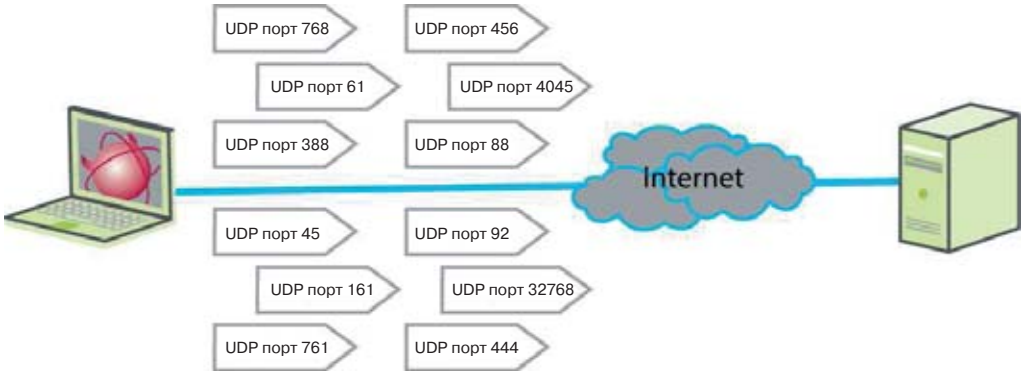
В случае атаки «Пинг смерти» посылается ICMP эхо-запрос (пинг) содержащий несколько фрагментированных пакетов, размер которых превышает максимальный размер пакета IP (63, 535 байт)

Поскольку полученный ICMP эхо-пакет больше, чем допустимый размер пакета IP, происходит сбои в удаленной системе при попытке собрать пакет.

5.2.8. Атака UDP Flood

Атака UDP Flood похожа на атаку ICMP flood. Разница в том, что используются UDP датаграммы различных размеров. При атаке UDP Flood злоумышленник отправляет пакет UDP к случайному порту в системе жертвы. Когда система жертвы получает пакет UDP, она проверяет, есть ли приложения, назначенное на работу с этим портом.

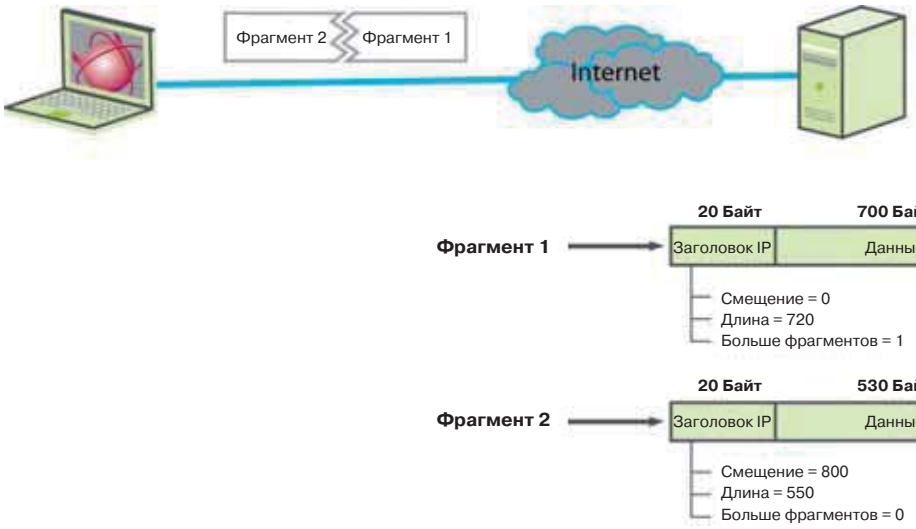
Если нет, то система отправляет пакет признака отсутствия соединения (ICMP Destination Unreachable) на недоступный поддельный IP-адрес. Если достаточное количество UDP пакетов успешно доставляются на достаточное большое количество портов жертвы, система выйдет из строя.



Основным мотивом UDP Flood атаки является не проникновение в систему, а попытка заставить систему отвергнуть корректный запрос подключения законного пользователя к конкретной службе.

5.2.9. Атака Teardrop

Атака Teardrop является наиболее популярным методом фрагментированной атаки. Она включает вставки ложной информации со смещением во фрагментированные пакеты. В результате, после сборки появляются пустые или перекрывающиеся фрагменты, которые могут привести систему к краху.



Основной мотивацией для атаки Teardrop является намерение заблокировать обработку или довести систему до аварии.

6. Глоссарий

Глоссарий терминов, используемых в документации по Безопасности и Обнаружению вторжений.

Этот словарь составлен на основе информации с сайта www.sans.org.

Для доступа к полному глоссарию, посетите http://www.sans.org/resources/glossary.php

A

Access Control – Контроль доступа
Access Control гарантирует, что ресурсы предоставляются только тем пользователям, которые имеют право на доступ к ним.

Access Control List (ACL) – Список контроля доступа
Механизм, который реализует управление доступом для системных ресурсов путем перечисления списка лиц, которым разрешен доступ к ресурсу.

Access Matrix - Матрицы доступа
Матрица доступа использует строки для представления субъектов и столбы для представления объектов с привилегии, перечисленными в каждой ячейке.

Account Harvesting – Формуляр учетных записей
Account Harvesting - это процесс сбора всех законных имен учетных записей в системе.

ACK Piggybacking - ACK наложения
ACK наложения – это принцип отправления ACK внутри другого пакета, который передается в тот же пункт назначения.

Activity Monitors - Мониторы Активности
Activity Monitors используются для слежения за системой с целью обнаружения вирусной инфекции путем мониторинга работы системы, а также для блокировки вирусной деятельности по возможности.

Address Resolution Protocol (ARP) - Протокол анализа адресов.
Address Resolution Protocol (ARP) является протоколом, предназначенным для организации привязки адреса Интернет-компьютера на физический адрес машины, которая признается в локальной сети. Таблица соответствия, обычно называемая кэш ARP, используется для хранения информации о соответствии физических MAC адресов и назначенных им IP-адресов. ARP-протокол поддерживает правила корреляции и обеспечивает преобразование адресов в обоих направлениях.

Advanced Encryption Standard (AES) - Улучшенный стандарт шифрования
Стандарт шифрования, разрабатываемый в NIST. Предназначен для использования неклассифицированных, публично раскрытых алгоритмов симметричного шифрования.

Auditing - Аудит
Сбор информации для аудита и анализа текущей ситуации на наличие уязвимостей и проверки соблюдения политик безопасности.

Authentication - Аутентификация
Authentication - это процесс проверки подлинности и подтверждения права на доступ.

Authorization - Авторизация
Authorization - это процесс подтверждения полномочий на получение разрешения или расширение полномочий с целью выполнения каких-либо действий.

Autonomous System - Автономная система
Одна сеть или несколько сетей, находящиеся под административным управлением. Автономную систему также иногда называют областью маршрутизации. Автономной системе присваивается глобальный уникальный номер, который иногда называют номер автономной системы (Autonomous System Number (ASN)).

B

Backdoor – Черный ход
Backdoor - это инструмент, устанавливаемый после компрометации для того, чтобы дать злоумышленнику возможность более легкого доступа к скомпрометированной системе в обход системы безопасности, которая установлена в системе.

Banner – Баннер - Заголовок
Banner - это набор сведений, которые транслируются удаленному пользователю, при попытке подключиться к службе. Он может включать в себя сведения о версии, системную информацию, или предупреждение об использованной системе контроля полномочий.

Basic Authentication - Обычная проверка подлинности
Basic Authentication - это простейшая веб-проверка подлинности на основе схемы, которая требует отправку имени пользователя и пароля при каждом запросе.

Bastion Host - Узел-бастион
Bastion Host называют узлы, защита которых была усилена (hardened) в ожидании уязвимости, которая еще не была обнаружена.

