



DEFEND

Managed Firewalls protect your perimeter with advanced technology managed by a 24x7x365 team of security experts.

MANAGED FIREWALL

Protect your business. Any place. Any time.

The first line of defense for any business is to keep intruders out of its network. As cybercriminals become ever more sophisticated, it becomes increasingly difficult for traditional firewalls and networking teams to keep up with the attacks.

Additionally, protecting the edge of the network has become much more complex than stopping incoming traffic. Phishing, remote workforces, and unsafe web content all present built-in risks that require more advanced protections to stop.

With a Managed Firewall service, you immediately gain greater visibility into your network to help increase performance and guard against attacks and unplanned downtime. With monthly reporting and reviews by security experts, you'll know more about your business than ever before.

Built on an industry-leading Next-Generation Firewall platform, and backed by the 24/7/365 Security Operations Center, you can rest assured that your network, your employees, and your data are protected.



UNIFIED THREAT MANAGEMENT /
ADVANCED THREAT PROTECTION



NETWORK ANTI-VIRUS /
ANTI-MALWARE



INTRUSION DETECTION
AND PREVENTION



WEB / CONTENT FILTERING



SECURE REMOTE ACCESS



Next-generation firewall protection backed by an experienced security operations center.



Unified Threat Management / Advanced Threat Protection

Unified Threat Management / Advanced Threat Protection provides multiple security features and services for your business via a common management framework.



Web / Content Filtering

With Web / Content Filtering, you can easily block or screen inappropriate or unsafe web content based on your corporate policies.



Network Anti-Virus / Anti-Malware

With Network Anti-Virus/ Anti-Malware, all traffic is scanned for known threats and will quickly block or flag suspicious behavior based on policies jointly created with our security specialists.



Secure Remote Access

Designed to prevent unauthorized access to an organization's data, Secure Remote Access includes a combination of process and technology to safeguard sensitive data from external access.



Intrusion Detection and Prevention

Intrusion Detection and Prevention provides a combination of reactive and proactive measures to identify and mitigate ongoing attacks. Quickly eliminate or prevent:

- Malware (i.e. trojans, backdoors, and rootkits)
- Detect social engineering (i.e. "man in the middle", phishing)
- Assaults that target sensitive information
- Remote file inclusions that facilitate malware injections
- SQL injections used to access critical databases

INCLUDED SERVICES:



Monitoring and alerting

- Performance and utilization
- Security events
- Trending and analysis



Support and maintenance

- 24/7/365 phone-based support
- Security Operations Center (SOC)
- Firmware management of firewall devices



Reporting and metrics

- Monthly threat reports
- Compliance / Regulatory reporting
- Custom ad-hoc reporting

RETHINK CONNECTED

