NASSTAR

THE NASSTAR GUIDE TO UNIFIED THREAT MANAGEMENT

Unified threat management, otherwise known as UTM, is a term that refers to one safety solution and generally to a single security device that offers various security functions at one point in the network.

A UTM device will generally include anti-virus, anti-spyware, anti-spam, firewalling, detecting, and preventing intrusion, content filtering, and leak protection. Some devices include remote routing, network address translation, and support for virtual private networks (VPN).

The solution's appeal is built on simplicity, so organisations with individual suppliers or equipment for each specific security duty may now be supported by one single IT team or segment and operated via a console, under a single supplier umbrella.

IN THIS GUIDE, WE WILL COVER:

WHAT IS UNIFIED THREAT MANAGEMENT?

UTM is generally viewed as the answer to all risks associated with networking.

There are many dangers online. The most prevalent being malware attacks that can target multiple Internet components.

To prevent such assaults, several firms employ additional software. It might be tough to maintain and frequently update multiple applications to prevent these consequences. It gets tougher when you need to keep track of all the information with new applications and suppliers.

Both UTM and next-generation firewalls (NGFWs) serve a similar objective, but several areas are distinct.

Initially, NGFWs were designed to cover network security holes left by conventional firewalls, including application intelligence, the IPS, and DoS defense. UTM means that the NGFW, firewall, and virtual private network (VPN) functions to execute on a single device, whereas NGFW is a network security platform that offers an internal and external network gateway.

KEY FEATURES OF UTM INCLUDE:

Anti-virus

Antimalware

Firewall

Intrusion prevention

Virtual private networking

Data loss prevention

Web filtering

UTM FEATURES IN FIREWALLS

\\ Stateful firewall

\\ Deep inspection intrusion prevention

\\ Web & email antivirus

\\ Web content filtering

\\ Rogue device and wireless access point detection

\\ Internal vulnerability scanning

\\ Virtual private networking

\\ Wi-Fi hotspot

WHAT IS THE DIFFERENCE BETWEEN FIREWALLS AND UTM?

The differences between firewalls and UTM can be subtle when looking in from the outside.The table below outlines the key differences.

FIREWALLS	UTM
A firewall is used for blocking entire protocols and types of traffic, but it does not look into the actual content.	UTM provides more protection like anti-spam, anti-virus, intrusion prevention systems, data loss prevention, WAF & advanced threat protection - including the firewall, all bundled on a single appliance.
Not all firewalls are UTM.	All UTM are firewalls.
Firewall functionality acts like a packet filter at layers 3 & 4 (IP address and ports).	UTM looks at layer 4, 5, 6, and 7 only.
Firewalls allow or deny traffic from IP-to-IP addresses on a specific port.	UTM can be configured to act as email security (email scanners), URL filtering (web proxy), wireless security, web application firewall, and VPNs.
Firewalls work on an applied set of rules. It matches all incoming and outgoing data packets with the ones in the database to figure out whether they are harmful or not.	UTM is connected to the leading network and works to provide maximum security against all incoming malwares.

WHAT IS A UNIFIED THREAT MANAGEMENT DEVICE?

A UTM device is a physical device that connects to the network perimeter of your company. It provides you with all the services you need to safeguard your network against the virus, unwanted entry, and other safety hazards.

A unified threat management unit or UTM security device can give small and medium-sized companies a cost-effective, comprehensive, and easily maintained security solution.

UTM equipment offers an alternate way to construct a safe solution from several components, frequently from different suppliers. These solutions are separate from each other and might comprise a hardware firewall, anti-malware scanning, and a network intrusion detection and prevention system to satisfy specific security features a company demands.

One example of a UTM device is a Bastion jump box.

WHAT IS A BASTION JUMP BOX?

Microsoft provides an Azure Bastion service enabling users to connect and access virtual machines (VMs) in a safer manner. The RDP and Secure Shell network protocol are used in conjunction with the Secure Sockets Layer (SSL) encryption.

Bastion links VMs and your local PCs without exposing them to public network connections. It streamlines the process of establishing and managing bastion hosts or jump boxes in your cloud environment as a platform as a service.

