



UNIVERSIDADE
ESTADUAL de LONDRINA

KAUEE ROCHA PUERTAS

SEGURANÇA, UNIFIED THREAT MANAGEMENT (UTM)

LONDRINA - PR
2023

Trabalho de Laboratório – 18/04/2023

Questão 01) O que é e quais suas funções?

Unified Threat Management (UTM) é um tipo de solução de segurança de rede que integra várias funções de segurança em um único dispositivo. As funções típicas incluem firewall, prevenção de intrusão, filtro de conteúdo da web, antivírus, antispam e detecção e prevenção de ameaças avançadas. A ideia por trás do UTM é simplificar a segurança da rede para empresas, fornecendo uma solução abrangente e fácil de gerenciar.

1. Firewall: proteção contra acesso não autorizado à rede.
2. Antivírus: proteção contra vírus, worms e outras ameaças de software malicioso.
3. Antispam: proteção contra e-mails não solicitados e indesejados.
4. Proteção contra intrusões: monitoramento e prevenção de tentativas de invasão.
5. Filtragem de conteúdo: bloqueio de conteúdo impróprio ou potencialmente perigoso.
6. VPN (Virtual Private Network): proteção da rede contra acesso não autorizado por meio de conexões seguras.
7. Gerenciamento de banda: controle do uso de banda e priorização de tráfego.
8. Controle de aplicativos: limitação do acesso a aplicativos específicos ou categorias de aplicativos.

Questão 02) Qual o valor estimado para o mercado mundial de UTM?

O mercado mundial de Unified Threat Management (UTM) está relacionado à segurança cibernética e é projetado para ajudar a proteger as empresas de uma ampla gama de ameaças à segurança, como vírus, spam, spyware, malware, phishing e outros ataques cibernéticos. O mercado de UTM está em constante crescimento, com a crescente necessidade de segurança cibernética em empresas de todos os tamanhos em todo o mundo.

De acordo com um relatório de mercado da MarketsandMarkets de fevereiro de 2021, o tamanho do mercado global de UTM deve crescer de US\$ 3,5 bilhões em 2020 para US\$ 7,1 bilhões até 2025, com uma taxa de crescimento anual composta (CAGR) de 15,1% durante o período de previsão. No entanto, é importante notar que outras estimativas podem variar de acordo com a metodologia e fontes utilizadas.

Questão 03) Apresentar o estudo comparativo sobre pelo menos 4 produtos diferentes.

Detecção de Intrusão:

- Fortinet FortiGate: possui um mecanismo de detecção de intrusão integrado que usa assinaturas, anomalias e comportamento.
- Sophos XG Firewall: possui um mecanismo de detecção de intrusão integrado que usa assinaturas, anomalias e comportamento.
- WatchGuard Firebox: possui um mecanismo de detecção de intrusão integrado que usa técnicas de detecção de assinaturas e anomalias.
- SonicWall NSA: possui um mecanismo de detecção de intrusão integrado que usa técnicas de detecção de assinaturas e comportamento.

Vírus, Trojans, Spyware:

- Fortinet FortiGate: usa o FortiGuard Security Service para proteger contra vírus, trojans, worms, spyware, adware e phishing.
- Sophos XG Firewall: usa o Sophos Security Heartbeat para compartilhar informações com o software de proteção de endpoint da Sophos e proteger contra vírus, trojans, worms, spyware e outros malwares.
- WatchGuard Firebox: usa o WatchGuard Gateway AntiVirus para proteger contra vírus, trojans, spyware e outros malwares.
- SonicWall NSA: usa o SonicWall Gateway AntiVirus e o SonicWall Gateway Anti-Spyware para proteger contra vírus, trojans, spyware e outros malwares.

Spam:

- Fortinet FortiGate: inclui recursos de antispam.
- Sophos XG Firewall: inclui recursos de antispam.
- WatchGuard Firebox: inclui recursos de antispam.
- SonicWall NSA: não há informações claras sobre a capacidade da solução de lidar com spam.

Worms:

- Fortinet FortiGate: usa o FortiGuard Security Service para proteger contra worms.
- Sophos XG Firewall: não há informações claras sobre a capacidade da solução de lidar com worms.
- WatchGuard Firebox: não há informações claras sobre a capacidade da solução de lidar com worms.
- SonicWall NSA: não há informações claras sobre a capacidade da solução de lidar com worms.

IPS:

- Fortinet FortiGate: possui um mecanismo de prevenção de intrusões integrado.
- Sophos XG Firewall: inclui recursos de prevenção de intrusões.
- WatchGuard Firebox: inclui recursos de prevenção de intrusões.
- SonicWall NSA: inclui recursos de prevenção de intrusões.

Filtro URL:

- Fortinet FortiGate: possui um filtro de URL integrado.
- Sophos XG Firewall: inclui recursos de filtro de URL.
- WatchGuard Firebox: inclui recursos de filtro de URL.
- SonicWall NSA: não há informações claras sobre a capacidade da solução de lidar com filtro de URL.