Block Cipher - Блочный шифр
Block Cipher шифрует один блок данных за один момент времени.

Boot Record Infector - Инфицирование загрузочной записи
Boot Record Infector - это фрагмент вредоносной программы, которая вставляет вредоносный код в загрузочный сектор диска

Brute Force - Грубая сила
Техника криптоанализа или другого вида атаки с участием исчерпывающих процедур, которые пытаются применить все возможности обойти защиту одну за другой.

Buffer Overflow - Переполнение буфера
Переполнение буфера происходит, когда программа или процесс пытается сохранить больше данных в буфере (область временного хранения данных), чем предполагалось хранить. Поскольку буферы создаются для хранения ограниченного объема данных, дополнительная информация, может вызвать переполнение буфера и привести к повреждению или перезаписи корректных данных, хранящихся в нем.

Business Continuity Plan (BCP) - План обеспечения непрерывности бизнеса
Business Continuity Plan является планом реагирования на чрезвычайную ситуацию, содержащий операции резервного копирования и восстановления после сбоя, которые обеспечат доступность критически важных ресурсов и способствовать бесперебойной работы в чрезвычайной ситуации.

C

Cache – Кэш-память
Явная кэш память – это специальный высокоскоростной механизм хранения. Это может быть либо защищенная часть основной памяти, либо независимое высокоскоростное устройство хранения данных. Два типа кэширования часто используется в персональных компьютерах: кэширование памяти и кэширование дискового пространства.

Cache Cramming - Кэш Крэминг
Cache Cramming - это техника обмана браузера для запуска кэшированного Java кода с локального диска, а не из зоны Интернета, чтобы он работал с менее строгими ограничениями.

Cache Poisoning – Отравление кэша
Вредоносный код или вводящие в заблуждение данные от удаленного сервера имен сохраняются в кэш [Cached] через другой сервер имен. Обычно для атаки используется кэш зараженного DNS сервера.

Call Admission Control (CAC) - Вызов контроля доступа (CAC)
Просмотр и контроль всех входящих и исходящих сообщений сети брандмауэром на основе пользовательских политик.

Certificate-Based Authentication - Аутентификация на основе сертификатов
Аутентификация на основе сертификатов состоит в использовании SSL и сертификатов для аутентификации и шифрования HTTP трафика.

Challenge-Handshake Authentication Protocol (CHAP) – Протокол аутентификации с «вызовом рукопожатия»
Challenge-Handshake Authentication Protocol использует механизм аутентификации типа «вызовом рукопожатия», где ответ меняется в каждом вызове для предотвращения атак.

Cipher - Шифр
Криптографический алгоритм для шифрования и дешифрования.

Ciphertext - Шифротекст
Ciphertext - это сообщения в зашифрованном виде, готовые к отправке.

Competitive Intelligence - Конкурентоспособный интеллект
Competitive Intelligence - это шпионаж, использующий законные, или, по крайней мере, не очевидно незаконные средства.

Computer Emergency Response Team (CERT) - Служба компьютерной безопасности
Организация, которая изучает компьютерную и сетевую безопасность (INFOSEC) для того, чтобы обеспечить оперативную помощь жертвам нападений, издает предупреждения относительно уязвимости, угроз, и предлагает другую информацию, чтобы помочь в усилении компьютерной и сетевой безопасности.

Countermeasure - Контрмера
Методы реакции, которые обычно применяются для предотвращения негативных проявлений, как только угроза была обнаружена. Системы предотвращения вторжения (Intrusion Prevention Systems (IPS)) обычно используются, как контрмеры для того, чтобы предотвратить негативное развитие событий, в случае ,если злоумышленник получил доступ к компьютерной сети. Другими встречными мерами являются: оперативное обновление ПО (patches), списки контроля доступа и фильтры вредоносного ПО.

Cryptanalysis - Криптоанализ
Математическая наука, которая ведет анализ криптографической системы для того, чтобы получить знание о том, что нужно сделать, чтобы сломать или обойти защиту, которая была встроена при проектировании системы. Другими словами, преобразование шифрограммы в открытый текст, не зная ключа.

Cryptographic Algorithm or Hash - Криптографический алгоритм или случайные данные
Алгоритм, который использует науку шифрования, включая алгоритмы кодирования, криптографические алгоритмы случайных данных, цифровые алгоритмы подписи и ключевые алгоритмы соглашения.

Cut-Through - "На лету"
Cut-Through - это метод переключения, где только заголовок пакета читается прежде, чем сообщение отправляется его адресату.

D

Data Encryption Standard (DES) - Стандарт кодирования данных
Широко используемый метод кодирования данных, использующий персональный (секретный) ключ. Существуют 72 000 000 000 000 000 (72 квадрильона) или более возможных ключей шифрования, которые могут использоваться. Для каждого конкретного сообщения ключ выбирается наугад из всего огромного количества возможных ключей. Так же как и для других методов криптографического шифрования, основывающихся на персональных ключах, и отправитель, и получатель должен знать и использовать тот же самый персональный ключ.

Data Mining - Поиск данных
Data Mining - это методика, используемая для анализа существующей информации, обычно с намерением открыть новые направления развития и поддержки бизнеса.

Day Zero - "Нуль Дня" или "Нулевой День"
"Day Zero" или "Zero Day" является днем, когда обнаружена новая уязвимость. В некоторых случаях, "нулевой день" означает появление опасности, для которой еще не сделано никакой защиты. ("День Один"- день, в который появилось доступное исправление или защита).

Decryption - Расшифровка
Decryption - это процесс преобразования зашифрованного сообщения в его первоначальный открытый текст.

Defacement - Нанесение ущерба
Defacement - это метод изменения содержимого веб-сайта таким способом, чтобы это наносило ущерб и сам веб-сайт становился "разрушенным" или порочащим его владельца.

Defense In-Depth - Всесторонняя защита
Defense In-Depth - это подход использования многократных уровней безопасности, чтобы принять меры против отказа отдельного компонента безопасности.

Demilitarized Zone (DMZ) - Демилитаризированная зона
В компьютерной безопасности, в общем случае Demilitarized Zone (DMZ) (демилитаризованная зона) или сетевой периметр являются областью сети (подсетью), которая находится между внутренней сетью организации и внешней сетью, обычно Интернетом. DMZ помогает организовать многоуровневую модель защиты, в которой

организована сегментация сети на подсети, основанная на соблюдении требований безопасности или политик безопасности. Демилитаризованная зона обеспечивает либо транзит сообщений из безопасного источника опасному адресату, либо из опасного источника - более безопасному адресату. В некоторых случаях, скрытая подсеть, которая используется для серверов, доступных для внешних пользователей, рассматривается как демилитаризованная зона DMZ

Denial of Service - Отказ в обслуживании
Предотвращение несанкционированного доступа к системному ресурсу или отсрочка системных операций и функций.

Dictionary Attack - Нападение по словарю
Нападение, которое пробует все фразы или слова из словаря, пробуя подобрать пароль или ключ защиты. Dictionary Attack использует предопределенный список слов по сравнению, в отличие от решения "в лоб" (brute force), которое пробует все возможные комбинации.

Diffie-Hellman - Мартин Хеллман
Алгоритм ключевых соглашений, опубликованный в 1976 Whitfield Diffie (Витфилд Диффи) и Diffie-Hellman (Мартин Хеллман). Diffie-Hellman генерирует ключ, который получается без кодирования. Однако, ключ, который он производит, может использоваться для кодирования, для дальнейших ключевых операций управления или для любого другого шифрования.

Digest Authentication - Идентификация обзора
Digest Authentication позволяет веб-клиенту сети вычислить случайный код пароля MD5, чтобы использовать его, как пароль для доступа.

