
Karl Kearney, solutions architect at Integrity 360

web filtering and mail filtering as well," said Conway. "Today we're seeing people add IPS (Intrusion Prevention Systems) and IDS (Intrusion Detection Sensors), adding more modules into the mix to upgrade the product they originally bought."

Conway reported some customers still investing in the original, physical UTM box, but a greater number opting for the virtual equivalent. "In most cases, an enterprise will go with the virtualised UTM, though with some smaller organisations they don't have a lot of virtual servers they can spin up, and plugging in a physical box makes more sense."

"Unfortunately, deciding on which type you need depends on you forecasting your needs and potential exposure," said Kearney. "If you have servers hosted in the cloud, you need cloud firewalls. The argument about on-premise virtual appliances or hardware appliances really depends on a number of variables that need to be identified by your business and usage needs."

Among UTM's many available 'add-on' features, IPS (an Intrusion Prevention System) is perhaps the most essential. Kearney said: "As far as individual UTM/NGFW services go, IPS is one of the most important and valuable. Often exploits like the ones that hit the news this year can be prevented by keeping an IPS system enabled, up-to-date and analysing everything."

In addition to customisation options, virtual UTM can end up being more affordable, providing services like round-the-clock monitoring which might be prohibitively expensive to run in-house. "I'm noticing the trend now is that people don't buy physical infrastructure much anymore," said Madden. "More and more people have moved into the big data centres, which provide control and sustainability. Dependant on what hosting provider you've gone with, they can provide more security services to protect against DDoS and other threats, and the service is available 24/7, so there's always someone there to alert you if the systems have gone down."

Hayden warned against vendors who sell a single appliance at first only to pressure you into investing in further appliances for reporting. Simplicity is the goal here – additional features will increase the complexity, and cost, of securing your business over time. With physical, virtual and cloud-based UTM, there are advantages and disadvantages to each option.

Hayden explained: "Hardware appliances mean that all elements are contained in a box with the vendor's name on the front, so configuration, ongoing management and support are simplified, in that it all belongs to one vendor. Virtual appliances do away with the cost of hardware appliance purchases, but the software must now be installed on a server or PC system. Lately, additional vendors are being introduced, which can add complexity for updating and support purposes. Meanwhile, cloud removes the need for a hardware appliance or internal computing resources, but there can be bandwidth issues if the cloud NGFW isn't just protecting systems already in the cloud . . ."

Hayden stressed that as a customer, remember that you have a choice. Consider the pros and cons of every option, and how you might add to your investment in the future. He said: "It's important to engage with next gen firewall vendors who can offer hardware appliances, virtual appliances or cloud without having to suffer missing features, dependent upon the option that's right for you."

Before making a decision, it's important to honestly and thoroughly assess the risks faced by your business. "In terms of cost, you can't afford to get this wrong," said Carpenter, "so unfortunately, it's better to pay for whatever solution you need. It's all about classification of risk – only this can define the cost you have to pay."

Carpenter advised businesses looking into investing in a new UTM to look for a single reporting interface and a variety of add-ons. "A firewall, no matter how advanced, only looks at north-south traffic, so that's traffic coming in and out of the network, wherweas UTM systems also look at east-west traffic, which is traffic within a network. A UTM is definitely the better option as it provides a range of security solutions, including a firewall, within a single application."

Once all these options are settled on, the final task is keeping your UTM updated. As with all cybersecurity measures, your UTM is only as good as its most recent update.

Conway explained that this is frequently neglected: "Sometimes we'll see people buying a firewall or a web filter or mail filter without live updating, but the thing about UTM is that it has to have live updating, because the threats it protects against will continue to be updated, too." Look for this option when choosing your UTM solution: "Anyone who has a UTM now should be opting for a managed service, with regular updates directly from the manufacturers website. If someone puts in a UTM but they don't update it, they'd be better off saving the electricity by turning it off."

What to look for in a UTM solution

The range of UTM solutions out there can seem like a minefield riddled with potentially costly mistakes. But this complexity can work to your advantage – take the time to research, and you'll be able to find the right blend of services, at the right cost, to suit your business.

"A UTM should empower you to control what comes in and out of your environment, what your users have access to and be monitoring and stopping threats 24/7, 365 days of the year," said Paul Irvine, director of major accounts for UK and Ireland at Fortinet.

"The right solution will also give you clear visibility into what is happening, traffic trends and give you the capability to easily prioritise what threats or issues you need to pay attention to, and where you need to take action. The feature set would include firewall, application control, web filtering, mail filtering, some traffic optimisation, malware/anti-virus, intrusion detection and authentication."

At present, UTM's function is extending beyond a single consolidated platform –instead, it should interact intelligently with the rest of your security measures, including end-point, firewalls and sandboxing. Irvine said: "The principles upon which UTM was founded remain the same in that you need multiple approaches to protect against multi-vector attacks, evolving now into a joined-up solution that combines these other technologies and touch points across the network."

While it's easy to dismiss UTM hardware as old-fashioned, there remain certain industries where their use is practical. Irvine explained that it depends entirely on what kind of protection the customer is looking for: "If we're talking perimeter security, it will typically need to be a hardware solution. Within the network for internal segmentation to contain threats, hardware options are typically needed to deliver the required performance. To protect data and applications in virtual or cloud environments, virtual versions of the security/UTM platforms are typically the right option."

Each has its pros and cons: "Hardware options tend to give you the best price/performance and don't require additional infrastructure to operate, while virtual deployments can be faster to deploy and more flexible. Ultimately, your choice should be driven by the requirement as to what your business needs most."

In synch, or insecure

In the recent history of UTM and next generation firewall technology, synchronised security stands out as one of the most important innovations. Dermot Hayden, of Sophos, explained: "This means that the UTM or firewall is no longer operating on its own at the network edge, but is in constant communication with the endpoint computers across the business, sharing relevant security information in real-time."

As an example, Sophos's XG Firewall employs a 'Security Heartbeat' which reports on the 'health status' of your managed endpoints. In case any of the systems are infected with malware, they will display on the dashboard as yellow or red.

Hayden said: "A key new development – one that is rapidly becoming more a basic requirement than an 'add on' – is synchronised security by deploying end-point security from the same vendor as your firewall so that both are working together as a system rather than independently and unintelligently as they would have in the past.

Cyber criminals are using increasingly complex techniques to expose the silo-based point product approach of the past, resulting in many businesses' defences not being as integrated or coordinated as the attacker's are. This needs to change!"

It's also important to consider event correlation, an increasingly crucial function of UTM systems, especially when using multiple security devices in a single environment. "More and more people are deploying SIEM (Security Information and Event Management) solutions in order to keep on top of security alerts and monitoring," said Karl Kearney, also highlighting the importance of event logging, preferably managed within a single platform: "When looking at fine tuning some of the feature sets (IPS), a high degree of logging is required in order to ensure that false negatives do not prevent legitimate traffic from traversing the firewall. Next generation firewalls allow for a single-management logging platform, as all of the protections are coming from the same device. With some vendors, you can also enhance or upgrade the logging and reporting components."

As threats become more sophisticated – enough to deliberately evade detection by rapidly switching their traffic profile – security measures are under pressure to keep pace. Hayden noted the importance here of synchronised app control: "Static application signatures don't work for custom, obscure, evasive, or any apps using generic HTTP or HTTPS. Synchronised app control automatically identifies all unknown applications, enabling you to easily block the apps you don't want and prioritise the ones you do."