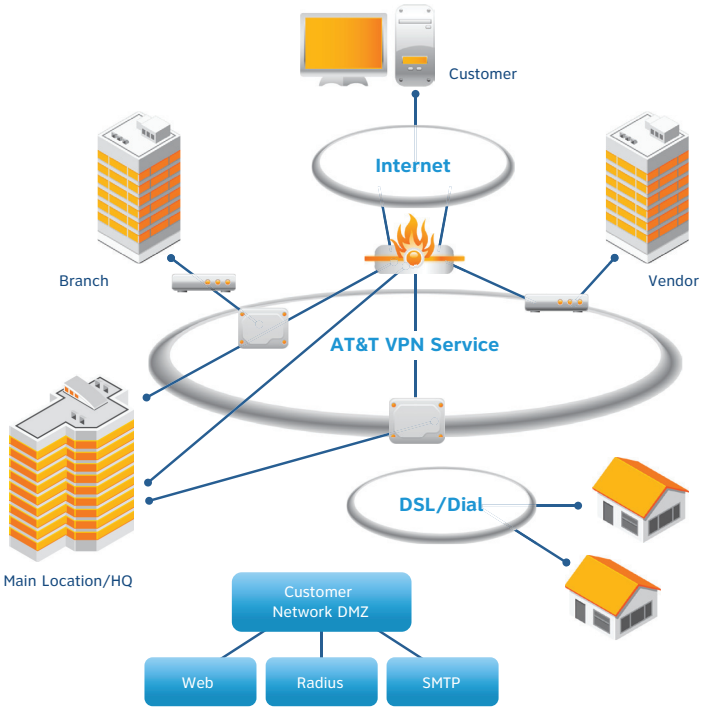
AT&T Network-Based Firewall Service℠

A key component in helping protect networks

With the growth and innovation of mobile technology, IT is transforming from a back-office operation to a facilitator of advancement, interaction and investment for customers and employees. It's the secret sauce to success.

IT is doing so much more than it used to – it's integrated in daily operations: supporting brand, providing service excellence, assisting with business development and keeping the business compliant, all while helping keep critical data secure. And, in order to help protect end user customer data from intrusions into network infrastructure, businesses need flexible, scalable and reliable security services. As part of a broader network and security strategy to manage and control company systems and information, businesses should have a strong, highly secure, cost-effective solution. And this is where Network-Based Firewall can help.

Think of the possibilities – reduce capital expenditures, decrease risk of technological obsolescence and the need for additional staff members – all with a solution that helps protect data. With Network-Based Firewall, businesses subscribe to, rather than purchase, their network security. The Network-Based security devices reside within AT&T owned and operated Data Centers, which provide 24x7x365 monitoring and attack management of the firewall service.



Potential Benefits

- Increased Efficiency – can eliminate the need for customer premises-based firewalls and dedicated internet connectivity at each location
- Improved Reliability – helps protect Internet, Intranet and extranet
- Greater Management Control – provides a central application of inbound/outbound security policies across business locations
- Increased Scalability – allows easy upgrade of bandwidth to/from the Internet as business and traffics grows
- Increased Productivity – freed resources can focus on mission-critical business and technology instead of daily firewall management

Features

- Transparent firewall
- Reports and Security Self Service through the AT&T Security Center Portal
- Static and many-to-one Network Address Translation (NAT)
- VPN tunneling through static NAT
- Hardened external DNS
- Option for multiple DMZ policies defined for different network segments
- Multiple bandwidth options to support end user customer requirements

AT&T Partner Exchange℠
Solution Provider

In addition, our highly specialized staff will help handle day-to-day operations of the Network-Based Firewall, freeing up business resources to focus on more mission-critical IT and business requirements. The security experts at AT&T will screen applications and administer firewalls, intrusion detection signatures, filters, patches and servers.

AT&T Network is an Integral Part of Security Solutions

Network-Based Firewall is designed to offer highly secure connections for end user customers, adding another layer of defense to their data. Using the economies of a large private network, AT&T helps businesses utilize their existing wide area network (WAN) investments by installing sophisticated security features directly into the AT&T network. This provides the end user customer the ability to access the Internet via existing Enterprise Permanent Virtual Circuits (PVCs) that are filtered and monitored. Since the firewall is administered in the AT&T network, businesses can potentially avoid the expense of homing remote traffic to a central security location only to be re-routed back to the Internet.

Network-Based Firewall can support different levels of configuration complexities, ranging from a simple outbound-only security policy to an extensive bi-directional policy with optional features, such as Web filtering and malware scanning.

Network-Based Firewall is designed to continuously inspect and treat inbound and outbound traffic according to the business' predefined security policies. Also, the end user customer can select required bandwidth allocation for Internet access through the firewall.

The optional intrusion detection feature inspects the content of the packet passing through the firewall and attempts to match it against patterns of known attack types or Internet worms. After a match is made, the packet will be discarded if directed by the pre-established security policy.

Reliable Firewall Management

Network-Based Firewalls are actively managed and monitored 24x7x365 by the AT&T Security Operations Center (SOC), a highly secure, fully-redundant, state-of-the-art management facility. Procedures are established between the Solution Provider and the AT&T SOC to execute configuration changes on the end user customer's security policy and firewall. Additionally, AT&T Network-Based Firewall provides a self-administration portal allowing businesses to implement changes to aspects of their firewall configuration and to view reports.

Administrators can spend countless hours analyzing rule bases and determining the requirements for each rule. AT&T Consulting Firewall Assessment Service ("FAS") is designed to address the complex configurations of today's firewall environment. FAS was created to assist organizations with internal and regulatory compliance requirements regarding firewall audits and policy review, provide administrators with information to help troubleshoot rule base issues, help identify risks to the security of protected environments and help bring order to an often chaotic rule base.