A análise de tráfego de rede (NTA) é a prática de monitorar e interpretar os dados que fluem pela rede para garantir desempenho, confiabilidade e segurança. As empresas contam com uma combinação de ferramentas — desde detectores de pacotes e software de análise de fluxo até sistemas avançados de NDR — para obter visibilidade do comportamento de sua rede.

Este guia explora os tipos de soluções NTA disponíveis, os principais recursos que fornecem visibilidade e controle sobre sua rede e onde tecnologias relacionadas, como ferramentas NDR, se encaixam em uma estratégia de rede moderna e segura.

Mas, primeiro, quero começar com alguns sinais de alerta que indicam que o tráfego de rede está escondendo gargalos de desempenho, ameaças cibernéticas sofisticadas ou ambos. Confiar nas ferramentas de ontem pode significar perder sinais de alerta críticos.

O que você vai ler:

Sete sinais de que você deve renovar a análise de tráfego de rede

Idealmente, a análise de tráfego de rede (NTA) oferece aos administradores uma visão clara e em tempo real de como os dados se movem pela rede. Isso os ajuda a detectar problemas de desempenho, monitorar o uso de recursos e identificar possíveis ameaças à segurança antes que se tornem problemas sérios.

Quando as ferramentas e a estratégia da NTA deixam pontos cegos críticos, ela não conseguirá detectar problemas de desempenho, ameaças à segurança ou padrões de tráfego inesperados que possam interromper as operações.

Abaixo estão alguns sinais de alerta e cenários que justificam uma revisão de sua abordagem atual e podem indicar a necessidade de uma reformulação estratégica de sua

análise de tráfego de rede. As bandeiras vermelhas incluem:

1. **Incidentes de segurança ou atividades suspeitas:** Um aumento nas violações de rede, acesso não autorizado ou fluxos de tráfego incomuns (por exemplo, tentativas de exfiltração de dados ou ataques DDoS) indica que sua estratégia atual pode não monitorar ameaças adequadamente ou alertá-lo em tempo real.
2. **Picos de tráfego imprevisíveis:** Se você notar aumentos inesperados no tráfego, como fora do horário comercial ou em períodos em que deveria haver baixa atividade, isso pode indicar um problema no modo como o tráfego está sendo gerenciado ou até mesmo atividade maliciosa. Se persistirem picos imprevisíveis, reavalie suas ferramentas de monitoramento de desempenho e detecção de ameaças para confirmar se elas estão proporcionando visibilidade total.
3. **Falta de visibilidade sobre tipos de tráfego específicos:** Se suas ferramentas ou estratégias existentes não fornecem informações claras sobre tipos específicos de tráfego — como VoIP, streaming ou dados criptografados — talvez seja hora de atualizar para uma solução mais sofisticada que ofereça inspeção profunda de pacotes e maior granularidade.
4. **Relatórios ou alertas inconsistentes:** Se o seu sistema atual não estiver fornecendo relatórios consistentes e acionáveis ou alertas oportunos, é um sinal de que a estratégia de tráfego de rede pode estar desatualizada ou configurada incorretamente. Revise seus limites, regras de detecção e políticas de alertas.
5. **Mudanças na infraestrutura de rede ou nas demandas de tráfego:** À medida que a infraestrutura de rede evolui (por exemplo, mudança para serviços em nuvem, trabalho remoto ou aumento da IoT), é crucial garantir que suas ferramentas e abordagem de NTA sejam adaptadas a essas mudanças, garantindo monitoramento e gerenciamento de tráfego contínuos.
6. **Dados de rede desconectados:** Se suas ferramentas NTA não estiverem bem integradas em vários segmentos ou sistemas de rede, pode ser difícil obter uma visão completa do desempenho da rede ou das ameaças à segurança. Uma abordagem unificada à análise de tráfego pode ser necessária para uma melhor compreensão.
7. **Conformidade ou alterações regulatórias:** Se novas regulamentações de conformidade ou padrões do setor (como GDPR ou HIPAA) afetarem a proteção e a privacidade de dados, poderá ser necessário revisar sua estratégia de NTA para garantir que ela atenda a esses requisitos e evite possíveis penalidades.

Há outros sinais de alerta que não capturei aqui, e novas explorações de dia zero surgem todos os dias.

