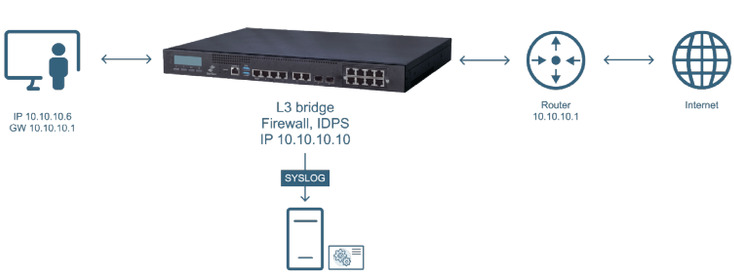
Система обнаружения вторжения (СОВ) в решениях UserGate

Компания UserGate использует в составе своего межсетевого экрана нового поколения систему обнаружения вторжений собственной разработки, созданную внутри компании без использования открытого кода.

Все применяемые сигнатуры для СОВ разрабатываются и верифицируются собственной командой аналитиков Центра мониторинга и реагирования UserGate (MRC-UG). На сегодня аналитиками центра разработано более 6000 сигнатур, и каждый день их число увеличивается. При разработке правил используется также и информация от различных центров реагирования на компьютерные инциденты, в том числе ФинЦЕРТ Банка России и GOV-CERT НКЦКИ.

Работа с зеркальным трафиком со SPAN порта коммутатора



Работа с транзитным графиком в режимах L3 или L2/L3 bridge

UserGate может использоваться как в режиме мониторинга, так и в режиме блокировки (IPS и IDS). UserGate обеспечивает защиту сети, выявляя во входящем и исходящем трафиках признаки атак, использующих те или иные известные уязвимости или осуществляющую вредоносную активность.

Так, например, распознаются признаки протоколов ботнет сетей, сигнатуры вирусов и т.п., а также действия пользователей, противоречащие корпоративной политике компании (например, использование торрентов).

Эвристические алгоритмы позволяют выявить новые или измененные способы атак, повышая уровень защищенности.

UserGate

О центре мониторинга и реагирования UserGate (MRC- UG)

Центр мониторинга и реагирования UserGate – это команда специалистов по информационной безопасности, которая занимается исследованием сетевых угроз. Сотрудники центра на регулярной основе ведут мониторинг появления новых опасностей и анализируют методы проникновения злоумышленников в корпоративные сети.

Специалисты Центра мониторинга и реагирования UserGate анализируют множество потоков данных таких как:

- данные от всевозможных платных подписок;
- информация с публичных и собственных honeypots;
- появление нового вредоносного ПО;
- появление новых уязвимостей как в российских (fin-cert, gov-cert и др.), так и в международных базах уязвимостей;
- данные за счет технологического партнерства с другими компаниями;
- публикации от исследователей информационной безопасности.

На основании этого опыта, как собранного в результате расследований инцидентов, так и полученного при изучении внешних материалов, специалисты центра разрабатывают новые и обновляют существующие сигнатуры хакерских атак.

Источники информации об инцидентах безопасности

UserGate создает свои сигнатуры на основе:

- образцов вредоносного трафика;
- публичных proof of concept на уязвимости;
- информации от различных CERT;
- анализа собираемых IoC.