Hillstone NETWORKS

Hillstone CloudHive Secures Private Cloud for a Large Provincial Government

The Customer

A large provincial government who runs a private cloud with over 30 servers and over 300 virtual machines running VMWare ESXi 5.5 and 6.0. The cloud platform primarily provides web hosting and e-government services to its 50 plus subsidiary government departments located in disparate places.

The Challenge

The customer's VM network topology is shown in Figure 1. There is no segmentation or isolation among different tenants; weather forecast bureaus, statistics bureaus, police departments, and investment organizations, etc. all share the same network properties. What is even more riskier is to have web servers, application servers, and database servers all in a non-segmented L2 network. This means that once a virtual machine in a non-classified department is breached, the threat can move to other classified or critical VMs without any checkpoint; and once an attacker gains control of a web server, he or she can easily get into the database servers to exfiltrate data as well as confidential records. In fact, this has

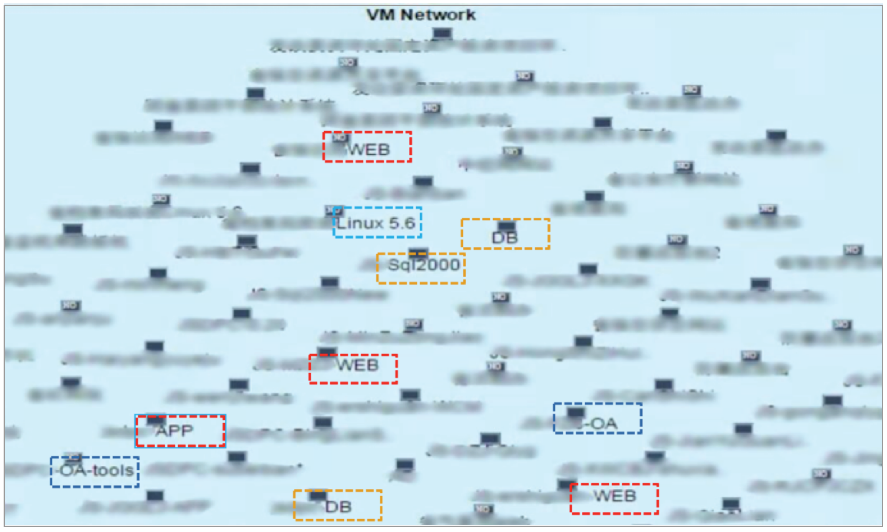


Figure 1: The Customer's VM Network Topology

happened in the past, and this customer is not alone. When a website hosted on their cloud platform was compromised with an SQL injection, they did not have a way to protect application and database servers. The IT department faced serious pressure and the team started to look for an effective solution that was easy to implement.

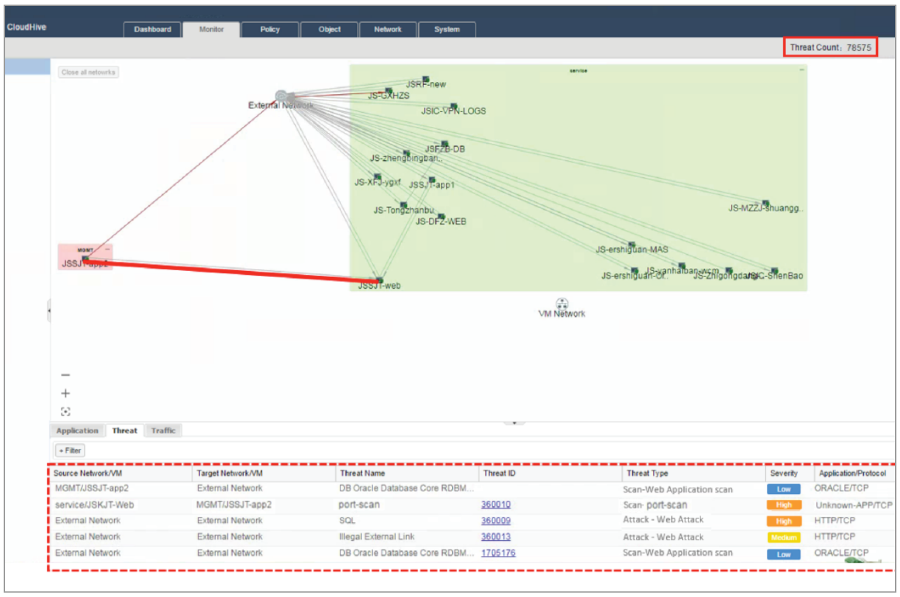
The Solution

Creating VLANs to segment different users and virtual machines through vCenter could be a solution for their situation. However, VLAN configurations are typically very complex. Administrators need to change all the configurations on each firewall, and on switches and routers by logging in individually on each of device, since it cannot be centrally configured through vCenter. Therefore, VLAN is not a viable solution.

When the operation team started to test the Hillstone CloudHive solution, they first found that it can be easily deployed via vCenter without any interruption of their existing network, and without any extra configuration needed on switches or firewalls or even on the VMs themselves. The administrators could easily add or remove CloudHive services on each VM base.

In addition, CloudHive detected over 80,000 threat events in the virtual network, which was entirely undetected previously. By drilling down further into each critical threat alerted, the admin easily found that the connection between a web server and the app2 server was abnormal (highlighted by a red link in Figure 2). In effect, the web server was launching a scanning attach to the app2 server. With CloudHive, the admin was able to take prompt action to resolve the compromised web server.

Moreover, the admin found they could add security to the VM network or VLANs based on business priorities and configure advanced security policies to protect highly classified assets.



Source Network/VM	Target Network/VM	Threat Name	Threat ID	Threat Type	Severity	Application/Protocol
MGMT/JSSJT-app2	External Network	DB Oracle Database Core RDBM...		Scan-Web Application scan	Low	ORACLE/TCP
service/JSKJT-Web	MGMT/JSSJT-app2	port-scan	360010	Scan- port-scan	High	Unknown-APP/TCP
External Network	External Network	SQL	360009	Attack - Web Attack	High	HTTP/TCP
External Network	External Network	Illegal External Link	360013	Attack - Web Attack	Medium	HTTP/TCP
External Network	External Network	DB Oracle Database Core RDBM...	1705176	Scan-Web Application scan	Low	ORACLE/TCP

Figure 2: Layered VM Network Topology after implementing CloudHive

The Conclusion

With the CloudHive micro-segmentation solution, the cloud operation team was able to run the virtual network effectively and securely. By gaining deep visibility of the virtual networks, traffic, applications and threats—down to each virtual machine—CloudHive has enabled the operation team to take prompt security action to stop breaches inside their cloud deployment, and thereby ensure the integrity of their assets.