PROLAN

ДИАГНОСТИКА
И УПРАВЛЕНИЕ СЕТЬЮ –
ТЕПЕРЬ РЕМЕСЛО,
А НЕ ИСКУССТВО

www.prolan.ru/prodefense

ProDefense™

Раннее Обнаружение Сетевых Аномалий

ProDefense™ – это комплексное решение компании ProLAN, включающее программные продукты и профессиональный сервис, предназначенное для быстрого выявления аномалий в работе IT-инфраструктуры. Решение ProDefense™ является примером использования пакета ProLAN NPM Analyst для повышения уровня информационной безопасности компании. Предлагаемое решение основано на технологиях ProLAN SLa-ON™ , NetFlow™, sFlow™, Cisco SAA, Cisco QoS, Iperf, SNMP, RMON, WMI и других.

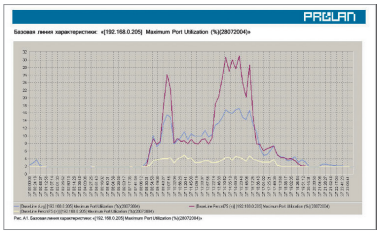
ProDefense™ – это решение «под ключ». Эксперты компании ProLAN предоставят все необходимое программное и аппаратное обеспечение и выполнят все работы по их установке и настройке. В результате вы получите готовую к применению систему, которая будет автоматически информировать администратора сети об аномалиях, являющихся следствием вирусной активности, хакерских атак, злонамеренных действиях внутренних пользователей, системных сбоев и т.п.

Решение ProDefense™ позволит вам:

- Автоматически получать Базовые Линии, характеризующие типичную работу IT-Инфраструктуры.
- Автоматически получать уведомление, если IT-Инфраструктура начинает работать не так, как обычно.
- Быстро определять причину нетипичной работы IT-Инфраструктуры.

Защищаемые компоненты сети:

- Коммутаторы, маршрутизаторы.
- Межсетевые экраны.
- Серверы MS Windows NT/2000/2003/XP.
- Каналы связи.
- Оборудование сетей VoIP.
- Последняя миля.
- Сервисы и приложения.



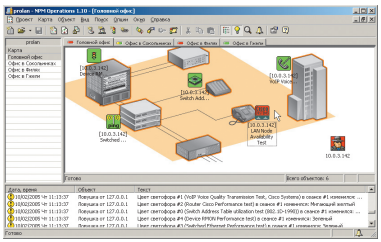
В рамках ProDefense™ могут создаваться базовые линии всех основных компонент IT-Инфраструктуры – коммутаторов, маршрутизаторов, межсетевых экранов, серверов, каналов связи, различных приложений и т.п.

Определение типичной работы IT-Инфраструктуры

Автоматическое построение Базовых Линий, характеризующих типичную работу IT-Инфраструктуры.

Базовая Линия характеристики – это результат статистической обработки значений этой характеристики. В ProDefense™ – это три метрики (среднее, перцентиль 75>, перцентиль 75<), показывающие каковы наиболее вероятные значения измеряемой характеристики. Например, чтобы получить Базовую Линию утилизации сети, значения этой характеристики нужно непрерывно измерять в течение длительного времени (не менее недели) и затем статистически обработать. В результате будут получены три новые метрики – средняя утилизация сети, утилизация сети – перцентиль 75>, утилизация сети – перцентиль 75<. Если посмотреть на графики этих характеристик, то можно увидеть, что между ними образуется «вероятностная труба». Если значение утилизации сети попадает в эту трубу, значит оно типично для данной сети.

Для расчета Базовых Линий используется сервис Тест-Ателье™ или программа NPM Reporter.



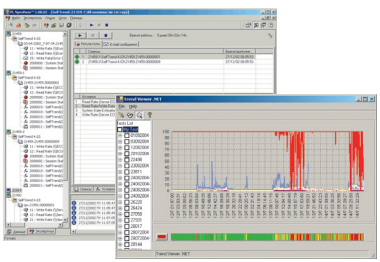
В рамках ProDefense™ для оповещения об аномалиях используется программа NPM Operations, входящая в состав пакета NPM Analyst, или уже используемое в сети клиента приложение Service Desk.

Оповещение об аномалиях

Оперативное оповещение о нетипичной работе IT-Инфраструктуры.

Зонд NPM Probe+ не только измеряет значения различных характеристик, но и автоматически сравнивает измеряемые значения с Базовой Линией. На основе результатов сравнения формируется интегральная оценка, имеющая вид светофора. Если IT-Инфраструктура работает типично, то светофор горит зеленым цветом. Как только IT-Инфраструктура начинает работать нетипично, светофор автоматически меняет свой цвет. Использование специального алгоритма предотвращает ложные срабатывания светофора.

Если в сети клиента используется приложение Service Desk, например HP OpenView Service Desk, то информация о нетипичной работе IT-Инфраструктуры (Trouble Ticket) автоматически доставляется в приложение Service Desk.



Чтобы определить причину аномальной работы IT-инфраструктуры вручную можно использовать программу Trend Viewer, для автоматического определения причин аномалий следует использовать экспертную систему NPM Visor.

Локализация причины аномалий

Быстрое определение причин нетипичной работы IT-Инфраструктуры.

Решение ProDefense™ позволяет решать эту задачу двумя способами – вручную и автоматически. В первом случае достаточно кликнуть на пиктограмму светофора и программа NPM Operations автоматически загрузит «сырые данные», из которых состоит светофор, а также вызовет программу Trend Viewer, представляющую сырые данные в удобном для анализа виде. Сопоставив «сырые данные» со светофором, можно установить причину аномалии

Если «сырых данных» много, для установления причины аномалий можно использовать экспертную систему NPM Visor, которая в режиме реального времени анализирует измеряемые характеристики и при обнаружении источника аномалий автоматически сообщает об этом администратору сети или оператору приложения Service Desk.