



Improving Profitability for MSSPs Targeting SMBs

Using a Multi-tenant Virtual Domain (VDM) Model to Deliver Cost-Effective Security Services

Introduction

In recent years the adoption of cloud services, including security services, has risen significantly. Gartner predicts that spending on public cloud products will reach over \$207 billion by 2016¹ and Frost & Sullivan in its 2012 report on the Global Managed Security Services reported a market size of nearly \$7 Billion with a growth rate of over 18% for the forecast period². Enterprise customers have driven much of the recent growth, but as the market is maturing, the SMB (Small and Medium Business) sector is now beginning to adopt in larger numbers. Research firm AMI anticipates that SMB spending on security services will rise over 10% per year through 2016³. The challenge with the SMB adoption rate is that the typical small and medium business expects lower price points, and in turn is pushing for less expensive services with many of the features that Enterprise-sized customers would expect. Standard deployments, including virtualized solutions, can still be expensive and deter the SMB from buying cloud security services. This same expectation can also make it difficult for providers to deliver services at a profitable price point.

Fortinet helps solve these challenges by leveraging Service Provider platforms and a Multi-Tenant VDOM (Virtual Domain) configuration to meet both the SMB and Enterprise service levels and price points. VDOMs enable a single FortiGate unit to split its resources and function as multiple independent units with customized policies and controls. Traditionally, Enterprise customers require highly customizable solutions utilizing a dedicated VDOM per customer to support those requirements. Enterprises are also willing to pay the market price for these services.

By contrast, the SMB sector generally cannot afford to pay what an Enterprise can yet requires similar services.

In order to address these challenges many providers have discovered that while SMB customers need the same kinds of services, they often require less customization than enterprise customers.

This white paper discusses a configuration option that allows the service provider to address enterprise and SMB managed services requirements, at a reasonable margin, on a single Fortinet chassis. This can be done by using a combination of dedicated and multi-tenant VDOMs to provide both service requirements. Dedicated VDOMs for enterprise customers needing a high level of customization and multi-tenant VDOMs for SMB customers delivered in pre-packaged control bundles. While this approach will not address every SMB environment, it does give providers another model to choose from that can lower costs of deployment and therefore lower service pricing while keeping margins intact.

The Growing Need for SMB Focused Managed Security Services

Managed security services have matured significantly over the past decade. Traditional managed security services have largely been limited to managed firewall and VPN. Over the last 5 years, the demand for other security services has increased significantly. Today, managed security services include a wide range of services including firewall, Layer 7 Application Control, IDS/IPS, content filtering, anti-virus, and many others. The interest and growth in these services has been strongly correlated with the sharp escalation in regulatory requirements felt across industry verticals and dramatic increase in security breach notifications in the media.

¹ <http://www.crn.com/news/cloud/240003408/gartner-spending-on-public-cloud-services-growing-rapidly.htm?pgno=1>

² 2012 North American Managed Security Service Providers Market, Frost & Sullivan

³ 2012 Global SMB Security Market Assessment, Access Markets International

Table 1: Breaches by Organization Size

| Organizations Size (Employees) | Number of Breaches | Percentage of Total |
|--------------------------------|--------------------|---------------------|
| 1 to 10 | 42 | 4.9% |
| 11 to 100 | 570 | 66.7% |
| 101 to 1,000 | 48 | 5.6% |
| 1,001 to 10,000 | 27 | 3.2% |
| 10,001 to 100,000 | 23 | 2.7% |
| Over 100,000 | 10 | 1.2% |
| Unknown | 135 | 15.8% |
| Total | 855 | 100.0% |

Many MSSPs have focused on the enterprise as the primary customer for security services. Given that enterprises had the most complex environments and the financial resources to afford MSSPs, this focus made sense. In recent years, MSSPs have begun targeting mid-sized enterprises, but many have avoided the SMB market entirely. However, the SMB segment has been facing increasing security challenges and in many cases have the same challenges as large and medium enterprises.

The most recent Verizon Data Breach Investigation report illustrates the need for security for the smallest organizations. As Table 1 illustrates, out of 855 reported breaches – 612, or just over 71%, occurred to companies that had between 1 and 100 employees. These companies do not have the infrastructure in place to prevent attacks and yet are being targeted more frequently. There is plenty of opportunity for providers to offer security to the SMB segment.

