



ANTI-VIRUS

Description of the Application

Anti-virus applications attempt to identify, thwart and eliminate computer viruses and other malicious software. There are tens of thousands of known viruses, with hundreds more being created every month. The ever-increasing use of the Internet to transmit data increases exposure to these viruses. Viruses often target the lifeblood of an organization, systems such as databases and email applications. Anti-virus software has become a critical tool in prevent viruses from causing substantial damage to the infrastructure of an organization. By inspecting files as they are downloaded to a computer, and searching for binary signatures (patterns) of known viruses attached to executable programs, anti-virus software systems block infections before they can cause harm.

Challenges to the Application Type

Organizations face a growing number of virus threats, and overwhelmed anti-virus systems often cannot handle this increased load. Most available anti-virus systems do not accommodate for scale. They have no built-in capability to provide additional protection through the addition of resources, which leaves organizations with less than optimal protection and performance, and a single point of failure in the network. Organizations should consider the following challenges when deploying anti-virus systems:

Providing high availability - Although infected or suspicious files may not comprise the majority of traffic in an enterprise, anti-virus systems always need to be on and available. Deploying a single anti-virus system introduces a single point of failure and exposes the organization to downtime and security risks.

Providing scalability - Not all business applications are downloading infected files or accessing compromised data, therefore not all business-critical application traffic needs to pass through the anti-virus layer. Organizations need to apply intelligent rules, routing suspect traffic to application-specific devices for anti-virus scanning. An organization should build an architecture that allows it to easily scale as application traffic increases and more security rules are applied.

Enhancing capabilities - Because anti-virus systems are not the only defense against attacks, other solutions need to be considered in how they complement anti-virus systems deployments. An organization should select solutions that can compliment the network security capability of anti-virus systems such as firewalls, Intrusion Detection Systems, and application traffic management products.

Enforcing anti-virus levels - Today, more and more employees are working from locations outside the corporate LAN. Remote access devices must be able to not only enforce anti-virus software on the client device, but ensure that the patch-levels are up-to-date.

Solution

F5 Networks' BIG-IP® Local Traffic Manager (LTM) product combines the expertise of anti-virus systems for email attachments, generic FTP, Web files and other application level scanning devices, and acts on their behalf to automatically respond to, act upon and prevent changing application level security threats. Using VLAN Mirroring or clone pools, the BIG-IP product directs traffic to the appropriate security device without disrupting the flow of traffic for virus checking, intrusion detection, email scanning, and other application level security services.

Organizations can use the BIG-IP LTM system to set up and enforce common application level security policies using the Universal Inspection Engine (UIE) and iRules™ to filter and block application level attacks and threats. The BIG-IP product, through the iControl™ API, is the unifying prevention point. Specialized devices can inject their knowledge by creating, deleting or editing iRules, which are then enforced by the UIE. This functionality can be used to secure anti-virus systems, web services, mobile applications, and nearly any IP based enterprise application.

The FirePass controller, F5's SSL VPN remote access solution, provides automatic integration with the largest number of virus scanning and personal firewall solutions in the industry (over 100 different AV & Personal Firewall versions), preventing infected PCs, hosts or users from connecting to your network. The FirePass controller checks client anti-virus software and patch levels, and if the appropriate software is not installed on the remote device, can be configured to automatically re-route these users to a location where they can update their anti-virus software.

Key Benefits of F5

- F5 can mirror traffic to a clone pool of anti-virus devices
- The FirePass controller integrates with over 100 different anti-virus and personal firewall versions
- iRules can set up and enforce common application level security policies.