VM-Series and Tencent Cloud

Enforce Consistent Security Posture on Tencent Cloud Using Palo Alto Networks VM-Series

Benefits

- Protect applications running on Tencent Cloud with advanced threat prevention capabilities and stop data exfiltration.
- Prevent lateral movement of threats with microsegmentation and advanced threat protection capabilities.
- Identify and control applications, grant access based on users, and prevent known and unknown threats.
- Centrally manage policies using Panorama to ensure consistent security posture for applications running on Tencent Cloud and on-premises.

The Challenge

Network security teams need better visibility into traffic from cloud service providers. Native cloud security requires more capability to protect against unknown threats and data exfiltration. Managing separate security policies for different platforms is also cumbersome.

The Solution

Applications that run in the cloud need best-in-class advanced threat prevention against unknown threats and protection against data exfiltration.

Tencent Cloud

Tencent Cloud's infrastructure is built on a globally distributed network of data centers, providing high availability, low latency, and robust performance for business worldwide. Tencent Cloud is available in 21 regions and over 58 availability zones across the globe, ensuring seamless connectivity and reliable service. With strong capabilities in networking, compute power, storage, and security, Tencent Cloud's infrastructure is designed to support a wide range of applications.

Palo Alto Networks VM-Series

The Palo Alto Networks VM-Series Virtual Next-Generation Firewall consistently protects public and private clouds, virtualized data centers, and branch environments by delivering inline network security and threat prevention. Public cloud platforms and software-defined network solutions lack the threat prevention capabilities needed to keep your environment safe. VM-Series virtual firewalls augment your security posture with the industry-leading threat prevention capabilities of the Palo Alto Networks Next-Generation Firewall in a VM form factor, making it automatable, scalable, and easily deployed.

Palo Alto Networks and Tencent Cloud

With VM-Series support on Tencent Cloud, customers can protect applications running on Tencent Cloud against incoming threats and data exfiltration and also prevent the lateral movement of threats within the Tencent Cloud environment. Additionally, you can manage firewalls running on all the platforms from a single place, thus allowing you to enforce consistent security policies regardless of whether your applications are running on Tencent Cloud or on premises.

Use Case 1: Inbound Threat and Data Exfiltration Protection

Challenge

Applications deployed on Tencent Cloud remain protected but can be vulnerable to network-based attacks and data exfiltration via command-and-control (C2) attacks, if appropriate protective measures are not implemented.

Solution

VM-Series identifies and stops inbound attacks originating from the public-facing internet, protecting applications against external threats. VM-Series also mitigates data exfiltration attempts by blocking connections to known bad destinations like C2 servers and inspecting the traffic for data patterns associated with sensitive data, such as credit card and Social Security numbers.

Use Case 2: Prevent Lateral Movement of Threats

Challenge

Security groups effectively minimize the attack surface, though threats could still migrate between applications that are allowed to communicate, resulting in lateral movement of threats.

Solution

VM-Series safeguards your Tencent public cloud deployment against lateral movement of cyberthreats by using Advanced Threat Prevention and DNS Security services between network segments. VM-Series can effectively block threats from moving laterally between applications and workloads, helping to ensure enhanced security in Tencent Cloud environments.

Use Case 3: Centralized Management and Consistent Security Posture Across Public and Private Clouds

Challenge

Every cloud has different security capabilities, and on-premises devices are managed separately from cloud security, resulting in multiple management tools and inconsistent network security.

Solution

Both VM-Series and physical Palo Alto Networks firewalls are managed from the centralized management plane called Panorama®, which allows you to maintain and enforce consistent security policies regardless of whether your applications are running on Tencent Cloud or on the private cloud. This enables you to maintain a consistent security posture while managing all your firewalls from a single place.

About Tencent Cloud

Tencent Cloud, one of the world's leading cloud companies, is committed to creating innovative solutions to resolve real-world issues and enabling digital transformation for smart industries. For more information, visit www.tencentcloud.com.

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. Our next-gen security solutions, expert services, and industry-leading threat intelligence empower organizations across every sector to transform with confidence. For more information, visit www.paloaltonetworks.com.

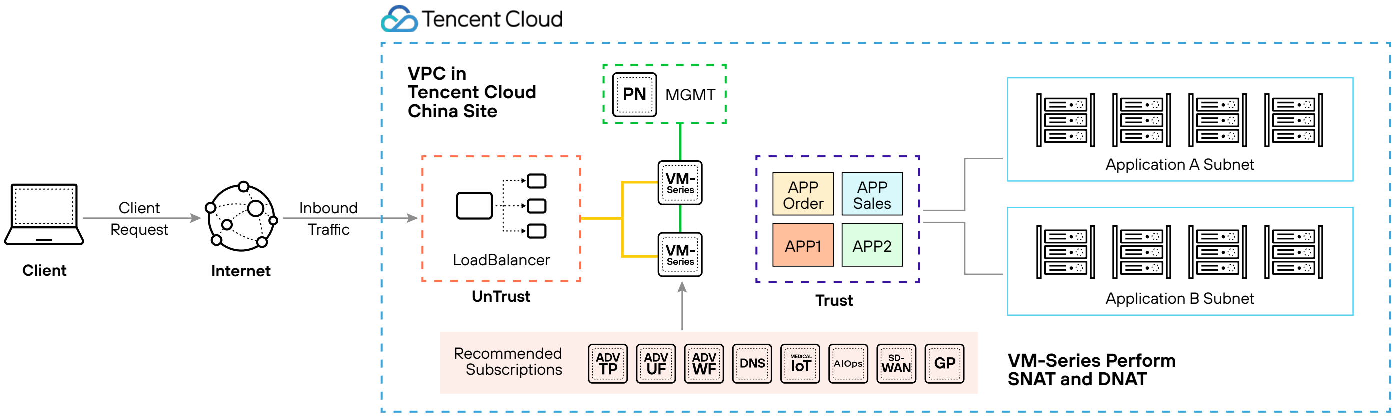

Figure 1: Tencent Cloud integration

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com