Шлюз однонаправленной передачи данных

Назначение шаблона

Шаблон предназначен для организации однонаправленной передачи данных из внутренней сети во внешнюю.

Примечание: *Шаблон с некоторой модификацией может использоваться для организации однонаправленной передачи данных из внешней сети во внутреннюю. Он используется в том случае, если целью является обеспечение конфиденциальности ресурсов во внутренней сети. Модификация исключает использование исходного шаблона.*

Типовые цели безопасности

Типовые цели безопасности при применении шаблона включают:

- отсутствие влияния агентов во внешней сети на внутреннюю сеть;
- обеспечение конфиденциальности и целостности ресурсов во внутренней сети;
- защиту внутренней компьютерной сети от атак.

Предположения безопасности

Предположения безопасности включают доверие к элементу системы, обеспечивающему передачу данных (для ПО программного-аппаратного шлюза – к драйверу сетевой карты).

Предположения и условия, при которых шаблон не может быть применен: существование альтернативных каналов связи внешней и внутренней сети.

Описание решения

Элементы системы, реализующей шаблон:

- агент источника данных;
- агент получателя данных;
- сервис обработки данных;
- монитор безопасности.

Разграничение доступа к внутренней и внешней сети обеспечивается использованием физически раздельных сетевых карт или реализацией шаблона «Разделение потоков данных на уровне драйвера ресурсов».

Монитор реализуется на основе шаблона «Монитор».

Взаимодействие элементов шаблона представлено на рисунке 1.

Рисунок 1 – Выделенный обработчик для очистки данных

Алгоритм осуществления однонаправленной передачи данных на основе шаблона:

Шаг 1 — Агент источника передает в сервис обработки данных информацию, которую требуется передать агенту-получателю;

Шаг 2 — Сервис обработки данных устанавливает маршрут передачи между агентом источника и агентом получателя, монитор отслеживает факт выполнения запроса и его параметры как минимум, получая информацию от сервиса обработки данных. Монитор может также независимо получать данные для отслеживания запросов из внутренней и внешней сети, к примеру, на интерфейсах взаимодействия агентов источника и получателя с внутренней и внешней сетью соответственно;

Шаг 3 — Агент получателя принимает данные и отправляет их во внешнюю сеть.

При попытке передачи любых данных из агента-получателя в сервис обработки данных срабатывает политика, запрещающая выполнение передачи данных. Попытки установления прямого соединения с внешней сетью и запросы из внешней сети отслеживаются монитором.

Требования к технологии разработки элементов системы

Поскольку шаблон использует шаблон «Монитор», применяются требования к технологии, определенные для базового шаблона.

Поскольку шаблон реализуется на основе шаблона «Разделение потоков данных на уровне драйверов устройств», применяются требования к технологии, определенные для базового шаблона.

Ограничения на применение шаблона

Поскольку шаблон реализуется на основе шаблона «Разделение потоков данных на уровне драйверов устройств», применяются ограничения, определенные для базового шаблона и шаблона «Монитор».

Допустимые модификации шаблона

Допустимость модификаций шаблона должна быть обоснована при проектировании архитектуры и формировании требований, предъявляемых к системе на основе целей и предположений безопасности для этой системы.