



TREND MICRO INTERSCAN

Enhancing Trend Micro InterScan Deployments with F5 Solutions

Executive Summary

Every month, hundreds of new viruses are developed and distributed throughout the Internet. One virus can infect and cripple an enterprise network, and ultimately cost the organization hundreds of thousands of dollars. With the increasing number of threats to the network, enterprise organizations need an anti-virus solution in place that can effectively protect the infrastructure, and easily scale as threats and the network grow. By integrating products from F5 Networks and Trend Micro®, enterprises have a solution that provides unmatched security, scalability, performance, and availability.

When F5 Networks' BIG-IP® product, a uniquely featured, high availability and security solution, is combined with Trend Micro InterScan® anti-virus products, enterprises benefit from a scalable, secure solution that provides high performance, comprehensive protection against viruses, and easy to use management tools to help monitor and control the type of information that enters or leaves via the gateway.

Challenges

Providing high availability, increased uptime, performance, scalability, and enhanced security for anti-virus deployments is critical for enterprise organizations. Anti-virus systems are typically deployed at key access points in network architectures that demand high availability and constant traffic flow. Traditional anti-virus systems may be monolithic, where one server supports multiple virus-scanning services like email and HTTP (Web traffic). This traditionally requires more expensive server hardware, does not allow for flexible scale, and can introduce latency when managing the load of complex filtering.

Adding security devices to a network without factoring best practice architectures can cause considerable downtime and network disruption. As network security policies become more complex, requiring more and more resources, demand for efficient traffic management becomes critical. Enterprises need a traffic management solution that allows seamless scalability across multiple virus scanning services, without adding administrative overhead.

Anti-virus systems are high-traffic network security devices that must constantly perform at their peak. If a device is overwhelmed or underpowered, the protection it provides an organization is greatly reduced. Organizations are challenged with finding a traffic management solution that not only extends the scope and interoperates with anti-virus systems, but also provide an extra layer of security itself.

Another challenge for anti-virus deployments is to create application awareness. Most network security components work independently of one another. These disparate devices lack the ability to communicate with one another, learn from, and react to identified threats, making it difficult to build a strong, more unified solution.

Solution

Organizations that deploy the BIG-IP traffic management product with Trend Micro's anti-virus solutions benefit through enhanced performance, security, uptime, and scalability for InterScan deployments. The result is a more cost effective anti-virus service implementation, easier administration, and anti-virus solutions that can be scaled across varying server platforms.

The BIG-IP product combines the expertise of Trend Micro's anti-virus systems, and can respond to, act upon, and prevent changing application level security threats. Using iRules and VLAN Mirroring or clone pools, the BIG-IP directs traffic to the appropriate device without disrupting the flow of traffic for the anti-virus system.

The BIG-IP product can greatly simplify management and scalability of a cluster of InterScan products. With the BIG-IP solution, you can easily create a specific InterScan pool dedicated to the specific InterScan service, which can contain multiple InterScan devices. For example, you can dedicate one pool to HTTP scanning and another to email scanning. Because email scanning is more processor intensive than scanning HTTP traffic, this solution provides the flexibility to assign the correct amount of hardware where it is needed most, and not overprovision for a service. Latency is reduced by allowing the BIG-IP to ensure constant throughput by managing traffic flow to the proper resources. It also provides for flexible scaling in that services can be scaled by simply adding another node to the pool.

For an additional level of protection, enterprises can use the BIG-IP product to set up and enforce common application level security policies using the product's Universal Inspection Engine (UIE) and iRules™ to filter and block application level attacks and threats.

About Trend Micro

Trend Micro provides centrally controlled server-based virus protection and content-filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies and managed service providers worldwide to stop viruses and other malicious code from a central point before these threats ever reach the desktop.