WHITE PAPER: **March 2024**

Threat Prevention with VMware Firewall and IDS

vmware® by Broadcom

Introduction

Segmentation, in all its forms, is likely the best place to begin to put up defences against attackers in the data center. Defenders were forced into this posture as attackers could continue to find ways past the perimeter-based security defences. The evolution of attackers and their TTPs has forced defenders to continue to evolve. This now includes advanced threat prevention technologies like IDS, anti-malware, and NDR to augment the existing segmentation-based controls currently used in the environment.

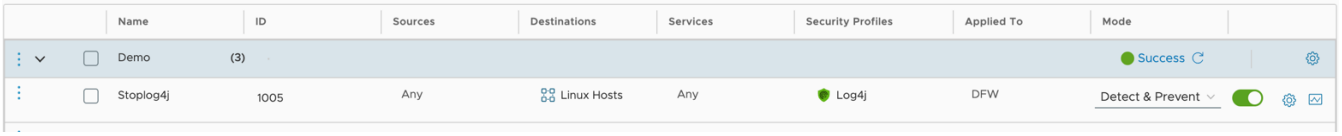
Firewalls play a crucial role in network security by operating at OSI layers 3 and 4, providing a robust defence against unauthorized access and potential threats. However, their effectiveness primarily focuses on controlling traffic based on IP addresses and port numbers, so they may not offer comprehensive protection against more sophisticated attacks targeting the application layer.

To address this limitation, IPS enhances security measures at OSI layer 7, the application layer. Unlike firewalls that primarily filter based on network parameters, an IPS takes a more granular approach by inspecting the actual content and behaviour of the data packets. This allows the IPS to analyze and respond to potential threats more intelligently and context-aware.

VMware has built an innovative firewall that is easily added to any data center network by breaking up and distributing the data plane to the virtual machine level. More recently, the addition of Advanced Threat Prevention at this same level has allowed the customer to continue to evolve their defences. Using technology like IDS in the data center has thus far been challenging to retrofit against legacy network-based threat detection solutions. With the VMware Firewall and Threat Prevention capabilities, the barriers to implementing this technology have been removed, making it far easier to deploy and manage.

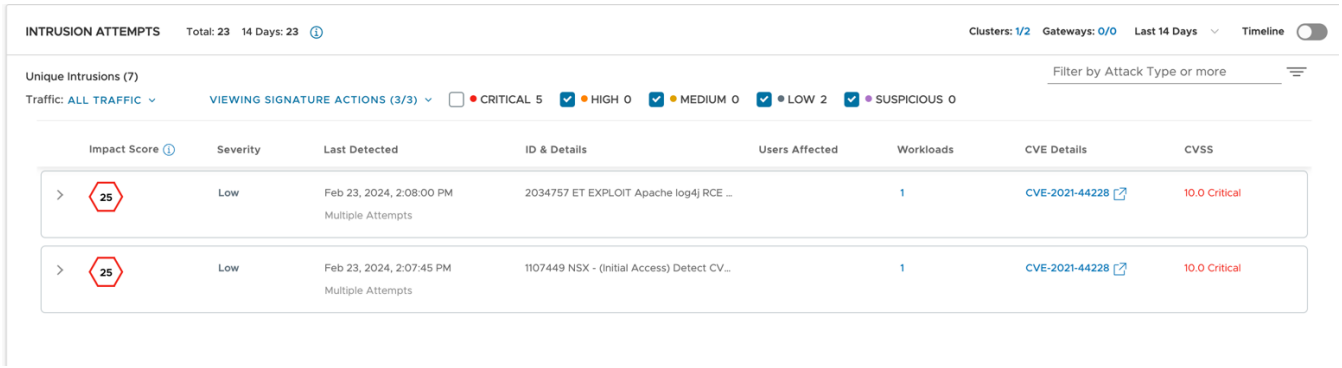
A technology like IDS has several use cases in the data center. These could include a Virtual Patching strategy to help protect assets against known threats and to assist companies in achieving and maintaining compliance. IDS excels at finding and preventing known threats. This can be especially useful in the data center as attackers are less likely to use advanced techniques once their foothold is established. They are far more likely to use our tools for their purposes, like moving and spreading laterally toward their ultimate target. This is commonly referred to as 'living off of the land.' LOTL involves the abuse of native tools and processes on systems, especially living off the land binaries, often referred to as LOLBins, to blend in with normal system activities and operate discreetly with a lower likelihood of being detected or blocked because these tools are already deployed and trusted in the environment.

