

Managed Firewall Service Network-Based

Protecting Your Network from Intrusions

The Internet has facilitated new business opportunities and revolutionized how you transact and communicate with your customers and partners. At the same time, the Internet has also left your data resources vulnerable to a variety of potential outside threats and attacks. As a result, protecting your information assets with a comprehensive, holistic security strategy, that provides secure Internet access while supporting your e-business infrastructure, is critical. AT&T Network-Based Firewall service provides a fully-managed, secure, cost-effective solution that allows you to manage and control employee access to the Internet while preventing unauthorized access into your network infrastructure.

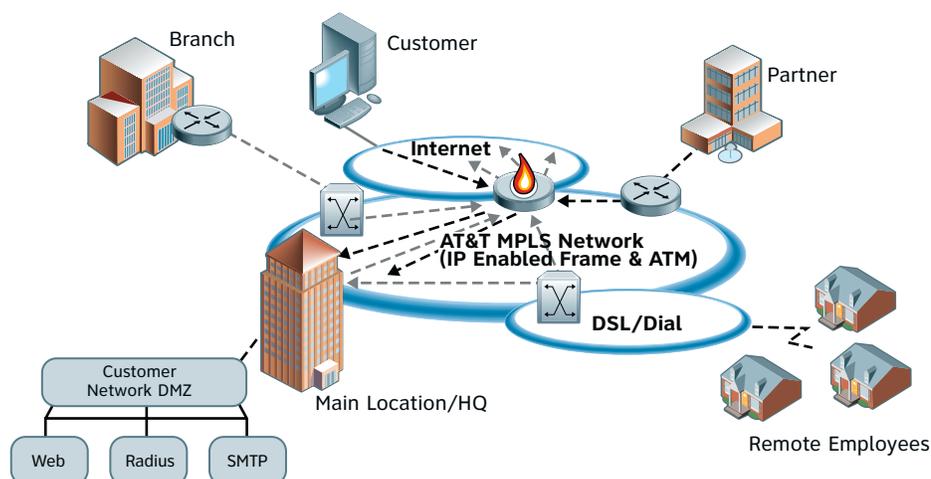
AT&T Network-Based Firewall service requires no additional equipment on your premises – you subscribe to, rather than purchase, network

security. There is no need to install customer premises firewalls and dedicated Internet connectivity at each of your locations. The Network-Based security devices reside in the AT&T Data Centers which reduces your capital expenditures, risk of technological obsolescence and need for additional staff members. AT&T owns all security assets and provides 24x7x365 monitoring and attack management of the firewall service.

The AT&T Network is an Integral Part of Your Security Solution

AT&T Network-Based Firewall service provides highly secure connections for AT&T provided transport customers along with a highly specialized staff to screen applications and administer firewalls, intrusion detection signatures, filters, patches and servers.

AT&T MPLS Network



Benefits

- Eliminates the need to install customer premises firewalls and dedicated internet connectivity at each of your locations
- Helps increase the security of your Internet, Intranet and extranet environments
- Provides central application of outbound or inbound/outbound security policies across your locations
- Allows easy upgrade of bandwidth to/from the internet as your company and traffic grows
- Available globally to enable local exit points to the internet

Features

- Transparent, stateful firewall
- Reports via website portal
- Static and many-to-one Network Address Translation (NAT)
- VPN tunneling through static NAT
- Hardened external DNS
- Numerous DMZ policies defined for different network segments
- Multiple bandwidth options to support your requirements
- Optional features, including scanning of protocols for malicious traffic, dynamic user authentication support and URL filtering
- Interworking with AT&T provided email hygiene service
- Bundled Secure Network Gateway Service that provides simple billing with one contract, one bill and price discounts when purchasing more than one service



Solution
Provider

Using the economies of a large private network, AT&T enables you to utilize your existing wide area network (WAN) investment by installing sophisticated security features directly into the AT&T network. This provides you the advantage of accessing the Internet via existing Enterprise PVCs that are filtered and monitored.

Since the firewall is administered in the AT&T network, you avoid the double expense of homing remote traffic to a central security location only to be re-routed back to the Internet.

AT&T Network-Based Firewall service supports different levels of configuration complexities, ranging from simple outbound only security policy to extensive bi-directional policy with optional features, such as URL filtering and multiple DMZs. This service will continuously inspect and treat inbound and outbound traffic according to your predefined security policies. You can also select your required bandwidth allocation for Internet access through the firewall.

The intrusion detection feature provides an additional layer of security by inspecting the content of the packet passing through the firewall and matching it against patterns of known attack types or Internet worms. After a match is made, the packet is discarded if directed by the pre-established policy. An additional feature available is the Firewall Rule Establishment option which identifies, rationalizes and analyzes your existing security and firewall rules policy to make appropriate recommendations at the technical and executive level. Periodic review of firewall rule policy is a security best practice and is required by many compliance standards.

AT&T Network-Based Firewalls are actively managed and monitored 24x7x365 by the AT&T Security Network Operations Center (S/NOC), a highly secure, fully-redundant state-of-the-art management facility. Secure procedures between you and the AT&T S/NOC are in place to execute configuration changes on your security policy and firewall. Additionally, AT&T Network-Based Firewall Service provides

a self-administration portal allowing you to implement changes to aspects of your firewall configuration and view reports.

True security comes from working with a technology partner that does more than just help overcome the pain when an attack is launched. AT&T provides best security practices and recommendations and works with you to help anticipate potential threats and mitigate impacts from the next, potentially debilitating assault on your network.

AT&T Secure Network Gateway

AT&T Secure Network Gateway service delivers state-of-the-art security features with proactive monitoring and management. We have conveniently packaged and simplified the purchasing, contracting and billing of AT&T Network-Based Firewall Service, AT&T Secure E-mail Gateway Service and AT&T Web Security Service under one contract and one invoice providing an efficient and cost-effective way to meet your business security needs.