

É uma realidade que a segurança está no topo das prioridades das empresas e que todas, independentemente da sua dimensão, requerem elevados níveis de segurança no acesso à Internet, em parte devido ao número crescente de ameaças e vulnerabilidades a que estão sujeitas as infra-estruturas de TI.

É assumido que o perímetro de segurança das organizações passou a ser bastante mais alargado, o que implica uma maior atenção no controlo e acesso aos recursos da rede. Para fazer face a este desafio as empresas têm realizado grandes investimentos em complexos sistemas de protecção no perímetro de segurança, desde o firewall, passando pelos antivírus, anti-spam até aos mecanismos de detecção e prevenção de intrusões, etc.

A gestão da segurança é para muitas empresas um verdadeiro problema, uma vez que operar correctamente múltiplos dispositivos de segurança é uma tarefa complexa que exige recursos especializados e dedicados. Por vezes as empresas relegam a gestão destes sistemas para segundo plano, no entanto esta gestão é crucial para a sua eficácia de actuação.

De nada servirá à empresa realizar importantes investimentos em soluções de segurança, se no final do dia não tiver a devida atenção à sua operação, manutenção e gestão. É também importante salientar que a manutenção acarreta custos de exploração que serão tão mais altos quanto maior for o número de equipamentos, licenças e sua complexidade tecnológica.

É aqui que as **soluções UTM Firewall (Unified Threat Management)** da PT Prime podem fazer a diferença, ao proporcionarem aos seus clientes uma solução de segurança unificada, adequada tanto a pequenas, como a médias e grandes empresas, independentemente do seu sector de actividade.

As soluções UTM Firewall da PT Prime, são comercializadas em regime de serviço, sem investimentos avultados e incorporam várias funcionalidades avançadas de segurança. As UTM Firewall são appliances que possuem uma única interface de gestão para todas as aplicações, de onde se destacam, firewall, prevenção de intrusão, antivírus, antispam, filtragem URL, QoS, VPN, SSL VPN, etc.

Firewall

As avançadas técnicas de segurança presentes na UTM Firewall, permitem a identificação e prevenção de ataques até ao nível da aplicação (nível 7 OSI). A maioria dos ataques complexos situa-se, hoje em dia, ao nível aplicacional, particularmente no tráfego http. É por isso que se torna obrigatória uma análise mais inteligente e precisa dos fluxos de tráfego IP ao nível do firewall.

Prevenção de Intrusão

O ASQ (Active Security Qualification) é o motor de prevenção de intrusões das soluções UTM Firewall. Este módulo, oferece o mais alto nível de segurança para desempenhos inigualáveis. O IPS (Intrusion Prevention System) completa as funcionalidades de segurança do firewall e garante uma prevenção contra intrusões em tempo real. Este tipo de desenvolvimento integrado corresponde ao objectivo da PT Prime em oferecer o mais elevado nível de segurança, combinando múltiplos módulos de análise.

Para oferecer um nível de segurança integral, a UTM Firewall utiliza as assinaturas como complemento da análise protocolar; a tecnologia ASQ, garante um nível óptimo de inspecção dos fluxos de tráfego IP, através da

combinação das tecnologias de análise protocolar, comportamental e contextual.

Prevenção de Ameaças do Dia - 0

O desenvolvimento do motor ASQ permite prevenir ataques ainda desconhecidos, isto significa ser capaz de proteger hoje contra ameaças ainda não conhecidas. Um exemplo concreto para ilustrar esta capacidade de fazer frente a novas ameaças, é o caso da vulnerabilidade que afectou os servidores de resolução de nomes (DNS) no ano passado: “DNS recursive attack” reportado por Kaminsky. Trata-se de uma vulnerabilidade que foi amplamente documentada nos meios de comunicação e que permitia aos atacantes ultrapassar os servidores web de sítios legítimos para capturar informação sensível, fundamentalmente as passwords dos utilizadores. Os servidores DNS dos clientes de UTM Firewall estavam já protegidos contra esta vulnerabilidade antes de ser conhecido ou reportado o problema, sem necessidade de actualizar, ou realizar patching do servidor de DNS para a última versão não vulnerável.

Filtragem de URL

A solução de filtragem de URL impede o acesso a sítios na Internet inadequados, sendo particularmente útil nas empresas, escolas e organismos governamentais.

Permite que as empresas beneficiem de aumentos de produtividade e reduzam os riscos de ilegalidade e de questões de privacidade. A solução de filtragem URL da UTM Firewall é um serviço integrado com uma base de dados dinâmica, que cataloga milhões de sites da Internet, classificando-os por categorias, sendo esta base de dados constantemente actualizada.

Antivírus

Devido à sua posição central no controlo da rede, a UTM Firewall é um elemento importante para garantir a correcta filtragem de vírus, worms, backdoors, trojan horses e outros tipos de malware que se encontram na Internet. Este serviço protege a rede de vírus, e restante malware, escondidos em tráfego SMTP, HTTP e POP3, utilizando o motor da Kaspersky Labs, sendo hoje considerado um dos melhores antivírus de rede disponível no mercado. Utilizando a segunda geração de análise heurística, desenhada para detectar vírus desconhecidos, serve-se também da sua gigantesca base de dados de assinaturas (mais de 200,000 assinaturas) para providenciar um efectivo sistema de defesa contra vírus gigantes e polimórficos.

Anti-Spam

Uma vez que o SPAM já representa mais de 70% do tráfego de email, a solução anti-Spam dos equipamentos UTM Firewall utiliza métodos bastante eficazes de detecção com elevadas taxas de detecção de Spam. As mensagens de Spam são reconhecidas ao nível do protocolo SMTP, onde o motor de anti-spam permite marcar os e-mails de Spam, sendo assim possível classificar automaticamente estas mensagens graças às Funções de "organização" do software de mail.