Digital Certificate - Цифровой сертификат
Digital Certificate - это электронная "кредитная карточка", которая устанавливает разрешение, заниматься той или другой деятельностью на сети. Этот сертификат выпускается авторизованный на эту деятельность организацией и подтверждает наличие полномочий. Сертификат содержит имя пользователя, серийный номер, дату окончания срока действия, копию ключа публики держателя сертификата (используемый для того, чтобы шифровать сообщения и цифровые подписи), и цифровую подпись выпускающей свидетельство организации для того, чтобы получатель мог проверить легальность свидетельства.

Digital Envelope - Цифровой конверт
Digital Envelope - это зашифрованное сообщение с зашифрованным ключом сеанса.

Digital Signature Algorithm (DSA) - Цифровой алгоритм подписи
Асимметричный криптографический алгоритм, который производит цифровую подпись в форме пары больших чисел. Подпись рассчитывается, используя правила и параметры, так, чтобы идентичность подписывающего лица и целостности подписанных данных может быть подтверждена.

Digital Signature Standard (DSS) - Цифровой стандарт подписи
Американский Правительственный стандарт, который определяет Digital Signature Algorithm (DSA), который подразумевает асимметричное шифрование.

Disaster Recovery Plan (DRP) - План восстановления после аварийной ситуации
Disaster Recovery Plan - это процесс восстановления IT-систем в случае сбоя или аварийной ситуации.

Domain Hijacking - Налет на домен
Domain Hijacking - это нападение, в котором нападающий проникает через первичную защиту и блокирует доступ к DNS-серверу доменной системы имен домена и, затем поставляет свой собственный сервер вместо оригинального.

Domain Name System (DNS) - Доменная система имен
Domain name system (DNS) - это механизм с помощью, которого Интернет-имена (доменные имена) передаются через Интернет пользователям компьютерной сети. Доменные имена - это простые для запоминания и использования "дескрипторы" для пользователей Интернет-ресурсов.

DumpSec – «Снимок»
DumpSec - это инструмент безопасности, который формирует "снимок" памяти с разнообразной информацией о пользователях системы, файловой системе, реестре, разрешениях, политике паролей и службах.

Dumpster Diving - Погружение в мусорный контейнер
Dumpster Diving - это процесс получения паролей и внутренней корпоративной информации путем просмотра данных, которые не были приняты в обработку.

E

Eavesdropping - Подслушивание
Eavesdropping - это простое подслушивание частных сеансов связи(разговоров) с целью получения информации, которая может обеспечить доступ к системе или сети.

Egress Filtering - Фильтрация Выхода
Фильтрация выходного трафика.

Encapsulation - Инкапсуляция
Включение одной структуры данных внутрь другой структуры данных так, чтобы исходная структура данных была скрыта в настоящее время.

Encryption - Шифрование
Криптографическое преобразование данных (называемое "открытым текстом") в форму (называемую "шифрограммой"), которая скрывает оригинальное значение данных, препятствуя тому, чтобы исходные данные были прочитаны или использованы.

Extensible Authentication Protocol (EAP) - Протокол расширенной аутентификации
Система, которая поддерживает множественный и расширенный механизмы распознавания для PPP (Point to Point Protocol- протокол канала связи), включая передачу пароля в текстовом виде, ответ вызова и произвольные последовательности диалога.

F

Filter - Фильтр
Фильтр используется, чтобы определить, какие пакеты будут, а какие не будут использованы. Фильтр может использоваться в системах просмотра трафика (снифферы), чтобы определить, какие пакеты отображать, или системами сетевой защиты, чтобы определить, какие пакеты блокировать.

Fingerprinting - Отпечаток пальца
Посылка странных пакетов к системе, чтобы определить, как она будет реагировать на эти запросы и на основании этой реакции определить, используемую операционную систему.

Firewall - Брандмауэр
Логическая или физическая неоднородность в сети, чтобы предотвратить несанкционированный доступ к данным или ресурсам.

Flooding - Лавинная адресация
Волновое распространение пакетов (в телекоммуникационной сети) метод, в котором каждая сетевая станция пересылает пакеты данных всем своим соседям.
Это атака, нацелена на то, чтобы вызвать сбой в системах безопасности компьютера или сетях передачи данных.

Fork Bomb - Бомба ветвления
Fork Bomb работает при использовании функции вызова процесса fork(), который является копией оригинала. При неоднократном выполнении все доступные процессы на машине могут быть запущены.

Form-Based Authentication - Аутентификация на основе формы
Form-Based Authentication использует форму ввода на веб-странице для того, чтобы предоставить пользователю возможность ввести информацию: пароль и имя пользователя.

H

Hardening - Повышение защищенности
Hardening - это процесс поиска и исправление слабых мест для предотвращения появления уязвимости в системе.

Hash Function - Хеш-функция
Алгоритм, который вычисляет значение на основе объекта данных, таким образом отображая объект данных, на основе меньшего объекта данных.

Hash Functions - Хеш-функции
(Криптографические) хеш-функции используются, чтобы генерировать "контрольную сумму" для большего объема текста, что упрощает проверку большого файла на наличие изменений. Результат этой хеш-функции может использоваться для того, чтобы получить информацию о том, что больший файл был изменен, при этом отсутствует необходимость сравнивать большие файлы друг с другом. Часто используются хеш-функции MD5 и SHA1.

Hijack Attack – Атака типа нападение
Форма активного перехвата, в которой нападающий захватывает управление, предварительно установленное через коммуникационный канал связи.

HTTP Proxy – Прокси HTTP
HTTP Proxy сервер - это сервер, который действует как посредник в коммуникации между клиентами HTTP и серверами.

HTTPS
Обычно используется в первой части URL (часть, которая предшествует двоеточию и определяет схему доступа или протокол), этот термин определяет использование HTTP, расширенного механизмом безопасности, который обычно построен на основе SSL.

Hybrid Attack - Гибридное нападение
Hybrid Attack основывается на методе нападения по словарю, добавляя цифры и символы к словам словаря.

Hybrid Encryption - Гибридное кодирование
Приложение шифрования, которое объединяет два или больше алгоритма шифрования, в частности комбинация симметрического и асимметричного шифрования.

Hypertext Markup Language (HTML) - Язык разметки гипертекста (HTML)
Набор символов разметки или кодов, вставленных в файле, предназначенном для отображения на странице браузера Всемирной паутины.

Hypertext Transfer Protocol (HTTP) - Язык передачи гипертекста (HTTP)
Протокол в межсетевом семействе протоколов (IP), применяемый для передачи гипертекстовых документов через Интернет.

I

Identity - Сущность
Identity - это то, что определяет лицо или предмет, например, имя, под которым известно данное лицо или предмет.

Incident – случай, случайность, происшествие, событие, эпизод
Incident - это неблагоприятное сетевое событие в информационной системе или сети или угроза возникновения такого события.

Ingress Filtering - Входная фильтрация
Входная Фильтрация фильтрует входящий трафик.

Input Validation Attacks – Атаки проверки правильности входа
Input Validation Attacks состоят в том, что нападающий преднамеренно посылает необычный входной сигнал в надежде на то, что он запутает приложение.

Internet Control Message Protocol (ICMP) – Протокол сообщений управляемый по интернет (ICMP)
Стандартный Интернет-протокол, который используется для сообщения об ошибке во время обработки IP-датаграммы и обмена другой информацией относительно состояния IP-сети.

Internet Protocol Security (IPsec) - Безопасность протокола интернет
Развивающийся стандарт сетевой безопасности или обработки пакетов на уровне сетевой коммуникации.

Intrusion Detection System (IDS) – Система обнаружения вторжения
Система управления безопасностью для компьютеров и сетей. Intrusion Detection System (IDS) собирает и анализирует информацию от различных областей в пределах компьютера или сети, чтобы идентифицировать возможные нарушения безопасности, которые включают оба вторжения (нападения снаружи организации) и неправильного применения защиты (нападения изнутри организации).