Once the attackers have their initial access, they will be forced to use the allowed communication channels for this movement. Adding security control to these permitted channels offers the best protection and chance to discover an attacker's movements at this level. Adding these protections took a lot of work before the VMware firewall and ATP additions. Adding these protections is as easy as adding a 5 Tuple-like policy to include the workloads protected by an IDS policy. The policy can be alert only (IDS) or prevention (IPS).



Getting Started with Threat Prevention

It is important to note that adding this capability has some prerequisites. First, an appropriate license is required to enable these features, and this also assumes that VMware Firewall has been installed and configured. Logically speaking, the IDS functionality sits immediately behind the firewall policy. This also means that the firewall policy must permit traffic. The IDS feature works on traditional VLAN-backed network segments as well as overlay networks. Another item to consider is a SIEM to collect event logs for further visibility and analysis. There are no other network changes required to make this functionality work. Start configuring the policy and watching for any alerts that signatures are matching.



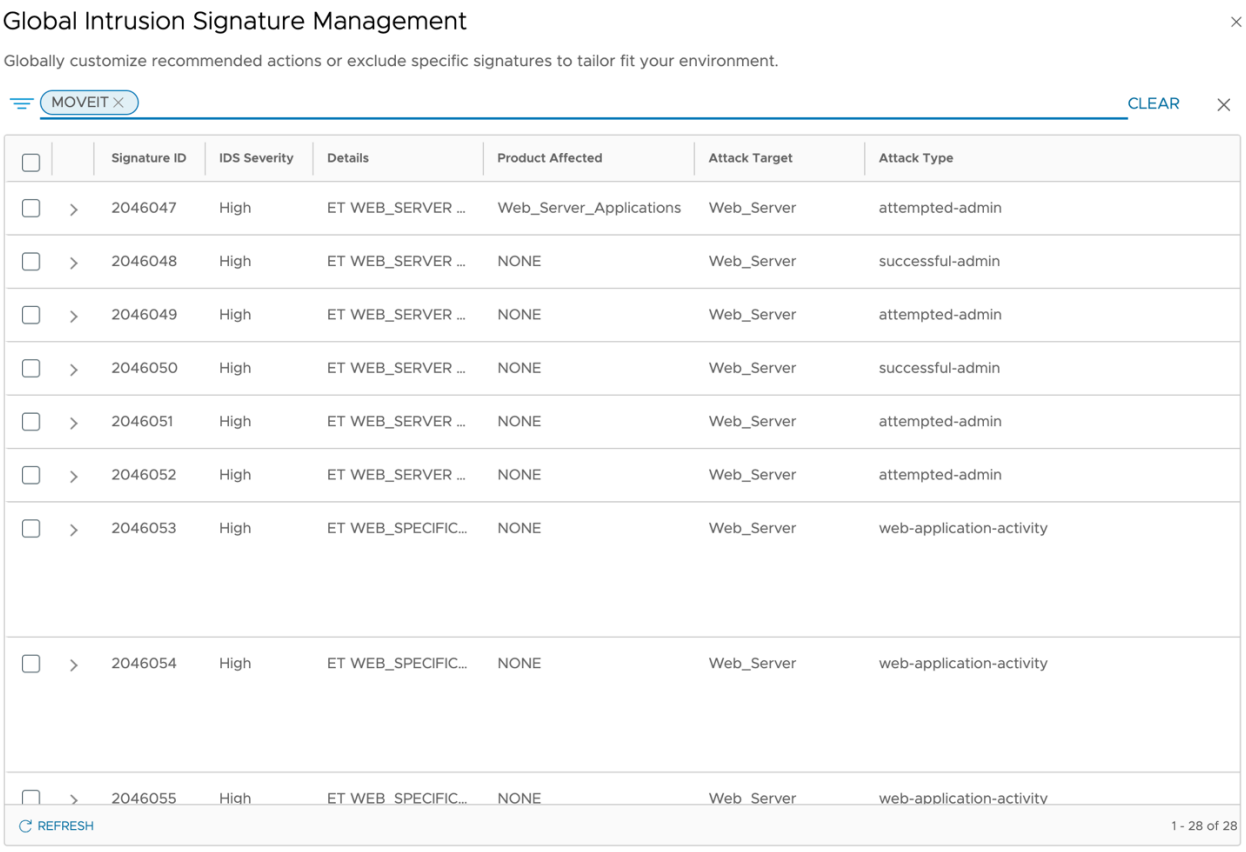
Please refer to the NSX Administration Guide for an overview on setting the Intrusion Detection system.