Adotar uma abordagem proativa com a NTA é uma ideia sábia. Operar com visibilidade inferior ao tráfego de rede é sinônimo de problemas – tanto o desempenho quanto a segurança estão em jogo.

Afinal, depois de terem acesso à sua rede, leva apenas dois dias para que os invasores possuam seus dados.

memória virtual

O que torna tão difícil melhorar a análise do tráfego de rede?

À medida que a tecnologia NTA evolui, torna-se cada vez mais poderosa e capaz de identificar ameaças sofisticadas.

Mas esses recursos aprimorados vêm com uma ressalva importante: você precisa de alguns recursos de TI realmente bem pagos internamente. Quanto mais avançada for a ferramenta, maior será o nível de experiência, conhecimento e mão de obra necessários para operá-la e gerenciá-la com eficácia.

Uma rede básica para um único escritório pode ser relativamente simples de implementar e monitorar com um mínimo de experiência. Uma grande rede com plataformas NTA de ponta requer profissionais de segurança qualificados que possam interpretar dados complexos, responder rapidamente a ameaças e ajustar o sistema para se adaptar às novas técnicas de ataque e tendências de ransomware.

Estes factores tornam as poderosas soluções NTA mais intensivas em recursos, exigindo pessoal qualificado e formação contínua para manter a sua eficácia. As organizações devem considerar não apenas as capacidades tecnológicas de uma solução NTA, mas também a capacidade da sua equipa para gerir e maximizar o seu potencial.

Tipos de ferramentas de análise de tráfego de rede

As ferramentas de análise de tráfego de rede são essenciais para monitorar e otimizar o fluxo de dados em uma rede. Eles ajudam a identificar gargalos, solucionar problemas e garantir o uso eficiente dos recursos. As principais categorias de ferramentas de análise de tráfego de rede são:

- **Farejadores de pacotes:** Essas ferramentas capturam e analisam o tráfego bruto da rede no nível do pacote. Ferramentas comuns, como o Wireshark, fornecem insights profundos sobre os tipos de dados que estão sendo transferidos e ajudam a identificar problemas como perda de pacotes ou incompatibilidades de protocolo.
- **Ferramentas de análise de fluxo:** Ferramentas como SolarWinds e NetFlow Analyzer rastreiam dados de fluxo, que mostram como o tráfego se move através de uma rede em termos de sessões ou conexões. Essas ferramentas concentram-se em dados agregados, como uso de largura de banda, o que ajuda a compreender o desempenho geral da rede.
- **Monitores de desempenho de rede:** Essas ferramentas, como o PRTG Network Monitor, analisam o tráfego e a integridade geral da rede, incluindo latência, taxa de transferência e status do dispositivo. Eles fornecem recursos de monitoramento e alerta em tempo real para rastrear tendências de desempenho e detectar anomalias.
- **Sistemas de Detecção de Intrusão (IDS):** Essas ferramentas, como Zeek e Snort,

monitoram o tráfego em busca de sinais de atividades suspeitas, como acesso não autorizado ou ataques. Eles se concentram no aspecto de segurança do tráfego de rede, analisando padrões e comportamentos.

Muitas das principais ferramentas para análise de tráfego de rede combinam múltiplas funcionalidades em uma única plataforma. Alguns exemplos de ferramentas “tudo-em-um” incluem SolarWinds NPM e PRTG Network Monitor, que fornecem soluções abrangentes para monitorar e analisar o tráfego de rede.

VEJO: Confira esta análise do SolarWinds NPM e esta análise do PRTG Network Monitor para saber mais sobre eles.

Essas plataformas normalmente integram detecção de pacotes, análise de fluxo, monitoramento de desempenho e até recursos de segurança em uma única interface, tornando-as altamente eficientes para organizações que precisam de uma visão ampla do desempenho e da segurança de sua rede.

No outro extremo do espectro, você poderá encontrar algumas ferramentas gratuitas que podem realizar algumas dessas tarefas – embora de forma limitada, com muitos upsell para sua ferramenta paga.

Uma última coisa a observar: você ainda terá que implementar uma solução separada de Detecção e Resposta de Rede (NDR) para fortalecer efetivamente a segurança da rede. As ferramentas NTA “integrais” têm recursos de NDR limitados – a maioria das organizações usa ambos para se proteger contra ataques de ameaças persistentes avançadas (APT).