IP Flood - волновое распространение IP пакетов
Нападение типа отказ в обслуживании, которое посылает хосту больше пакетов эхо-запросов ("ping"), чем протокол может обработать.

IP Forwarding – Пересылка IP - IP-форвардинг
IP Forwarding - это функциональная возможность операционной системы, которая позволяет хосту действовать как маршрутизатор. На системе, которая имеет больше одной сетевой интерфейсной платы, должен быть включен селектор IP-форвардинг для того, чтобы система могла работать, как маршрутизатор.

IP Spoofing – IP «спуфинг» - или подмена IP
Атаки, при которых подставляется фальшивый IP-адрес в сообщения.

K

Kerberos - технология Kerberos
Система, разработанная в 1980-х годах в Технологическом Институте Штата Массачусетс MIT, которая заключается в применении паролей и симметрического шифрования (стандарт кодирования данных) для того, чтобы осуществить авторизацию на основе билета, службы идентификации равного по положению объекта и службы управления доступом, распределенное в сетевой среде на основе архитектуры клиент-сервер (соответствует стандарту DES описано в RFC 1510). Kerberos используется в Microsoft Windows начиная с версии 2000. В русском переводе Kerberos - Цербер. Так в древнегреческой мифологии назывался трёхголовый пёс, охранявший вход в подземное царство

L

Layer 2 Forwarding Protocol (L2F) - Форвардинг протокола уровня 2
Межсетевой протокол (первоначально разработанный корпорацией Cisco), который использует туннелирование PPP по IP, чтобы создать виртуальное продление модемной линии связи через сеть, инициализируемое сервером модемной связи и прозрачное для пользователя модемной связи.

Layer 2 Tunneling Protocol (L2TP) - Протокол туннелирования уровня 2
Layer 2 Tunneling Protocol (L2TP) – это расширение протокола туннелирования типа точка-точка, используемого провайдером услуг Интернета, чтобы разрешить работу виртуальной частной сети VPN по Интернету.

List Based Access Control - Управление доступом на основе списка
List Based Access Control связывает список пользователей и их привилегий с каждым объектом.

M

MAC Address – MAC-адрес – физический MAC-адрес
Физический адрес, числовое значение которого, однозначно определяет то сетевое устройство, на котором он установлен, он является уникальным для каждого устройства на планете.

Malicious Code - Враждебный программный код
Программа (например, Троянский конь), которая, под видом выполнения полезной или желательной функции, фактически получает несанкционированный доступ к системным ресурсам или обманывает защитные настройки системы и выполняет другие злонамеренные действия.

Malware - Вредоносное программное обеспечение - Мэлвер
Обобщенное название для множества различных типов враждебного программного кода.

Masquerade Attack - Атака подменой
Тип нападения, в котором система неправомерно представляет себя, как объект другой системы (подразумевает идентичность).

Md5
Один из вариантов представления криптографической хеш-функции. Также см. "хеш-функции" и "sha1".

N

Network Address Translation (NAT) - Трансляция сетевого адреса.
Применяется для того, чтобы совместно использовать один или несколько открыто маршрутизируемых IP-адресов среди большого количества хостов. На хостах назначены частные IP-адреса, которые "транслируются" в один из маршрутизируемых публичных IP-адресов. Обычно в малых домашних сетях или сетях малого бизнеса используют NAT, чтобы совместно использовать один IP-адрес на DLS линии или телефонном модеме. Однако в некоторых случаях NAT используется для серверов, как дополнительный уровень защиты.

National Institute of Standards and Technology (NIST) - Национальный Институт Стандартов и Технологии
National Institute of Standards and Technology - это отдел американского Отдела Торговли. Прежде известный как Национальное Бюро Стандартов, NIST предлагает и поддерживает эталоны. Он также имеет активные программы для того, чтобы поощрять применение и помогать промышленности и науке разрабатывать и использовать эти стандарты.

Network Address Translation - Трансляция сетевых адресов
Трансляция Интернет адресов, используемых в пределах одной сети к другим IP-адресам, используемым в пределах другой сети. Одна сеть определяется, как внутренняя сеть, а другая сеть - как внешняя сеть.

Network-Based IDS – Система Обнаружения Вторжения на уровни сети
Network-Based IDS система контролирует трафик на своем сегменте источника данных. Это в общем случае достигается путем запуска сетевой интерфейсной платы в различных режимах, чтобы зафиксировать весь сетевой трафик, проходящий через неё. Сетевой трафик на других сегментах и трафик на других коммуникационных средствах (таких, как телефонные линии) не может быть проверен. Network-Based IDS обеспечивает просмотр пакетов на сети так же, как будто они проходят перед неким датчиком. Датчик может видеть только сетевые пакеты, которые проходят через сетевой сегмент, к которому он подключен. Сетевые пакеты подлежат просмотру и представляют интерес, если они соответствуют подписи. Система обнаружения вторжения на основе просмотра сети пассивно контролирует сетевую деятельность для обнаружения нападений. Контроль сетевой активности имеет несколько преимуществ перед традиционными системами обнаружения вторжения на базе хоста. Поскольку в последнее время много вторжений проводятся по сетям, и сети все чаще становятся объектами нападения, то эти методики защиты являются превосходным методом обнаружения многих нападений, которые могут быть пропущены традиционными механизмами обнаружения вторжений на базе хоста.

P

Packet - Пакет
Часть сообщения, передаваемого по сети пакетной коммутации. Одна из главных особенностей пакета это то, что он содержит адрес назначения в дополнение к данным. В сетях IP, пакеты часто называют датаграммами.

Packet Switched Network - Сеть коммутации пакетов
Packet Switched Network - это сеть, где индивидуальные пакеты следуют один за другим по их собственным путям от одной конечной точки до другой.

Password Authentication Protocol (PAP) - Протокол идентификации пароля
Password Authentication Protocol - это простой опознавательный механизм, когда пользователь вводит пароль и этот пароль посылается через сеть, обычно в декодированном виде.

Password Cracking - Раскалывание пароля
Password Cracking - это попытка угадать пароль, учитывая информацию файла пароля.

Password Sniffing - Подслушивание пароля
Пассивное перехватывание, обычно на локальной сети для того, чтобы собрать информацию и выбрать из неё пароли.

Patch - "Заплатка" - Обновление
Patch - это маленькое обновление, выпущенное изготовителем программного обеспечения, чтобы установить ошибку в существующей программе.

Penetration - Преодоление защиты
Получение неправомочного доступа к уязвимым данным, обходя защиты системы.

Penetration Testing – Тест на проникновение
Испытание системы на проникновения используется, чтобы проверить внешнюю безопасность периметра сети или оборудования.

Permutation - Перестановка
Для шифрования сообщений перестановка сохраняет те же буквы в сообщении, но изменяет их позиции в текст.

Personal Firewalls - Персональные брандмауэры
Персональными брандмауэрами называют брандмауэры, которые установлены и работают на отдельных ПК.

Pharming - Фарминг
Это более сложный вид атаки MITM и разновидность кибер-мошенничества. Автоматическое перенаправление пользователей на фальшивые сайты, являющихся копиями оригинальных. Обычно злоумышленники изменяют адреса онлайновых банков, в этом случае при авторизации пользователь вводит в формы конфиденциальные данные, не подозревая, что они тут же становятся известны преступникам.
Это может быть достигнуто путем перенастройки DNS-сервера в Интернете и, использования фальшивых URL для перенаправление пользователей на шпионский IP-адрес веб-сайта. Почти все пользователи банков используют URL, такие как www.worldbank.com вместо реальных IP (192.86.99.140). После получения данных пользователя, злоумышленник может получить доступ к реальным сайтам, например, www.worldbank.com и проводить операций с использованием учетных данных пользователя на этом сайте.