Once your environment is prepared for IDS/IPS, you start by identifying where to place these protections within the Data Center. Traditionally, you had to make difficult choices on where to place these protections due to the limitation of the network-based technology. The VMware solution does not force you to make this choice as you can easily apply the control at virtually any workload within the datacenter. While this is a completely distributed system, there are constraints to consider when applying these protections. Consider whether the control you are considering can increase security posture overall.

Items to consider might also be:

- Have existing security controls already scanned the traffic?
- Is the traffic encrypted or otherwise obfuscated, rendering signature matching blind to the payload.
- Is the relative value of the asset critical to the overall security of the environment?

The choice of IDS Signatures to use in the profile you will assign to watch over the traffic is also essential. Should you scan for Critical and High vulnerabilities only? Or do you wish to include lower-severity signatures as well? Often, this will come down to ensuring a balance between false positives and false negatives. Security Operations are already awash with too many alerts without tools. Having another data source with additional metadata to enrich the overall campaign may be beneficial. It is best to start these discussions with the SOC sooner rather than later.



Signature ID	IDS Severity	Details	Product Affected	Attack Target	Attack Type
2046047	High	ET WEB_SERVER ...	Web_Server_Applications	Web_Server	attempted-admin
2046048	High	ET WEB_SERVER ...	NONE	Web_Server	successful-admin
2046049	High	ET WEB_SERVER ...	NONE	Web_Server	attempted-admin
2046050	High	ET WEB_SERVER ...	NONE	Web_Server	successful-admin
2046051	High	ET WEB_SERVER ...	NONE	Web_Server	attempted-admin
2046052	High	ET WEB_SERVER ...	NONE	Web_Server	attempted-admin
2046053	High	ET WEB_SPECIFIC...	NONE	Web_Server	web-application-activity
2046054	High	ET WEB_SPECIFIC...	NONE	Web_Server	web-application-activity
2046055	High	ET WEB_SPECIFIC...	NONE	Web_Server	web-application-activity