Principais recursos de análise de tráfego de rede

Concentre-se nos recursos que ajudarão você a atingir os principais objetivos da análise de tráfego de rede: aumentar a visibilidade, otimizar o desempenho, garantir a segurança e manter a eficiência operacional.

Esses são cinco dos recursos gerais mais importantes nos quais acho que a maioria das pessoas estará interessada. Eles também são recursos cuja profundidade varia de fornecedor para fornecedor.

1. Monitoramento e alertas em tempo real

A capacidade de monitorar o tráfego de rede em tempo real e receber alertas sobre comportamento incomum ou degradação de desempenho é essencial para solução de problemas proativa e resposta imediata.

A maioria das soluções NTA oferece monitoramento e alertas em tempo real – uma boa solução minimiza a fadiga dos alertas ao priorizar insights acionáveis. Procure ferramentas

que forneçam alertas sensíveis ao contexto com detalhes relevantes e permitam limites personalizáveis para atender às necessidades exclusivas da sua rede.

Outra forma de reduzir alarmes falsos e alertas intermináveis é utilizar uma solução NTA com correlação e agrupamento de alertas, que pode consolidar notificações relacionadas. Isso pode ajudar sua equipe a manter o foco nos problemas certos, em vez de ficar sobrecarregada com alertas redundantes ou de baixa prioridade.

2. Classificação automatizada de tráfego

Muitas ferramentas NTA podem realizar categorização básica de tráfego, como distinguir entre tipos de dados gerais como HTTP, DNS ou FTP. Um recurso de classificação de tráfego automatizado mais poderoso vai além da categorização básica, oferecendo identificação granular de aplicativos, protocolos e tipos de dados, garantindo a alocação precisa de recursos.

Por exemplo, ferramentas avançadas de NTA podem reconhecer e categorizar aplicativos específicos, como identificar o tráfego do Microsoft Teams em comparação com a navegação geral na web. Isso é fundamental para identificar a origem dos picos de tráfego, por exemplo, e torna mais fácil priorizar recursos discretos e melhorar o desempenho geral da rede.

3. Relatórios detalhados e dados históricos

A capacidade de gerar relatórios detalhados e personalizáveis permite que as equipes acompanhem tendências ao longo do tempo, identifiquem problemas recorrentes e tomem decisões baseadas em dados para planejamento de capacidade ou alocação de recursos. Os dados históricos são particularmente valiosos para diagnosticar problemas intermitentes e realizar análises pós-incidentes, oferecendo uma imagem mais clara do que ocorreu e porquê.

4. Visibilidade e descriptografia aprofundadas

Não deixe a criptografia ocultar atividades maliciosas. Escolha uma solução NTA que analise tráfego criptografado e não criptografado para descobrir ameaças ocultas em túneis de dados. Além disso, procure recursos que vão além dos cabeçalhos de pacotes para analisar protocolos, aplicativos e comportamento do usuário para fornecer informações detalhadas sobre a atividade da rede. Escolha sempre um NTA que rastreie o movimento lateral para expor adversários que se movem através de canais laterais e evitar que ameaças passem despercebidas na sua rede.

5. Integração com outras ferramentas de gerenciamento de rede

A integração com outras soluções de gerenciamento de rede, como sistemas de

monitoramento de desempenho de rede (NPM) e gerenciamento de eventos e informações de segurança (SIEM), é vital para criar uma visão unificada da integridade da sua rede.

Se o objetivo é aumentar a visibilidade, não deixe que as ferramentas de rede vivam em silos.

Existem muitos recursos adicionais, desde detecção avançada de anomalias até painéis personalizáveis, que podem ajudar a adaptar a ferramenta às necessidades exclusivas da sua rede. A chave não está apenas em selecionar os recursos certos, mas em usá-los de forma eficaz para obter insights práticos sobre o desempenho e a segurança da sua rede.

No final das contas, a ferramenta mais poderosa é a experiência da equipe que a utiliza.

O valor real da sua solução NTA reside em quão bem seus profissionais entendem e aproveitam seus recursos. À medida que você avança, confie que a combinação da tecnologia avançada e do conhecimento da sua equipe fornecerá os insights necessários para se manter à frente das ameaças em evolução e otimizar o desempenho da rede com confiança.