Phishing – Фишинг - Выуживание
Использование электронной почты для того чтобы сделать видимость получения сообщения из проверенного источника для того, чтобы обмануть пользователя и принудить его к вводу своих корректных пользовательских данных на поддельный сайт. Обычно адрес электронной почты и веб-сайт выглядят так, как будто они являются частью банка, с которым пользователь имеет реальный договор.

Ping of Death – «Пинг смерти»
Нападение, которое посылает некорректно большой пакет ICMP эхо запрос ("пинг") с целью переполнения входного буфера машины назначения, что приводит машину к краху.

Ping Scan – «Пинг-сканирование»
Пинг-сканирование ищет машины, которые отвечают на ICMP Echo запросы.

Ping Sweep – «Пинг-подмена»
Нападение, которое заключается в отправке ICMP эхо-запросов ("пинг") на диапазон IP-адресов, с целью нахождения компьютеров, которые могут быть исследованы на наличие уязвимостей.

Point-to-Point Protocol (PPP) - Протокол "точка-точка"
Протокол для связи между двумя компьютерами через последовательный интерфейс, как правило, подключение личного компьютера к серверу, через телефонную линию. Для этой коммуникации используются IP-пакеты, которые отправляются на сервер, где они могут быть перенаправлены в Интернет.

Point-to-Point Tunneling Protocol (PPTP) - Протокол "точка-точка" для тоннеля
Протокол "точка-точка" для тоннеля, позволяет корпорациям через закрытые "тоннели" расширить свою корпоративную сеть, передавая данные через публичные сети Интернет.

Poison Reverse – Возврат невозможен
Split horizon с Poison Reverse (проще говоря, Возврат невозможен) подразумевает не включение в себя таких маршрутов передачи данных, но устанавливает признак возможности их использования на бесконечность. По сути, предположение о том, что маршруты не достижимы.

Polyinstantiation - Полиреализация
Polyinstantiation - это способность базы данных обслужить многократные записи с тем же самым ключом. Это используется для того, чтобы предотвратить нападения типа inference (умозаключение).

Polymorphism – Полиморфизм
Polymorphism - это процесс, с помощью которого вредоносное программное обеспечение изменяет свой основной код, чтобы избежать обнаружения.

Post Office Protocol, Version 3 (POP3) - Протокол POP, Версия 3 (POP3)
Стандартный интернет-протокол, в соответствии с которым рабочая станция клиента может динамически обратиться к почтовому ящику на хосте сервера, чтобы отыскать сообщения почты, которые сервер получил и хранит для клиента.

Pretty Good Privacy (PGP)TM – Высокая степень секретности
Trademark of Network Associates, Inc, относится к компьютерной программе (и связанным с ней протоколам), которые применяют шифрование для того, чтобы обеспечить безопасность данных для электронной почты и других приложений в Интернете.

Private Addressing - Частная адресация
IANA зарезервировало три адресных интервала для использования частными или неподключенными к Интернет сетями. Эти области памяти упоминаются, как частное адресное пространство и определены в документе RFC 1918. Зарезервированные блоки адресов: 10.0.0.0 до 10.255.255.255 (10/8 префикс) 172.16.0.0 до 172.31.255.255 (172.16/12 префикс) 192.168.0.0 до 192.168.255.255 (192.168/16 префикс).

Promiscuous Mode - Разнородный режим
Машина читает все пакеты из сети, независимо от того, кому они адресованы. Этот режим используется сетевыми администраторами, чтобы диагностировать сетевые проблемы, но также и сомнительными личностями, кто пробует подслушать сетевой трафик (который мог бы содержать пароли или другую информацию).

Proxy Server - Прокси-сервер
Сервер, который действует как посредник между рабочей станцией пользователя и Интернетом так, чтобы предприятие могло гарантировать безопасность, административное управление и службу кэширования. Прокси-сервер связан или со шлюзом, который отделяет сеть предприятия от внешней сети, или с сервером системы сетевой защиты, который защищает сеть предприятия от внешнего вторжения.

Public Key - Общественный ключ
Публично-открытый компонент пары криптографических ключей, используемых для асимметричного шифрования.

Public Key Encryption - Общественное ключевое кодирование
Популярный синоним для "асимметричного шифрования".

Public Key Infrastructure (PKI) - Общественная ключевая инфраструктура
PKI (Public Key Infrastructure) разрешает пользователям в основном в незащищенной общественной сети, типа Интернета обмениваться данными, электронными деньгами и прочими важными ресурсами надежно и безопасно при использовании общественной и частной криптографической ключевой пары, которая назначается и распределяется через авторизованные для этих целей службы. Общественная ключевая инфраструктура предусматривает цифровое свидетельство, которое может идентифицировать человека или организацию и позволяет сохранять и применять необходимые свидетельства из локального каталога.

Public-Key Forward Secrecy (PFS) - Общественный ключ, пересылающий безопасность
Для протокола соглашения о ключах, основанного на асимметричном шифровании это свойство, которое гарантирует, что ключ сеанса, полученный из ряда долгосрочных общественных и частных ключей, не будет поставлен под угрозу в будущем, если один из частных ключей будет поставлен под угрозу.

R

Race Condition - Состояние Гонки
Race Condition подразумевает маленькое окно времени между применением настроек безопасности и началом использования службы.

Reconnaissance - Исследование
Reconnaissance - это фаза планирования нападения, когда злоумышленники находят новые системы.

Reverse Address Resolution Protocol (RARP) - Обратный Протокол определения адресов
RARP (Reverse Address Resolution Protocol) - это протокол, в соответствии с которым физическая машина в локальной сети может запросить получение IP-адреса для себя из таблицы Address Resolution Protocol (протокола определения адресов), шлюза или кэша. Сетевой администратор создает таблицу в межсетевом маршрутизаторе в локальной сети, который содержит физические адреса машин (Media Access Control или MAC-адреса) и соответствующие им Internet Protocol адреса (IP-адреса). Когда включается новая машина, ее программа RARP-клиент посылает запросы к RARP-серверу на маршрутизаторе, запрашивая получение IP-адреса для неё. Просматривая свою таблицу маршрутизатора, сервер RARP находит в ней заданный IP-адрес и возвращает его на машину, которая будут использовать его в будущем.

Reverse Lookup - Обратный поиск
Чтобы узнать имя хоста, которое соответствует специфическому IP-адресу, используется Reverse Lookup, который на основе IP-адреса выдает имя домена.

Reverse Proxy - Обратный прокси
Reverse Proxy собирает общественные запросы HTTP и передает их конечному веб-серверу для того, чтобы настроить пересылку содержимого ему, таким образом, прокси-сервер может послать содержимое конечному пользователю.

Risk - Риск
Risk - это величина уровня угрозы с уровнем уязвимости. Он задает вероятность успешного нападения.

Risk Assessment - Оценка риска
Risk Assessment - это процесс с помощью, которого идентифицируются риски и определяется их воздействие на систему.

Risk Averse – Избежание риска
Избежание риска, даже если это приводит к потере некоторых возможностей. Например, использование (более дорого) подключения по телефону вместо отправки электронной почты с целью избежание рисков, связанных с использованием электронной почты, вместо которого можно позвонить по телефону.

S

S/Key – S/Код
Механизм безопасности, который использует криптографическую хеш-функцию, чтобы генерировать последовательность 64-битовых одноразовых паролей для удаленного входа в систему. Клиент генерирует одноразовый пароль, применяя криптографическую хеш-функцию MD4, несколько раз к секретному ключу пользователя. Для каждой последовательной идентификации пользователя, номер хеш-функци уменьшается на единицу.

Scavenging - Просмотр остатка данных (в памяти)
Поиск остатка данных в системе с целью получения неофициальных знаний об уязвимых данных.

