Unified Threat Management (UTM)

Unified Threat Management (UTM)

Previously, you learned about several network security topics, including network hardening best practices, firewall essentials, and the foundations of IEEE 802.1X. In this reading, you will learn about a robust solution for network security, Unified Threat Management (UTM), along with its features, benefits, and risks.

UTM solutions stretch beyond the traditional firewall to include an array of network security tools with a single management interface. UTM simplifies the configuration and enforcement of security controls and policies, saving time and resources. Security event logs and reporting are also centralized and simplified to provide a holistic view of network security events.

UTM options and configurations

UTM solutions are available with a variety of options and configurations to meet the network security needs of an organization:

UTM hardware and software options:

- Stand-alone UTM network appliance
- Set of UTM networked appliances or devices
- UTM server software application(s)

Extent of UTM protection options:

- Single host
- Entire network

UTM security service and tool options can include:

- **Firewall:** Can be the first line of defense in catching phishing attacks, spam, viruses, malware, and other potential threats that attempt to access an organization's network. Firewalls can be hardware devices or software applications. Firewalls filter and inspect packets of data attempting to enter and exit a managed network. Rules can be configured to permit or prevent certain types of packets from entering the network.
- **Intrusion detection system (IDS):** Passively monitors packets of data and network traffic for unusual patterns that could indicate an attack. IDS devices can monitor entire networks (NIDS) or just a single host (HIDS). IDS identifies, logs, and alerts IT Support about suspicious traffic. However, IDS does not prevent an attack from occurring. This system gives IT Support professionals the opportunity to inspect flagged events to determine how to handle the threat on a case by case basis.
- **Intrusion prevention system (IPS):** Actively monitors packets and network traffic for potential malicious attacks. IPS systems can be configured to automatically block attacks or to allow manual interventions. IPS devices can monitor entire networks (NIPS) or just a single host (HIPS).
- **Antivirus software:** Uses a signature database to obtain the profiles of malicious files, such as spyware, Trojans, malware, worms, and more. The antivirus software monitors the organization's network and systems for these virus signatures. Once identified, the software will block, quarantine, or destroy them.
- **Anti-malware software:** Scans information streams for known malicious malware signatures and blocks threats. Additionally, anti-malware software can use heuristic analysis to detect novel malware threats by identifying key behaviors and characteristics. The software can also use sandboxing to isolate suspicious files.
- **Spam gateway:** Filters, identifies, and quarantines spam email. Spam gateways are network servers that use Domain Name Server (DNS) management tools to protect against spam.
- **Web and content filters:** Block user access to risky and malicious websites. When a user attempts to access an unauthorized or suspicious website using a browser, the UTM web filter can prevent the website from loading. The filter can also be customized to block certain types of websites or specific URLs, like social media or other websites that might be a distraction in the workplace.
- **Data leak/loss prevention (DLP):** Monitors outgoing network traffic for personal, sensitive, and confidential data. DLP includes a verification system to determine if the external data transfer is authorized or malicious, and can block unauthorized attempts.
- **Virtual Private Network (VPN):** Encrypts data and creates a private "tunnel" to safely transmit the data through a public network.

Stream-based vs. proxy-based UTM inspections

UTM solutions offers two methods for inspecting packets in UTM firewalls, IPS, IDS, and VPNs:

- **Stream-based inspection, also called flow-based inspection:** UTM devices inspects data samples from packets for malicious content and threats as the packets flow through the device in a stream of data. This process minimizes the duration of the security inspection, which keeps network data flowing at a faster rate than a proxy-based inspection.
- **Proxy-based inspection:** A UTM network appliance works as a proxy server for the flow of network traffic. The UTM appliance intercepts packets and uses them to reconstruct files. Then the UTM device will analyze the file for threats before allowing the file to continue on to its intended destination. Although this security screening process is more thorough than the stream-based inspection technique, proxy-based inspections are slower in the transmission of data.

Benefits of using UTM

UTM solutions can offer multiple benefits to an organization:

- **UTM can be cost-effective:** Reduces the time and resources needed to manage multiple stand-alone security tools. Purchasing a suite of integrated tools may also be less expensive than buying each tool separately.
- **UTM is flexible and adaptable:** Offers flexible solutions and options for security management. The security services and tools in a UTM can be implemented in any combination that is appropriate for each network environment.
- **UTM offers integrated and centralized management:** Consolidates multiple security tools into a central management console. This simplifies monitoring and addressing security threats, as well as streamlines the management of updates to the UTM components. The central management feature also helps IT Support staff identify and stop the full extent of an attack across an entire network.

Risks of using UTM

- **UTM can become a single point of failure in a network security attack:** If an attack disables an entire UTM solution, there would be no other backup security services or tools to stop that attack. One of the core principles of information systems management is to design and implement redundant, backup, and failover systems. When one element of an IT system is attacked or experiences a failure, there should always be a backup or parallel system to replace it.
- **UTM might be a waste of resources for small businesses:** Small businesses may not need a robust security solution like UTM. The time and money needed to purchase, implement, and manage a complex UTM system may not provide a significant return on security benefits for a smaller network. Cybercriminals are more likely to attack larger targets.

Key takeaways

- Unified Threat Management (UTM) systems offer multiple options in a comprehensive suite of network security tools. UTM solutions can be implemented as hardware and/or software and can protect either a single host or an entire network.
- UTM security services and tool options include firewalls, IDS, IPS, antivirus and anti-malware software, spam gateways, web and content filters, data leak/loss prevention, and VPN services.
- The benefits of using a UTM solution include having a cost-effective network security system that is flexible and adaptable with a management console that is integrated and centralized. The risks of using UTM include creating a single point of failure for a network security system and it might be an unnecessary use of resources for small businesses.

Mark as completed