Table of Contents

Общее описание

В случае DoS атаки злоумышленнику важно замаскировать обратный адрес, чтобы его было невозможно блокировать по IP. Поэтому DoS атака представляет собой бомбардировку серверов жертвы отдельными пакетами с фиктивным обратным адресом. Отказ в обслуживании в этом случае наступает либо вследствие переполнения (забивания трафиком) арендуемой клиентом полосы, либо при бомбардировке пакетами, которые вызывают повышенный расход ресурсов на атакуемой системе.

В первом случае единственной эффективной защитой является временная аренда широкого канала и перенаправление на него всего входящего трафика через BGP анонс или DNS. Данный вид защиты обычно предлагается специализированными компаниями, но в ограниченных масштабах может осуществляться оператором или клиентом самостоятельно.

Во втором случае оператор или клиент могут самостоятельно организовать защиту, отфильтровав зловредные пакеты данных из входящего трафика до того, как они достигнут атакуемую систему.

Типичными атаками такого рода являются:

1. SYN flood - атака SYN пакетами
2. RST flood - атака RST пакетами [1)]
3. fragmented UDP flood - атака фрагментированными UDP пакетами

Современные операционные системы умеют в определенных пределах противостоять этим видам атак, но если они не справляются, то решением проблемы является использование системы фильтрации, установленной перед атакуемой системой.

1)
наши тесты показали, что против современных ОС эта атака неэффективна, но если эксплуатация покажет, что защита от этого типа атак по прежнему востребована, то мы добавим ее в ближайших обновлениях