Secure Electronic Transactions (SET) - Защита электронных транзакций
Secure Electronic Transactions - это протокол, разработанный для проведения транзакций кредитными картами, в которых все стороны (клиенты, торговцы и банк) заверены, используя цифровые подписи, кодирование защищает содержимое и обеспечивает целостность и непрерывную безопасность для транзакций кредитной карты онлайн.

Secure Shell (SSH) – Защитная оболочка
Программа ведения журнала регистрации в другом компьютере по сети, выполнения команд на удаленной машине и перемещения файлыов от одной машины к другой.

Secure Sockets Layer (SSL) - Уровень безопасного сокета SSL
Протокол, разработанный Netscape для передачи частных документов по интернет. SSL работает, используя общественный ключ, чтобы зашифровать данные, которые передаются через SSL-подключение.

Security Policy - Политика безопасности
Набор правил и действий, которые определяют или регулируют, как система или устройство организуют службы безопасности, чтобы защитить чувствительные и критические системные ресурсы.

Segment - Сегмент
Segment - это другое название для TCP пакетов.

Session - Сессия
Session - это виртуальное подключение между двумя хостами, во время которых хосты передают сетевой трафик.

Session Hijacking – Сеанс налета
Организуется через уже установленную сессию.

Session Key - Ключ сеанса
В контексте симметрического кодирования это ключ, который является временным или используется в течение относительного короткого промежутка времени. Обычно, Session Key используется в течение определенного периода коммуникации между двумя компьютерами для поддержки отдельного подключения или набора транзакций, либо ключ используется в приложении, которое защищает большие объемы данных и, поэтому, он должен часто изменяться.

SHA1
Одно из применений криптографической хеш-функции. Смотрите также "MD5"

Shadow Password Files - Теневые файлы пароля
Системный файл, в котором хранятся пользовательские пароли в закодированном виде, чтобы они не были доступны для людей, которые пытаются незаконно подключиться к системе.

Signature - Подпись
Signature - это различимый набор символов в сетевом трафике, который может быть идентифицирован на определенном инструменте или средстве.

Simple Integrity Property - Простое свойство целостности
В Simple Integrity Property пользователь не может передать данные на более высокий уровень целостности, чем он сам имеет.

Simple Network Management Protocol (SNMP) - Простой протокол управления сетью
Протокол, занимающийся управлением сетью, контролем сетевых устройств и их функций. Входит в набор протоколов для управления сложными сетями.

Smurf - Смарфинг, Smurf-атака, Смарф-атака (вид сетевого терроризма, полностью парализующий работу интернет-узла - в случае атаки компьютер-жертва получает тысячи ответов на запрос, который никогда не посылался; по названию компьютерной программы)
Smurf-атаки заключаются в отправке ping-запроса в широковещательном режиме для отдаленной сети, что приводит к большому количеству ответов на ping запросы, возвращаемых адресату.

Sniffer – «Сниффер» программа наблюдения
Sniffer - это инструмент, который контролирует сетевой трафик, проходящий через сетевой интерфейс.

Sniffing - пассивное прослушивание сети
Синоним для "пассивное перехватывание".

Social Engineering - Социальная инженерия
Эвфемизм для нетехнических или низко-технологических методов, типа лжи, пародирования, уловок, взяток, шантажа и угроз, часто применяемых для нападения на информационные системы.

Spam - "Спэм"
Ненужная электронная почта или отправленные по почте ненужные группы новостей.

Split Horizon – Разделение горизонта
Split horizon - это алгоритм, который работает на маршрутизаторе и позволят запомнить и исключить из использования маршруты, по которым были получены вредоносные коды.

Split Key – Разделенный ключ
Криптографический ключ, который разделен на два или больше отдельных элемента данных, которые индивидуально не представляют никакого смысла и требуют рассмотрения целого ключа, появляющегося после объединения элементов.

Spoof – мистификация – обман - ввод в заблуждение
Попытка неправомочным пользователем получить доступ к системе, изображая зарегистрированного пользователя.

SQL Injection - Инъекция SQL
SQL Injection - это тип нападения при проверке правильности входного подключения, специально для систем управления базами данных, где код SQL вставлен в прикладные запросы для управления базами данных.

Stack Mashing – Путаница в стеке
Stack Mashing - это методика использования буферного переполнения с целью обмануть систему и заставить компьютер выполнять произвольный код.

Stateful Inspection – Осмотр состояния
Так называемая динамическая фильтрация пакета. Stateful Inspection - это брандмауэрная архитектура системы сетевой защиты, которая работает на сетевом уровне. В отличие от статической фильтрации пакета, которая исследует пакет на основании информации в его заголовке, Stateful Inspection исследует не только информацию заголовка, но также и содержание пакета на прикладном уровне, чтобы получить больше информации о пакете, чем только информация о источнике передачи и её адресате.

Static Host Tables - Статические таблицы хостов
Static Host Tables - это текстовые файлы, которые содержат имя хостов и назначенные им сетевые адреса.

Static Routing - Статическая маршрутизация
Static Routing означает, что информация, содержащаяся в таблицах маршрутизации, не изменяется.

Stealthing –«стилфинг»
Stealthing - это термин, который определяет механизмы, используемые враждебными программными кодами, чтобы скрыть свое присутствие в инфицированной системе.

Steganalysis – «стеганализис»
Steganalysis - это процесс обнаружения и нанесения поражения, используя steganography.

Steganography – Стеганография
Методы сокрытия существования сообщений или других данных. Эти методы отличаются от шифрования, которое скрывает содержание сообщения, но не скрывает наличие сообщения непосредственно. Пример стенографического метода - это "невидимые" чернила.

Stream Cipher - Шифрование потока
Stream Cipher заключается в кодировании сообщения отдельно по битам, байтам или компьютерным словам одновременно.

Subnet Mask – Маска подсети
Subnet Mask используется, чтобы определить количество битов, используемых для кодирования подсети и части хостов в адресе. Маска представляет собой 32-разрядное число, которое использует один бит для сети и частей подсетей и нулевые биты для части хостов.

Switch - Коммутатор
Switch - это активное сетевое устройство, которое следит за физическими адресами устройств (MAC-адресами), подключенных к каждому из его портов. Это устройство передаёт данные только в тот порт, к которому подключено устройство с адресом получателя данных.

Switched Network - Коммутируемая сеть
Система коммуникаций, типа общественной телефонной сети, в которой любой пользователь может быть связан с любым другим пользователем с помощью сообщения, линии связи или пакетной коммутации и устройств управления. Любая сеть обеспечивает коммутируемую службу связи.

Symbolic Links - Символьные ссылки
Специальные файлы, которые указывают на другой файл.

Symmetric Cryptography - Симметричное шифрование
Раздел шифрования, подразумевающий алгоритмы, которые используют тот же самый ключ для двух различных шагов алгоритма, типа кодирования и расшифровки, или создания подписи и проверки подписи. Symmetric Cryptography иногда называют "шифрованием с секретным-ключом" (в отличие от шифрования с открытым ключом), потому что объекты совместно используют ключ.

Symmetric Key - Симметричный ключ
Криптографический ключ, который используется в симметричном криптографическом алгоритме.

SYN Flood –Избыток SYN
Атака типа DoS или отказ в обслуживании в ходе которой посылается хосту больше TCP SYN-пакетов (запрос синхронизировать порядковые номера, используемые при открытии соединения), чем реализация протокола может обработать.

T

TCP Fingerprinting - Отпечаток TCP
TCP Fingerprinting - это комбинация заголовков TCP пакетов, используемая для определения операционной системы удаленного устройства.

TCP Full Open Scan - Полный просмотр открытых портов TCP
TCP Full Open Scan - это процесс, при котором по отдельности проверяется каждый порт, выполняя попытку установления связи с тройными путями на каждом порту, чтобы определить, является ли порт открытым.

TCP Half Open Scan - Половинный просмотр открытых портов TCP
TCP Half Open Scan выполняется путем проверки перовой половины алгоритма установления связи с тройными путями на каждом порту, чтобы определить, является ли порт открытым.