The Traditional Approach to Using Fortinet equipment in Managed Security Service Provider Environments

As the complexity of the service increases, the amount of administration time increases, thus increasing the overall cost of goods sold.

It is common for Service Providers to size hosted service bundles using an amount of bandwidth enforced with tiered service levels. The example below is just one illustration of how a service provider might define their services. There are many variations depending on the number of services that the provider chooses to offer.

In a traditional approach, a provider would assign one Fortinet Virtual Domain (VDM) to every customer, giving the customer its own environment that could be controlled and managed by both the provider and the customer. The full breadth of UTM services could be allocated based on each customer's environment. While this is an ideal scenario for enterprise customers who have the need for shared administration and dedicated ports, the price of this solution is fixed to a large extent by preventing economies of scale from being achieved. There is another model that still provides dedicated security, but allows providers to share the cost of VDMs amongst multiple customers. This allows for service providers to lower their prices while offering similar services and service levels to their customers.

Cloud MSS Example:
Bronze, Silver, Gold Security levels.

1 Meg, 10Meg, 20Meg, 50Meg, 100Meg or 200Meg Firewall Ports with common service options:

Bronze: Basic security with fewer controls in place. It may include basic firewall services with limited policy change requests per month, services like stateful packet inspection, NAT, port address translation and an uptime SLA included.

Silver: This level would include all the services of the Bronze level, but adds more security controls, often bundled for simplicity. Web filtering, application control and IPS are high value controls that tackle several SMB pain points driving a higher price point. This level may also include basic reporting.

Gold: This premium service would be the most expensive of the three choices but also offer the most functionality. With all of the controls in Silver, it may include read access or co-administration of web filtering and enhanced reporting. This level may require a separate VDM depending on the Service Provider's customer service portal preparedness.

Advantages of Using a Single VDOM for Multiple Customers

Small and Medium businesses are often amenable to a more standardized security offering and may have less stringent co-administration and compliance requirements than enterprise customers. As mentioned earlier, one of the key challenges for providers seeking to address the SMB market has been providing security services at a price point that is palatable to the SMB. Table 2 shows average industry pricing for some of the most common managed security services as determined by Frost & Sullivan.⁴ These annual prices are far too high for most SMBs.

Fortinet gives providers another option. Provisioning multiple customers into a single VDOM. Because every Fortinet appliance has the ability to perform advanced routing functions, Fortinet enables service providers the ability to route and segment customer traffic using Virtual LANs (VLANs) and Virtual Routing & Forwarding (VRF). By segmenting customer traffic via VLANs using existing VDOM technology, providers can leverage Fortinet equipment to provide secure segmentation of customers into standardized support bundles, taking advantage of economies of scale to lower costs.

Multi-tenant VDOM Considerations

While the multi-tenant VDOM model opens up the possibility of moving more customers onto a single appliance with lower licensing costs, there are still considerations that the provider has to keep in mind. The following considerations have to be evaluated by the provider based on individual customers and the size of their managed service operation.

Implementation Sizing

Fortinet estimates user count, per multi-tenant VDOM, to be around 500, where the customer's throughput is 1 to 2 Mbps with an average of 10 users per customer. On chassis-based systems like the 5140, this deployment could

use a separate blade within the chassis, supporting 5,000 users running about 50K concurrent sessions (assumes an average of 10 sessions per user and 100% utilization). Smaller systems can be specified based on growth expectations and service complexity relative to hardware resource consumption.

These numbers are greatly simplified and should only serve as a guideline that will vary depending on the service options deployed. A single blade dedicated to a multi-tenant VDOM with other individual VDOM customers running on separate 5001C blades is optimal to insure shared VDOM customers don't impact performance on the same blade. Fortinet recommends that the provider purchase dedicated blades for this low end service in order to make provisioning easier, as well as manage capacity.

Session Tables

While traffic is securely separated by VLANs, Multi-Tenant VDOMs share firewall session tables, this can be an inhibitor for maintaining compliance in highly sensitive security environments. Many SMB customers are not going to be concerned with sharing session tables if their traffic is securely separated via VLAN. VLANs are used extensively in the LAN and by the service provider for traffic segmentation and security.

