[illegible] (NGFW) [illegible]

[illegible]

[illegible] next-generation firewall [illegible] (NGFW) [illegible]:

application awareness ([illegible])

integrated intrusion prevention systems (IPS) [illegible]-

identity awareness -- user and group control[illegible] -

bridged and routed modes [illegible]-

the ability to use external intelligence sources [illegible] -

Межсетевые экраны нового поколения

Межсетевые экраны нового поколения (NGFW) — это устройства, которые выполняют функции традиционных межсетевых экранов, а также дополнительные функции, такие как глубокая инспекция пакетов, предотвращение вторжений, фильтрация контента, VPN-шлюзы, SSL- и SSH-инспекция, а также функции управления качеством обслуживания (QoS). Они работают на более высоких уровнях модели OSI, обычно на уровнях 4–7.

Прокси-серверы

Прокси-серверы — это промежуточные серверы, которые принимают запросы от клиентов и перенаправляют их на целевые серверы. Они могут использоваться для кэширования, фильтрации контента, анонимизации и обхода ограничений. Прокси-серверы могут работать на различных уровнях модели OSI, от прикладного до транспортного.

Системы обнаружения и предотвращения вторжений

Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS) — это устройства, которые анализируют сетевой трафик на предмет признаков вредоносной активности. IDS только обнаруживает и сообщает о подозрительной активности, в то время как IPS может также блокировать вредоносный трафик. Они могут использовать сигнатурный анализ, анализ аномалий или поведенческий анализ.

Трансляция сетевых адресов

Трансляция сетевых адресов (NAT) — это процесс изменения IP-адресов в заголовках пакетов при их прохождении через маршрутизатор. NAT используется для экономии IP-адресов, скрытия внутренней структуры сети и обеспечения доступа к внешним ресурсам. Существуют различные типы NAT, такие как статический NAT, динамический NAT и PAT (Port Address Translation).

Демилитаризованная зона

Демилитаризованная зона (DMZ) — это сегмент сети, который находится между внутренней сетью и внешней сетью (Интернетом). DMZ используется для размещения серверов, которые должны быть доступны из Интернета, таких как веб-серверы, почтовые серверы и DNS-серверы. Это позволяет изолировать эти серверы от внутренней сети, чтобы в случае компрометации они не представляли угрозу для внутренних ресурсов.

رمزگذاری قدرتمند در لایه وب، ضدویروس‌ها و ضدبدافزارها هنوز هم برای محافظت از شبکه‌های سازمانی لازم است.

در مقرون به صرفه‌ترین حالت، سازمان‌ها باید به فکر استقرار محصولات امنیتی تحت شبکه قدرتمند و نظارت مستمر بر ترافیک شبکه با هدف کاهش بردارهای حمله ناهمگن باشند . علاوه بر این، تعامل میان محصولات امنیتی می‌تواند به بهبود عملکرد محصولات امنیتی، کاهش مصرف منابع و پهنای باند، زمان پاسخگویی سریع‌تر و دفع حملاتی که توسط مکانیزم‌های رایج شناخته نمی‌شوند، اما دیوارهای آتش و ضدویروس‌های جدید قادر به شناسایی آن‌ها هستند کمک فراوانی کند .

نویسنده :
حمیدرضا_تائبی
دسته بندی:
امنیت
تاریخ انتشار :
12:10 - 29/12/1398
برچسب:
دیوار آتش نسل_بعد - next-generation firewall - دیوار آتش NGFW

نشانی
□□□□:https://www.shabakeh-mag.com/security/16660/%D8%AF%DB%8C%D9%88%D8%A7%D8%B1-%D8%A2%D8%AA%D8%B4%E2%80%8C-%D9%86%D8%B3%D9%84-%D8%A8%D8%B9%D8%AF-ngfw-%DA%86%DB%8C%D8%B3%D8%AA-%D9%88-%DA%86%D9%87-%D9%82%D8%A7%D8%A8%D9%84%DB%8C%D8%AA%DB%8C-%D8%AF%D8%A7%D8%B1%D8%AF%D8%9F