

PRODUCT BRIEF

Managed Firewall Service Premises-Based

Business Demand for Improved Security

The surge in Internet, Intranet and Extranet technologies has provided users the convenience of connecting into a standard-based protocol network to transmit or access applications. The widespread adoption of these technologies has also given rise to security risks and the ability to eavesdrop, impersonate, infiltrate networks and distribute computer viruses. To detect and mitigate these risks, firewalls have become an important part of any corporate security program, and should be looked upon as the foundation of inter-network security.

AT&T Premises-Based Managed Firewall Service provides a highly functional layer of security to your networks. The service is a fully managed solution, which includes all hardware and software components, configuration, installation, day to day management and maintenance, as

well as expert customer support and proactive network monitoring. The service is designed to:

- Defend against unauthorized connections to your LANs
- Provide security to your users with remote accessing needs, via data encryption
- Provide a secure environment to companies who need to support an unlimited number of concurrent user sessions
- Support remote monitoring and management of the firewall server

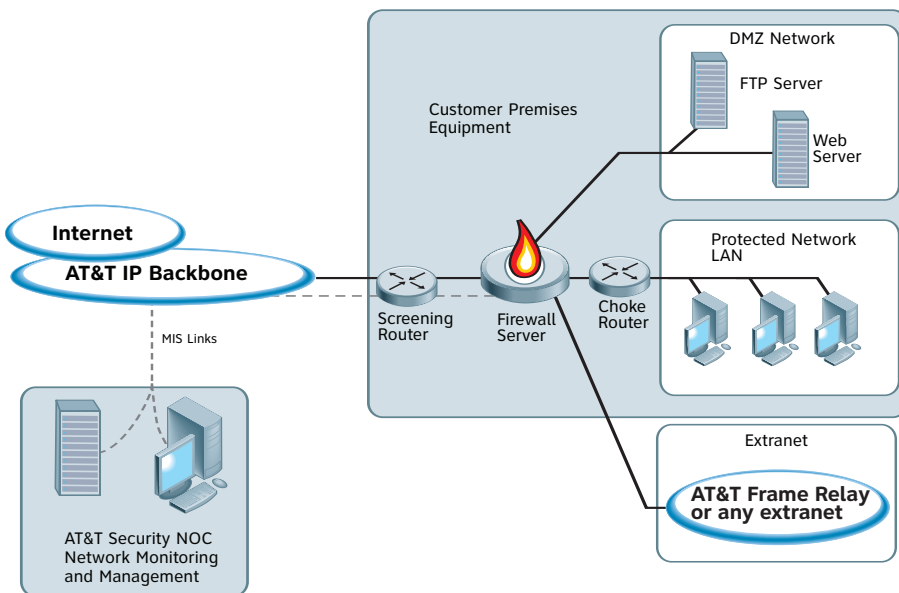
Variety of Firewall Solutions to Fit Your Business Needs

You can choose from four AT&T Premises-Based Firewall solutions that best meets your business requirements. All these services let you define

Benefits

- Increases the security of your Internet, intranet and extranet environments
- Offers you a fully managed end-to-end solution
- Reduces your capital investments, staffing and maintenance expenses
- Reduces the complexity associated with managing your IP network firewall security solution
- Allows you to customize your security policies and define different levels of security for various users and applications
- Utilizes industry-leading hardware and software with proven and reliable technology

AT&T Premises-Based Firewall Solutions



Features

- Stateful inspection
- DMZ/extranet support on most models
- High availability configurations on most models
- URL screening option for Checkpoint® on Sun Server firewall
- VPN Connectivity Option with Checkpoint and Cisco ASA firewalls
- Option to implement Nokia and Cisco ASA firewalls into AT&T Internet Data Centers
- Security reporting for Checkpoint and Cisco ASA firewalls



your own security policy and tailor the solution to the size of your user base and enforce security policy on each interface of the firewall.