Customer Self-Service

In order for customers to be able to co-administer the firewall in a shared VDOM, the service provider would have to integrate a customer service portal using the Fortinet Software Development Kit (SDK) with FortiManager. This is due to FortiManager's self service administration being allocated per VDOM. Alternatively, no co-administration would be allowed and service provider must handle all change requests. Customers wanting this level of service will often be willing to pay for an upgrade to an individual VDOM.

Table 2: Industry Pricing for Managed Services

| Service | Managed/Monitored Customer Premise Equipment (CPE) | Cloud Based |
|--------------------|---|----------------------------------|
| Firewall/IPSEC VPN | \$300 - \$1,500 per month; price decreases depending on volume | \$400 - \$600 per month per site |
| IDS/IPS | \$3500- \$1,200 per month; price increases depending on bandwidth | \$300-\$400 per month per site |
| Content Filtering | \$900 - \$1500 per month per device | \$400 - \$600 per month per site |
| SIEM | \$1,300 - \$14,000 per month | \$1,000 - \$12,500 per month |

⁴ Global Analysis of the Managed Security Service Providers Market, Frost & Sullivan, 2012

Rule Implementation

Operationally the MSSP will need procedures to ensure rules are grouped together, or identified with a naming convention specific to each customer to assist in the change request and troubleshooting process.

Overlapping Addresses

Assuming most use private address space, everyone must have unique addresses or use public IPs within a shared VDOM. This will also drive the limited number of customers on a VDOM. When a customer has overlapping space and no public IPs, they would need to be in a separate VDOM or card. This is also a limitation for IPsec VPNs due to overlapping private addresses.

Documentation of IP addresses

For reasons discussed regarding overlapping addresses, IP address specification and documentation is something that will need to be very closely tracked and reviewed before new customers are provisioned to ensure duplicate IPs are not configured into a single VDOM.

Resource Allocation

Per VDOM resource allocation can be modified to limit or guarantee a certain amount of sessions. This will keep this VDOM from consuming resources used by higher paying customers. Using VLANs to separate customers will be required each customer to have a unique VLAN ID for logical traffic separation.

Table 3: Cost Comparison between Single and Multiple VDOM Configurations

| Number of Customers | Single Tenant VDOM Solution | Single Tenant Solution Pricing | Multi-Tenant Solution | Multi-Tenant Solution Pricing | Cost Savings (Multiple VDOM vs Single) |
|---------------------|---|--------------------------------|--|-------------------------------|--|
| 25 | 2-1000C FortiGates FortiManager FortiAnalyzer Support for 25 VDOMs | \$116,284 | 2-1000C FortiGates (10 VDOMs already included) FortiManager FortiAnalyzer | \$81,984 | \$34,300 |
| 50 | 2-1000C FortiGates FortiManager FortiAnalyzer Support for 50 VDOMs | \$145,034 | 2-1000C FortiGates FortiManager FortiAnalyzer Support for 25 VDOMs | \$114,534 | \$30,500 |
| 100 | 2-1000C FortiGates FortiManager FortiAnalyzer Support for 100 VDOMs | \$187,080 | 2-1000C FortiGates FortiManager FortiAnalyzer Support for 50 VDOMs | \$145,284 | \$41,796 |
| 250 | 2-3950B FortiGates FortiManager FortiAnalyzer Support for 250 VDOMs | \$402,275 | 2-1000C FortiGates FortiManager FortiAnalyzer Support for 100 VDOMs | \$183,784 | \$218,491 |
| 500 | 2-3950B FortiGates FortiManager FortiAnalyzer Support for 500 VDOMs | \$575,214 | 2-1000C FortiGates FortiManager FortiAnalyzer Support for 250 VDOMs | \$231,784 | \$343,430 |
| 1000 | 4-3950B FortiGates FortiAnalyzer FortiManager Support for 1000 VDOMs | \$943,545 | 2-3950B FortiGates FortiManager FortiAnalyzer Support for 500 VDOMs | \$497,855 | \$445,690 |

FortiManager Considerations

Strict naming conventions for security objects will have to be enforced so management of multiple customers can be tracked and troubleshooting simplified. FortiManager provides a tagging feature that can be used to uniquely tag each customer's policies. The Fortinet SDK allows providers to develop customizable customer facing web portals, allowing a customer's IT staff to make changes to a number of configurations such as whitelists and web filtering rules.

FortiAnalyzer Considerations

Analyzer or SIEM reporting – running reports by VDOM will not allow separate customer reporting, will need to run reports by VLAN ID, or IP address. This will require extra work from the provider to configure.