TCP Wrapper - Упаковка TCP
Пакет программ, который может использоваться для ограничения доступа к определенным сетевым службам на источнике подключения; простой инструмент контроля и управления входящим сетевым трафиком.

TCPDump – «ДампTCP»
TCPDump - это свободно распространяемый анализатор протоколов для Unix, который может контролировать сетевой трафик на линии.

TELNET
Стандартный Интернет-протокол на основе прикладного уровня TCP, для удаленного подключения одного хоста к другому.

Threat - Опасность - Угроза преодоления защиты (угроза безопасности)
Потенциал нарушения безопасности, который существует, когда есть обстоятельство, возможность, действие или событие, которое может нарушить безопасность и причинить вред.

Threat Assessment - Оценка угрозы
Threat Assessment - это процесс определения типов угроз, воздействию которых может подвергаться организация.

Threat Model - Модель угроз
Threat Model используется для описания возможной угрозы и оценки вреда, который она может нанести системе, если система имеет уязвимость для этой угрозы.

Threat Vector – Вектор угрозы
Это метод, который использует злоумышленник, чтобы достичь цели.

Time to Live - Время жизни
Это значение в пакете Интернет-протокола, которое говорит маршрутизатору сети о том, как долго пакет находится в сети и когда он должен быть уничтожен.

Tiny Fragment Attack - Крошечный фрагмент, доступный для атаки
Во многих реализациях IP-протокола можно настроить необычно маленькие размеры фрагмента исходящего пакета. Если настроенный размер фрагмента достаточно мал, то некоторые из TCP пакетов могут размещать поля заголовка TCP во втором фрагменте, при этом правила фильтрации, которые определяют шаблоны для этих полей, не будут выполняться. Если в ходе фильтрации не обнаруживается минимальный размер фрагмента, то запрещенный пакет может быть передан, поскольку на него не были наложены фильтры. Правила, изложенные в статьях STD 5 и RFC 791, гласят: каждый Интернет-модуль должен быть в состоянии направить датаграмму из 68 байтов без дальнейшей фрагментации. Поэтому Интернет-заголовок может быть до 60 байтов, а минимальный фрагмент 8 байтов.

Transport Layer Security (TLS) - Безопасность транспортного уровня
Это протокол, который обеспечивает конфиденциальность общения между приложениями и пользователями в Интернете. Когда сервер и клиент общаются, TLS гарантирует, что никакая третья сторона не может подслушать или подделывать сообщения. TLS является преемником протокола Secure Sockets Layer.

Triple DES - Тройная DES
Это блочный шифр, основанный на DES, который преобразует каждый блок 64-бит открытого текста, применяя Data Encryption Algorithm три раза последовательно, используя два или три различных ключа, при эффективной длине ключа 112 или 168 бит.

Triple-Wrapped – Тройная обертка
Использование S/MIME: данные, которые были подписаны цифровой подписью, а затем зашифрованы и подписаны еще раз

Trojan Horse - Троянский конь
Компьютерная программа, которая, маскируясь под выполнение полезной функции, также имеет скрытые и потенциально опасные функции, она может уклоняться от механизмов безопасности, иногда за счет использования законных разрешений системного объекта, который вызывает программу.

Trust – доверие – ответственность – обязательство
Trust определяет, какие разрешения и какие действия другие системы или пользователи могут выполнять на удаленных машинах.

Trusted Ports - Доверенные порты
Trusted Ports - это порты с номерами ниже 1024. Они обычно разрешены для открытия пользователям.

Tunnel - Туннель
Канал связи, созданный в компьютерной сети путем инкапсуляции пакетов данных протокола связи во второй протокол, который обычно осуществляет передачу выше или на том же уровне коммуникационной модели, что и первый. Чаще всего, туннель является логическим точка-точка, то есть, уровень 2 модели связи ИОО создается путем инкапсуляции уровня 2 протокола в транспортный протокол (например, TCP), в протоколе сетевого уровня или межсетевой протокол (такой как IP), или в другой протокол канального уровня. Туннелирование может передавать данные между компьютерами, несмотря на то, что используемые для коммуникации протоколы не поддерживаются в коммуникационной сети.

U

UDP Scan - UDP сканирование
UDP сканирование выполнятся для того, чтобы определить, какие UDP порты открыты.

Unicast - Индивидуальная передача
Передача от одного к другому.

User Contingency Plan - Пользовательский план действий для чрезвычайных ситуаций
User Contingency Plan - это план альтернативных методов продолжения ведения деловых операций, если ИТ-системы будут недоступны.

User Datagram Protocol (UDP) - Протокол пользовательских датаграмм
Протокол связи, например TCP, работает на верхнем уровне IP-сетей. В отличие от TCP / IP, UDP / IP предоставляет очень мало возможностей по устранению ошибок, предлагая вместо этого прямой путь для передачи и приема датаграмм по сети IP. Он используется в основном для передачи широковещательных сообщений по сети. UDP использует Интернет-протокол, чтобы передать датаграммы с одного компьютера на другой, но не делить сообщение на пакеты (датаграммы) и собрать сообщение на другом конце. В частности, UDP не обеспечивает упорядочение пакетов для входящих данных.

V

Virtual Private Network (VPN) - Виртуальная частная сеть
VPN - это ограниченные для использования, логические (например, искусственные или смоделированные) компьютерные сети, не пользующиеся системными ресурсами общественной или физической (т.е. реальной) сети (например, Интернет), часто с использованием шифрования (расположенной на хостах или шлюзах), а часто и туннельных связях виртуальной сети по всей реальной сети. Например, если корпорация имеет несколько локальных сетей на нескольких различных промышленных объектах, каждый из которых подключен к Интернет с помощью брандмауэра, корпорации может создать VPN (а) с помощью шифрованных туннелей, чтобы связаться от брандмауэра к брандмауэру через Интернет и (б) не позволять передавать любой другой трафик через брандмауэры. VPN, как правило, дешевле в создании и эксплуатации, чем построение реальной сети, потому что стоимость виртуальных сетевых ресурсов общего доступа ниже, так как их стоимость разделяется с другими пользователями реальной сети.

Virus - Вирус
Скрытый, самостоятельно копирующийся раздел компьютерного программного обеспечения, как правило, содержит, вредоносную логику, которая распространяется путем заражения другого программного обеспечения - то есть, вставляет копию себя в другую программу и становится частью другой программы. Вирус не может работать сам по себе, он требует, чтобы его запустил его хозяин (программа, в которую он встроен), при этом вирус активизируется.

Voice Firewall - Голосовой брандмауэр
Voice Firewall - это система обеспечивающая физический разрыв в контролируемой телефонной сети, в случае получения предупреждения об опасности при управлении входящей и исходящей активностью телефонной сети на основе определенных пользователем политик «управления приемом вызовов» (Call Admission Control (CAC)). Она обеспечивает необходимый уровень безопасности работы голосовых приложений для защиты от угроз или несанкционированного использования сервиса.

Voice Intrusion Prevention System (IPS) - Голосовая система предотвращения вторжений
Голосовая IPS является системой обеспечения безопасности в голосовых сетях, которая контролирует голосовой трафик для нескольких моделей вызова или нападения/ злоупотребления подписями для активного выявления и предотвращения мошенничества, отказа в обслуживании, телекоммуникационных атак, злоупотребления сервисом и другой аномальной деятельности.

Vulnerability - Уязвимость
Ошибка или недостаток в разработке системы, реализации или эксплуатации и управлении, которые могут быть использованы для нарушения политики безопасности системы.

W

War Chalking - Разметка Мелом
War Chalking означает отметку областей, как правило, на тротуарах мелом, в которые можно получать беспроводные сигналы, которые могут быть использованы для беспроводного доступа.