- Checkpoint® on Nokia
- Checkpoint® on Sun Server
- Cisco ASA Firewall

These solutions combine the leading security industry software, Checkpoint, with either Nokia hardware or on a hardened Sun Server, or use the Cisco ASA hardware and Software platforms.

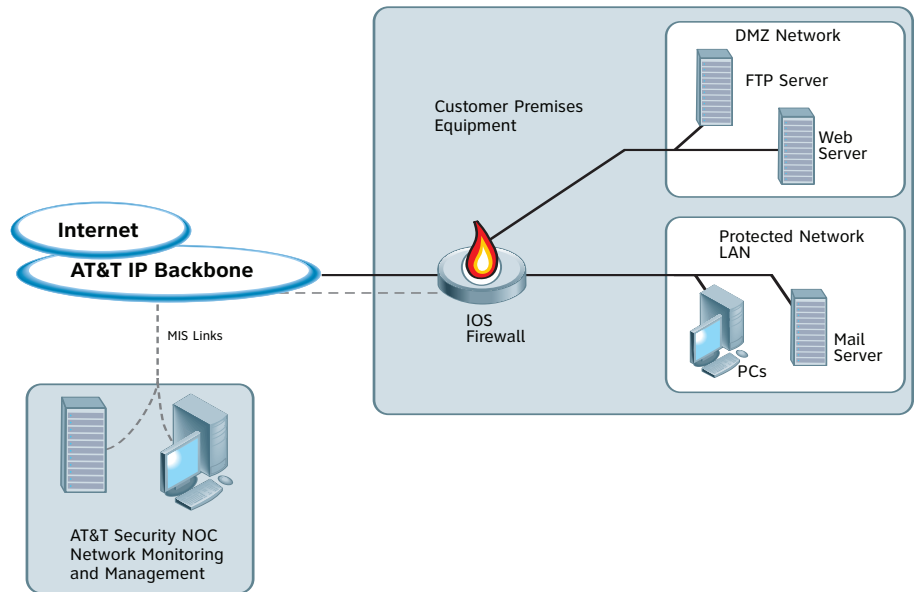
These services provide features such as High Availability configurations, higher bandwidth and security reporting capability. Depending on the firewall type and model, the configurations provide DMZ, Extranet and VPN connectivity options. The Nokia and Cisco ASA configurations can also be implemented in an AT&T Internet Data Center.

- Cisco IOS® Firewall feature on Cisco router

This configuration is appropriate for small offices that require basic security with bandwidth throughput of T1 and below. This solution is a highly functional, economical and fully managed security and firewall service on a Cisco router.

The Cisco IOS firewall code has achieved ICSA 4.1 Certification making it compatible with other firewall solutions. The AT&T supplied router connects to the Internet via a serial interface. In addition, two Ethernet interfaces are provided for a private LAN with client devices such as laptops or PCs and a DMZ LAN with servers that service requests from the public Internet.

AT&T Premises-Based Firewall Solutions



AT&T's State-of-the-Art Security Network Operations Center (S/NOC)

The firewalls are actively managed and monitored by AT&T security professionals based on your unique network security policy. These activities take place in AT&T's 24x7 S/NOC, a highly secure, fully redundant site equipped with emergency backup power. Secure procedures between you and the AT&T S/NOC are in place to provide configuration changes to the policy and firewall.

The firewalls inspect each packet and either allow entrance, deny access or pass an alert to the S/NOC. Security event logs are both collected on the firewall for customer review and sent to the S/NOC for further analysis and alerting. If there is an unauthorized

attack or suspected security breach, the AT&T S/NOC can remotely dial into a software power switch and shut down the Internet link. Together, these components provide a powerful, all in-one solution that perform routing, provide secure Internet connectivity, and apply distinct security characteristics according to a user-defined security policy.

Your ability to survive in business may depend on how well you protect assets from outside attack. Let AT&T help you defend your networks and develop an appropriate security policy.

For more information contact your AT&T Representative or visit us at www.att.com/business.



at&t

Your world. Delivered.