A Comparison of Single and Multi-tenant VDOM Pricing

The determining factors in choosing the proper Fortinet equipment to provide security services is the overall price and margins that an MSSP can generate from their business. This section will illustrate the significant cost savings that can be achieved through the use of a multi-tenant model. These cost savings can then be used by the provider to meet SMB customer price points while maintaining profitability. A mix of dedicated and multi-tenant VDOMs can provide a solid ROI for service providers and allow them to meet the needs of SMB and enterprise customers on a single appliance.

Table 3 illustrates the price differences between supporting 25, 50, 100, 500, and 1000 customers. This example assumes the same bandwidth requirements, management and reporting services per customer as well as a high availability configuration.⁵

As shown in Table 3, the cost savings for using a multi-tenant solution can be significant, especially during the ramp phase of service creation and as the number of supported customers goes up. Even more important than cost savings is increased revenue. This is one area with the ability to use a multiple VDOM model makes a significant difference. Table 4 illustrates a cost and margin analysis of single versus multiple VDOM models. It should be obvious from the analysis below that a multiple VDOM model opens up the ability for an MSSP to host many more customers, providing increased revenue and significant improvements to the overall margins generated by the business.

Conclusion

The SMB segment is proving to be an easy target for attackers due to the smaller budgets and fewer resources these businesses can deploy to stop cyber threats. Unfortunately, margin-focused Cloud MSSPs have avoided this market due to the high price sensitivity of SMB companies. Cost considerations have always been a limitation for SMB companies weighing their IT security options, regulatory requirements now affect many of these small companies, requiring them to look for partners to provide broad security at lower price points.

This configuration option allows the service provider to address enterprise and SMB managed services requirements, at a reasonable margin, on a single Fortinet chassis. Dedicated VDOMs can be used to address enterprise customer's needs for customization and higher security. Multi-tenant VDOMs can be used for SMB customers and through simplified pre-packaged control bundles; cost of goods sold can be reduced.

Fortinet allows MSSPs to deliver cutting edge security technologies to SMBs, while preserving their margin

Table 4: Margin Comparison between Single and Multiple VDOM Solutions

| Total Users | Solution Cost per Year for 3 Years (Single VDOM) | Solution Cost per Year for 3 Years (Multi-VDOM) | Margin per Year for 3 Years (Single VDOM) | Margin per Year for 3 Years (Multi VDOM) | Margin difference per Year |
|-------------|--|---|---|--|----------------------------|
| 25 | \$38,761 | \$27,328 | \$28,739 | \$40,172 | \$11,433 |
| 50 | \$48,345 | \$38,178 | \$86,655 | \$96,822 | \$10,167 |
| 100 | \$62,360 | \$48,428 | \$207,640 | \$221,572 | \$13,932 |
| 500 | \$134,092 | \$61,261 | \$1,215,908 | \$1,288,739 | \$72,830 |
| 750 | \$191,738 | \$77,261 | \$1,833,262 | \$1,947,739 | \$114,477 |
| 1000 | \$314,515 | \$165,952 | \$2,385,485 | \$2,534,048 | \$148,563 |

⁵ For this example, we are using list pricing for all equipment. HA configurations require complete duplication of the hardware and VDOM licenses. In order to maintain realism, the multi-tenant solution still assumes that 30% of customers will require their own VDOM, making these values conservative to some real world scenarios.

requirements and addressing broader markets. Through innovative approaches in providing security services such as using multi-tenant VDOMs, Fortinet gives providers the flexibility to grow their businesses into green field opportunities that are unreachable using any other equipment provider.

About Fortinet

Fortinet delivers unified threat management and specialized security solutions that block today's sophisticated threats. Our consolidated architecture enables our customers to deploy fully integrated security technologies in a single device, delivering increased performance, improved protection, and reduced costs. Purpose-built hardware and software provide the high performance and complete content protection our customers need to stay abreast of a constantly evolving threat landscape. Our customers rely on Fortinet to protect their constantly evolving networks in every industry and region in the world. They deploy a robust defense-in-depth strategy that improves their security posture, simplifies their security infrastructure, and reduces their overall cost of ownership. ■



GLOBAL HEADQUARTERS

Fortinet Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE

120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE

300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE

Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480