The jump boxes work similarly: they are separated from external traffic between a private network or server group. In general, using SSH or RDP, you are connected. They create a single access point to a cluster, although they are subtly different in practice from the original purpose and architecture.

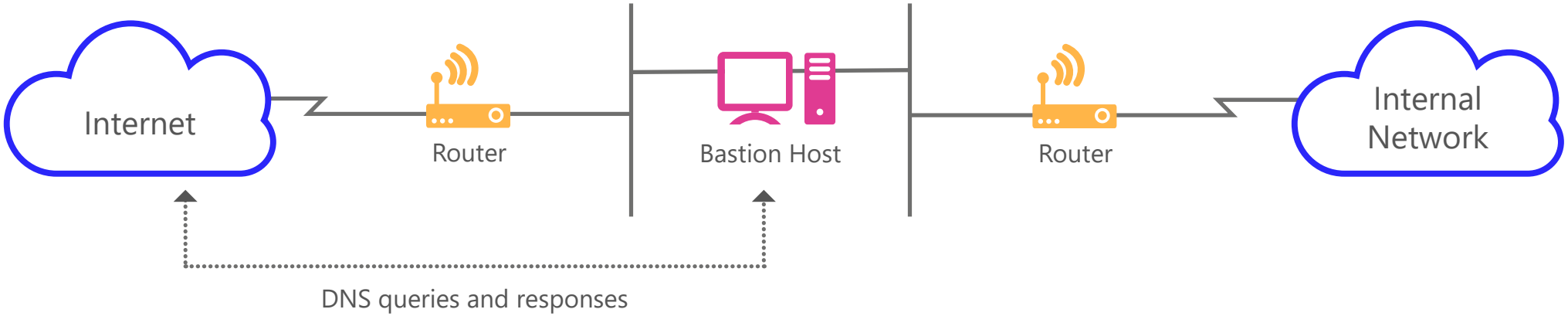
A virtual computer used to run other systems is a jump server. Sometimes, we call these “pivot servers.”

Jump servers generally harden and treat security as a single entrance from your security zone or the entire network into a server group. A jump server is a bridge across two secure networks. There are two different security zones, both of which are regulated.

A bastion host will likewise be treated and connected to a secure zone with specific security considerations, but it lies outside your network security area. The bastion host will allow access from external networks like the public internet to a private network. Sometimes bastion hosts include email servers, web servers, security honeypots, DNS servers, FTP servers, VPNs, firewalls, and security devices.

In both circumstances, the connected server can be considered a single audit point for tracking subnetwork access.

If both jump servers and bastion servers provide a gateway type, their use should be evident in the public cloud. While still retaining remote access to your servers, you may delete the public IPs.



Azure Bastion has been considered to make it easier to provide and manage these connected servers. As PaaS, it just requires a few clicks and fits into your Azure virtual network. According to your policy, you can use network safety group settings to block RDP and SSH traffic via your bastion servers.

Azure competing companies offer similar features like AWS. Instead of handling each bastion or jump box server by getting into the box directly and setting any linked subnets manually, you may use global administration from your cloud portal. The result is increased automation and simple administration throughout your system.

NASSTAR BASTION JUMP BOX EXAMPLE

One Nasstar customer example is for two companies that operate a joint venture.

Users from each company routinely access each other's applications and systems. This was previously done via a 'trusted connection' that had been configured between the two businesses.

The existing policy relied on user authentication and validation checks of each business and allowed authenticated users to traverse the trusted connection.

The risks with this approach were significant. Not only was there a lack of control but if either business suffered a security breach, the trusted connection could serve as a route to cross infect the other business.

Nasstar implemented a Bastion jump box to provide external users access to the services they need without exposing either business to the risk of infection, data exfiltration etc. posed by malicious actors.

WHAT IS THE PURPOSE OF UNIFIED THREAT MANAGEMENT?

For small and medium-sized companies, UTM systems provide unique advantages to improve the security of their programs.

Because many specialised programs have the capabilities of a single device, UTMs minimise the complexity of the security system of an enterprise.