War Dialer – Разведывательный дозвон
War Dialer - это компьютерная программа, которая автоматически набирает серии телефонных номеров, чтобы найти линий, подключенные к компьютерным системами, и записать эти номера в каталог для того, чтобы злоумышленник мог попытаться взломать системы.

War Dialing - Разведка дозвоном
War Dialing является процессом, который используется для поиска модемов, подключенных к телефонной станции, и определения их восприимчивости к компромиссу и возможности обойти периметр безопасности.

War Driving – Транспортная разведка
War Driving - это процесс поиска в окружающем пространстве беспроводных точек доступа из транспортного средства. Обнаруженные коммуникационные каналы могут быть использованы для получения доступа к сети.

Web of Trust - Сеть доверия
Web of Trust - это процесс, естественного развития, когда пользователи начинают доверять друг другу и подписи другого пользователя, которому они доверяют.

Wired Equivalent Privacy (WEP) – Проводной эквивалент конфиденциальности
Протокол безопасности для беспроводных локальных сетей, определенный в стандарте 802.11b IEEE.

Worm - Червь
Компьютерная программа, которая может работать самостоятельно, распространить полную версию своего кода на другие узлы в сети и может разрушительно потреблять ресурсы компьютера.

Wrap - Обертка
Это сервис при помощи, которого работают программы шифрования для обеспечения конфиденциальности данных.

7. Ссылки

Департамент Национальной Безопасности США:

http://www.us-cert.gov/control_systems/

Каталог безопасности систем управления: рекомендации для разработчиков стандартов -2008

Guide to Industrial Control Systems (ICS) Security -National Institute of Standards and Technology (NIST), Keith Stouffer, Joe Falco, Karen Scarfone – 2008

Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program -U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, National SCADA Test Bed (NSTB) -2008

Control Control Systems Cyber Security: Defense in Depth Strategies – Idaho National Laboratory – May 2006

The Instrumentation, Systems and Automation Society (ISA):

Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks

2004

Mitigations for Security Vulnerabilities Found in Control System Networks -2006

2008 CSI Computer Crime & Security Survey -Robert Richardson, CSI Director

Design Secure Network Segmentation Approach -SANS Institute InfoSec Reading

Room – 2005

VLAN Best Practices – White paper FLUKE networks -2004

OPC Security Whitepaper #3 Hardening Guidelines for OPC Hosts -Digital Bond,

British Columbia Institute of Technology, Byres Research – 2007

http://www.vicomsoft.com/knowledge/reference/firewalls1.html

Schneider Electric в странах СНГ

Пройдите бесплатное онлайн-обучение в Энергетическом Университете и станьте профессионалом в области энергоэффективности.

Для регистрации зайдите на www.MyEnergyUniversity.com

Беларусь

Минск
220006, ул. Белорусская, 15, офис 9
Тел.: (37517) 226 06 74, 227 60 34, 227 60 72

Казахстан

Алматы
050009, пр-т Абая, 151/115
Бизнес-центр «Алатау»
Тел.: (727) 397 04 00
Факс: (727) 397 04 05

Астана
010000, ул. Бейбитшилик, 18
Бизнес-центр «Бейбитшилик 2002»
Офис 402
Тел.: (3172) 91 06 69
Факс: (3172) 91 06 70

Атырау
060002, ул. Абая, 2 А
Бизнес-центр «Сутас-С», офис 407
Тел.: (3122) 32 31 91, 32 66 70
Факс: (3122) 32 37 54

Россия

Волгоград
400089, ул. Профсоюзная, 15
Офис 12
Тел.: (8442) 93 08 41

Воронеж
394026, пр-т Труда, 65, офис 227
Тел.: (4732) 39 06 00
Тел./факс: (4732) 39 06 01

Екатеринбург
620014, ул. Радищева, 28, этаж 11
Тел.: (343) 378 47 36, 378 47 37

Иркутск
664047, ул. 1-я Советская, 3 Б, офис 312
Тел./факс: (3952) 29 00 07, 29 20 43

Казань
420107, ул. Спартаковская, 6, этаж 7
Тел./факс: (843) 526 55 84 / 85 / 86 / 87 / 88

Калининград
236040, Гвардейский пр., 15
Тел.: (4012) 53 59 53
Факс: (4012) 57 60 79

Краснодар
350063, ул. Кубанская набережная, 62 /
ул. Комсомольская, 13, офис 224
Тел.: (861) 278 00 62
Тел./факс: (861) 278 01 13, 278 00 62 / 63

Красноярск
660021, ул. Горького, 3 А, офис 302
Тел.: (3912) 56 80 95
Факс: (3912) 56 80 96

Москва
129281, ул. Енисейская, 37, стр. 1
Тел.: (495) 797 40 00
Факс: (495) 797 40 02

Мурманск
183038, ул. Воровского, д. 5/23
Конгресс-отель «Меридиан»
Офис 739
Тел.: (8152) 28 86 90
Факс: (8152) 28 87 30

Нижний Новгород
603000, пер. Холодный, 10 А, этаж 8
Тел./факс: (831) 278 97 25, 278 97 26

Новосибирск
630132, ул. Красноярская, 35
Бизнес-центр «Гринвич», офис 1309
Тел./факс: (383) 227 62 53, 227 62 54

Пермь
614010, Комсомольский пр-т, 98, офис 11
Тел./факс: (342) 290 26 11 / 13 / 15

Ростов-на-Дону
344002, ул. Социалистическая, 74, литера А
Тел.: (863) 200 17 22, 200 17 23
Факс: (863) 200 17 24

Самара
443096, ул. Коммунистическая, 27
Тел./факс: (846) 266 41 41, 266 41 11

Санкт-Петербург
196158, Пулковское шоссе, 40, кор. 4, литера А
Бизнес-центр «Технополис»
Тел.: (812) 332 03 53
Факс: (812) 332 03 52

Сочи
354008, ул. Виноградная, 20 А, офис 54
Тел.: (8622) 96 06 01, 96 06 02
Факс: (8622) 96 06 02

Уфа
450098, пр-т Октября, 132/3 (бизнес-центр КПД)
Блок-секция № 3, этаж 9
Тел.: (347) 279 98 29
Факс: (347) 279 98 30

Хабаровск
680000, ул. Муравьева-Амурского, 23, этаж 4
Тел.: (4212) 30 64 70
Факс: (4212) 30 46 66

Украина

Днепропетровск
49000, ул. Глинки, 17, этаж 4
Тел.: (380567) 90 08 88
Факс: (380567) 90 09 99

Донецк
83087, ул. Инженерная, 1 В
Тел.: (38062) 385 48 45, 385 48 65
Факс: (38062) 385 49 23

Киев
03057, ул. Смоленская, 31-33, кор. 29
Тел.: (38044) 538 14 70
Факс: (38044) 538 14 71

Львов
79015, ул. Тургенева, 72, кор. 1
Тел./факс: (38032) 298 85 85

Николаев
54030, ул. Никольская, 25
Бизнес-центр «Александровский», офис 5
Тел./факс: (380512) 58 24 67, 58 24 68

Одесса
65079, ул. Куликово поле, 1, офис 213
Тел./факс: (38048) 728 65 55, 728 65 35

Симферополь
95013, ул. Севастопольская, 43/2, офис 11
Тел.: (380652) 44 38 26
Факс: (380652) 54 81 14

Харьков
61070, ул. Академика Проскуры, 1
Бизнес-центр «Telesens», офис 569
Тел.: (38057) 719 07 79
Факс: (38057) 719 07 49

Центр поддержки клиентов
Тел.: 8 (800) 200 64 46 (многоканальный)
Тел.: (495) 797 32 32, факс: (495) 797 40 04
ru.csc@ru.schneider-electric.com
www.schneider-electric.ru

MKP-TECHCOL36-11
04/2011