



Omantel secures international gateway and server farms with TippingPoint Intrusion Prevention Systems



CASE STUDY

User:
Omantel

Country:
Sultanate of Oman

Industry:
Telecommunications

UAE
102, Building No. 5
Dubai Internet City
P. O. Box 500285
Dubai, UAE
Tel: +971 4 4294900
info@fvc.com

Saudi Arabia
18, Al Khozama Center
P. O. Box 11583
Riyadh, Saudi Arabia
Tel: +966 1 2175530
info@fvc.com

Lebanon
4th Floor, Block C
Mkalles 2001 Center
Mkalles, Lebanon
Tel: +961 4 699033
info@fvc.com

Egypt
6 A, Sebaq St.
Heliopolis
Cairo, Egypt
Tel: +20 2 26435280
info@fvc.com

Morocco
Technopark
Bureau 357 - 358,
3eme Etage
Route de Nouaceur
Angle RS 114 CT 1029
Casablanca, Morocco
Tel: +212 22 958450
info@fvc.com

BACKGROUND

Oman Telecommunications Company (Omantel), established in 1987, is the largest telecommunications company in the Sultanate of Oman. It is engaged in establishing, operating, maintaining and developing fixed and mobile telecommunication services for residential, corporate and government customers in the Sultanate. Omantel is 70% government owned. In April 2008, it acquired a 65% share in WorldCall Pakistan.

The company's vision is to be a highly innovative telecommunications company providing high quality telecommunications services at reasonable prices in order to satisfy the needs of its valued customers.

CHALLENGES

Omantel's main challenge was to protect its server farms from latest threats such as attacks on un-patched systems and zero-day attacks on patched systems. The company also wanted to create a time-window for adhering with the patch management policy. Omantel follows a strict patch and change management policy with all patches tested before deploying on production systems and this required sufficient time. With a shrinking timeline between each patch and exploit release, there was a risk to these production servers remaining "unpatched" while the security team followed the patch management steps.

Omantel had been using Intrusion Detection System (IDS) sensors from two different security vendors to manage the threats to the system. Salim Al-Mazroui, General Manager - IT from Omantel said, "Our initial plan was to upgrade our existing IDS sensors to Intrusion Prevention System (IPS) sensors. Our evaluation team realized that upgrading the current products would not meet their requirements for several reasons including the fact that IDS was a sniffer-based reactive technology with too many false-positives. It was also cumbersome to manage and consumed operational time."

The security team at Omantel decided that it needed an in-band, real-time traffic classification and policy enforcement system that both detects and blocks unwanted traffic. Omantel decided to conduct a Proof of Concept (PoC) with the top 4 vendors within Gartner Leader's Magic Quadrant including TippingPoint.

SOLUTION

After a thorough evaluation by the team, TippingPoint was selected to partner with Omantel. TippingPoint IPS sensors were initially plugged into a lab setup and later to different parts of the production network. The evaluation and final selection were based on the following key criteria:

TippingPoint



Omantel secures international gateway and server farms with TippingPoint Intrusion Prevention Systems



CASE STUDY

User:
Omantel

Country:
Sultanate of Oman

Industry:
Telecommunications

UAE
102, Building No. 5
Dubai Internet City
P. O. Box 500285
Dubai, UAE
Tel: +971 4 4294900
info@fvc.com

Saudi Arabia
18, Al Khozama Center
P. O. Box 11583
Riyadh, Saudi Arabia
Tel: +966 1 2175530
info@fvc.com

Lebanon
4th Floor, Block C
Mkalles 2001 Center
Mkalles, Lebanon
Tel: +961 4 699033
info@fvc.com

Egypt
6 A, Sebaq St.
Heliopolis
Cairo, Egypt
Tel: +20 2 26435280
info@fvc.com

Morocco
Technopark
Bureau 357 - 358,
3eme Etage
Route de Nouaceur
Angle RS 114 CT 1029
Casablanca, Morocco
Tel: +212 22 958450
info@fvc.com

1. **Performance** - Despite knowing that in-line devices add network latency, Omantel wanted the selected IPS to provide one-way latency of less than 150 microseconds at 10 Gigabit speed.
2. **Availability** - The selected IPS needed to provide 99.999% network availability, whatever the circumstance whether it was a failure in the IPS from power supply, chip, software or any hardware perspectives.
3. **Scalability** - The IPS solution needed to be scalable to deep inspect up to 20 Gbps of full duplex traffic in a single 10 GbE link.
4. **Security Effectiveness** - The IPS should be able to provide proactive zero day vulnerabilities as well as vulnerability coverage especially for Microsoft software.
5. **Ease of Management** - Administration/manual intervention should be minimal and the technology should be capable of proactively blocking attacks with zero false positives.
6. **Training** - Omantel needed the support of the vendors local partners to build its knowledge-skill internally.

Al-Mazroui added, "TippingPoint outperformed all the vendors in the evaluation. They were able to meet all our performance and scalability parameters especially with their pay-as-you-grow model where we can scale from a 2 Gbps solution to a 20Gbps solution over a period of time. We conducted reference checks on other customers of TippingPoint and they showed strong support across the board, including in-band deployments, effectiveness of security filters, ease of IPS configuration, and repeat IPS purchase intentions."

TippingPoint IPS sensors are now deployed at Omantel's international gateway and server farms. TippingPoint's Core Controllers are deployed at its 10 GbE international gateway for a 10 Gbps deep inspection initially, with the ability to scale up to 20 Gbps of inspection later.

RESULT

"The live deployment showed the same results as the PoC," added Al Mazroui. "Our international internet pipe delivered far less noise traffic than before and we are now able to provide our customers with a cleaner Internet connection. Thanks to TippingPoint's Recommended Settings, we are protected from critical attacks with minimum manual intervention. TippingPoint is able to deliver on their commitments. They have experts locally available to carry out the deployment and future support."

According to Omantel, the deployment of IPS sensors before the server farm has helped its System and Security teams to go through its step-by-step patch management processes without rushing into any emergency patching measures.