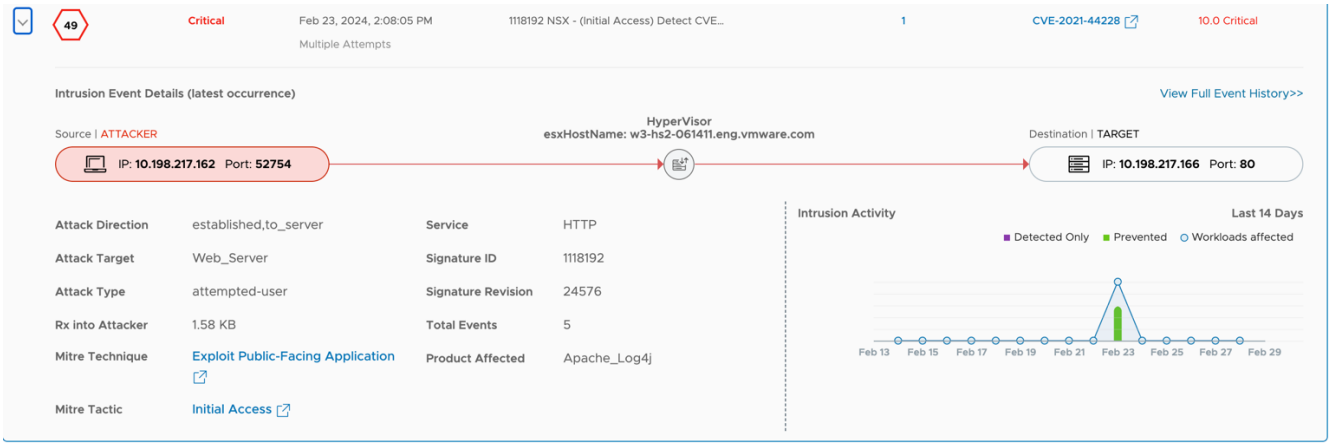
A common approach to adding a security control like IDS into a brownfield will be to start in the Development or Test networks. Using an alert policy (IDS) here will allow practitioners to fine-tune the Policy before moving into production with a detect and prevent policy (IPS).

One key feature of the IPS is its ability to enforce pre-defined rules for network traffic. When incoming or outgoing data matches a specified rule, the IPS can take immediate action, such as blocking malicious traffic, alerting administrators, or initiating predefined responses via a SOAR platform. This proactive approach significantly strengthens the overall security posture, providing a dynamic defense mechanism against emerging threats that may exploit vulnerabilities in applications or services.

To optimize the effectiveness of the IPS solution, it is crucial to maintain the currency and relevance of the configured rules. Regularly updating and fine-tuning the rule set is essential for staying abreast of evolving threats and vulnerabilities in the dynamic landscape of cybersecurity. The significance of keeping rules up to date lies in the proactive nature of cybersecurity defense. As new attack vectors emerge and threat actors employ sophisticated techniques, IPS rules must be continuously refined to detect and mitigate these evolving threats effectively. Timely updates ensure the IPS is equipped with the latest intelligence, enabling it to promptly recognize and thwart emerging risks. The VMware Threat Intelligence team can release a new signature in as little as 20 minutes. Customers can also choose whether to accept these updates in an automated fashion.

Moreover, an up-to-date rule set enhances threat detection accuracy, minimizing false positives and negatives. This, in turn, reduces the likelihood of disrupting legitimate network activities while simultaneously bolstering the system's ability to identify and respond to genuine security incidents. Regular reviews of the IPS rule set should be integrated into the overall cybersecurity strategy. This involves updating the rules based on new threat intelligence and aligning them with the organization's specific security policies and compliance requirements.

To fortify defenses against potential adversaries, minimizing the attack surface by diligently applying software patches and updates is crucial. While this process is straightforward in smaller environments, it becomes increasingly complex in mid to large-sized setups. To tackle this challenge effectively, implementing an automated software solution is imperative. Furthermore, establishing an enterprise-wide vulnerability management program is essential, wherein comprehensive vulnerability scans are conducted weekly across the entire infrastructure. Often, customers will focus their patching efforts on the externally accessible assets in the environment. This can be a costly mistake if an adversary can gain some initial access and pivot toward a higher-value target in the data center. It becomes almost trivial to exploit these unpatched systems as, traditionally, fewer controls are in place at this level to catch this attack. Using Threat Prevention techniques like IDS can offer a compensating control akin to having ‘Patched Virtually.’ The attacker will be thwarted and will raise the alarm to their presence.



Conclusion

Adding on VMware Firewall with ATP is an easy additional security to install and configure in both Brown and Green Field environments. The addition of these controls can offer a measurable increase in the overall security posture that will have direct benefits to an organization's security program.

Do NOT delete section break or footers will be lost. Undo (CTRL+Z) **immediately** if this happens. There is no recovery if Undo is not used.

vmware® by Broadcom

Item No: vmw-bc-wp-temp-uslet-word-2024 1/24