Likewise, a safety control program minimises the level of training provided to workers when they are employed or migrated to a new system. This makes it possible to manage them easily in the future. In the long term, you can save money instead of repeatedly buying new equipment.

For organisations in tightly regulated industries, specific UTM systems give extra benefits.

Appliances that use identity-based security for user activity reports while enabling user-related policy development to fulfill regulatory compliance standards (like HIPPA, CIPA, and GLBA) need control of access and audits by data leakage control.

UTM systems also contribute to the protection of networks against compounded hazards.

These risks include multiple malware and assaults that target individual sections of the network at the same time.

It is often challenging to avoid these combination assaults when employing different devices for each security wall. This is because every security wall must be run separately to keep the evolving security threats up to date. As UTM is a unique defensive point, it simplifies the treatment of coupled threats.

As UTM integrates network firewall capabilities, network intrusion detection and prevention, and gateway anti-virus, some UTM offerings go further, incorporating an anti-spam and URL filtering capability on a hardened operating system as well.

There are reasons for integrating various threat prevention apps into the same device and the same interface, even beyond ease and practicality.

Today, many attacks are mixed attacks that use no single-attack vehicle alone. A blended assault can target several protocols like email (SMTP) and web (HTTP), for example, and maybe done by sending an email that fools the recipient into clicking a web link. The receiver is then sent to an infected site where a virus may be downloaded.

This type of attack might be mitigated either by using the anti-spam (emails) program that recognises the nature of this attack or, in the second stage, by blocking the URL filter in the user attempting to visit the infected website.

Adding URL filters is an essential component of UTM. URL filtering, especially against zero-hour attacks, is typically the first line of protection. Furthermore, spam has evolved into a sophisticated and severe issue, and the spam risk with the UTM's best-of-breed anti-spam capabilities is reduced.

UTM systems also contribute to the protection of networks against compounded hazards.

These risks include multiple malware kinds and assaults that concurrently target individual sections of the network. It might be challenging to avoid these combination assaults when employing different devices for each security wall.

As UTM is a unique defensive point, it simplifies the treatment of coupled threats.

WHAT ARE THE BENEFITS OF UNIFIED THREAT MANAGEMENT?

Organisations using several autonomous security technologies are long gone, costly, difficult to maintain, and confuse the internet security framework.

This problem is addressed with unified threat management. UTM may be characterised as a single device that can execute various security functions consolidating essential security functions.

Companies now consolidate their network safety under a uniform framework by using unified threat management.

THE BENEFITS OF A UNIFIED THREAT MANAGEMENT SYSTEM ARE:

- Flexibility and adaptability
- Ease of deployment
- Centralised integration and management
- Cost-effectiveness
- Increased awareness of network security threats

Companies appreciate UTM for the simplification of the handling of software and solutions by one device. It helps reduce communication among different suppliers, and generally, one IT staff member can maintain a unified threat management device.

A UTM solution is often more affordable as everything in one location is managed instead of being paid by multiple suppliers for various software solutions and maintenance.

WHAT ARE THE DISADVANTAGES OF UNIFIED THREAT MANAGEMENT?

While UTM is a relatively easy way to address typical risks and security concerns recommended by many manufacturers, there are downsides:

\\ Single point of failure

\\ Difficult to scale in very large environments

\\ Limited feature set standalone

With a single solution, all threat management connected with that solution is susceptible if it fails. This might cause issues for companies and leave them uncontrolled if a system breakdown is improbable.

A further potential downside is that, although it can be a cost-effective and cost-effective solution, it can be challenging to scale up as firms expand in size or their safety requirements get increasingly complicated. It is also a matter of whether these solutions can be adapted to accommodate new threat management if new security issues arise.

Also, by their very nature, these all-in-one gadgets contain only what they provide. More safety features or solutions may be purchased by other providers specializing in different areas independently (anti-virus vs. network protection vs. cloud security solutions, for example).

The remedy to these disadvantages often lies with your managed service provider. By integrating systems and devices, everything works more smoothly and effectively.

NASSTAR

nasstar.com
+44 345 003 0000
enquiries@nasstar.com