Intermedia Secure^{SM}

Service Description for Managed Firewall

Revision 8/2/99

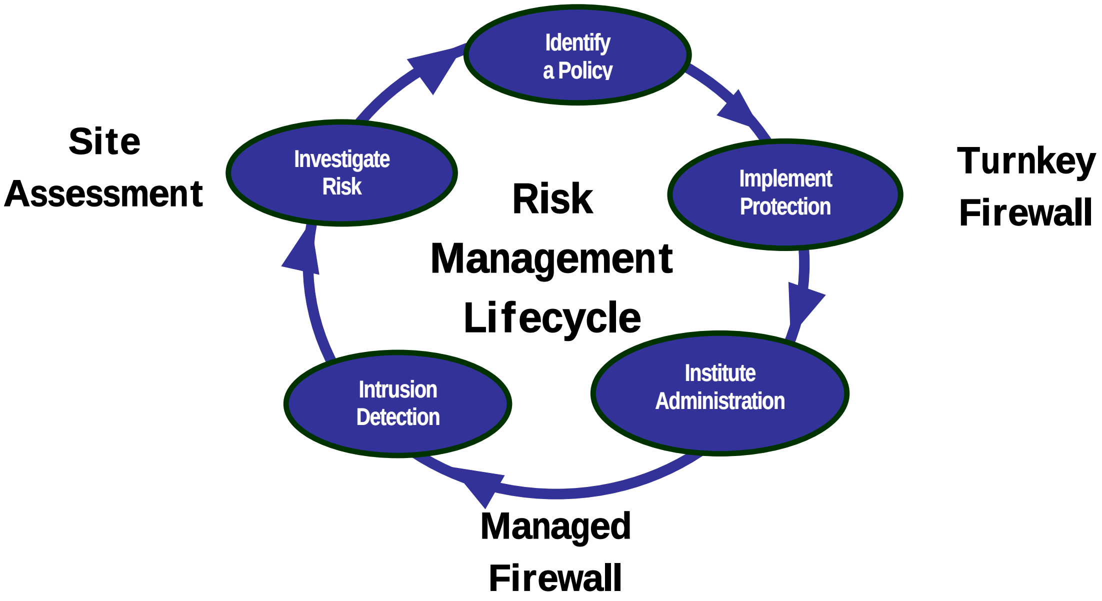
intermedia
COMMUNICATIONS

Table of Contents

1 Overview of Intermedia Secure Services

1.1 Lifecycle of Security Solutions

The Intermedia Secure Offering is an active policy-based approach to security. The latest Stateful Inspection, Virtual Private Networking and Security Management technologies are employed to ensure the premier Internet security solution set. Indeed, Intermedia's philosophy for *secure* Internet access is outlined in our Five "I"s Security Model. Each of the Intermedia Secure component offerings is designed to accomplish one or more of these key elements of effective, *secure* risk-management process.



1.2 Components of Intermedia Secure

1.2.1 Intermedia Secure Site Assessment

The Site Assessment assists customers in identifying priorities for risk management. This two-day, interview-style assessment is conducted by Nichols Research, a respected third-party security expert, to produce an inventory of security requirements and inputs from the customer's management teams. Executive management receives a prioritized report that identifies steps required to manage threats specific to the customer's business risk. To our knowledge, Intermedia is the only security solutions provider that is committed to providing this kind of third-party objectivity.

1.2.2 Intermedia Secure Turnkey Firewall

This solution delivers on-site firewall installation and integration. Security Engineers install the firewall systems and use our comprehensive Acceptance Test for quality assurance. Engineers work with customers to enforce a security policy that manages the risk identified in the Assessment. The firewall(s) provide access control, perimeter defense, and Virtual Private Networking.

1.2.3 Intermedia Secure Managed Firewall

The Managed Firewall Service is a complete solution for enterprise networks, because it delivers comprehensive security management, including a completely managed Firewall-1 solution. As data center and customer satisfaction experts, we built and operate the Security Management Center (SMC). This state-of-the-art facility is constructed with network, power, and system redundancies. Skilled professionals operate the SMC on a 24x7x365 basis, serving the complex security needs of financial, retail, educational, and government customers.

2 Why Intermedia is your Best Choice for Managed Security Solutions.

2.1 A Strong Commitment to Excellence

The only true metric for success is *customer confidence* with Internet access. Intermedia is unrelenting in securing unique redundancies for Managed Firewall customers. Many providers offer basic configuration management and remote-controlled firewalls. However, Intermedia delivers comprehensive security where customers receive tangible benefits daily. Examples of the many features that set apart from other providers are Redundant Hard Drive Solutions, Secure Out-of-Band (OOB) access and intervention, guaranteed Service Level Agreements, Comprehensive Reports, and Daily Archiving of Firewall Logs.

The Intermedia Secure solution is fully scalable to meet a corporation or agencies' needs now and in the future.

2.2 Strong Vendor Partnerships

Intermedia overwhelmingly has the best and broadest relationships with the major security product vendors in the marketplace. As an Axent VAR, ISS Partner, Cisco Powered Network, and Check Point Premier Partner, Intermedia can deliver better products faster than many other managed firewall vendors who have limited exposure to changing developments in the security industry. The true indicator of the Intermedia difference is our customers' evaluation of our performance. Intermedia customers give us a 99% satisfaction rating in supporting them as both customers and business partners.

2.3 Open Security Standards & Alliances

As the IP networking and data networking needs converge with a more globally focused economy, the need for more comprehensive and cohesively managed security is evident. Intermedia holds the view that no one security vendor or service company can provide the best solutions without adopting an open and extensible architecture that allows best-of-breed products to inter-operate, delivering the required integration with the network, and the networked user. Intermedia is a proud member of both OPSEC and ANSA because of our commitment to deliver comprehensive and adaptive security management to business customers.

2.3.1 Adaptive Network Security Alliance (ANSA)

ANSA, The Adaptive Network Security Alliance, is the first step towards self-curing networks. ANSA is an open, technology-focused partnership program initiated by ISS (Internet Security Systems, Inc.) and over 40 leading partners. The goal of ANSA is to deliver the technology needed to create interoperability between adaptive network security products and traditional security and network infrastructure products.

2.3.2 Open Platform for Secure Enterprise Connectivity (OPSEC)

OPSEC is single platform architecture designed to allow integration and management of all aspects of network security through an open extensible framework. By selecting OPSEC Certified products, you can be guaranteed interoperability at the policy level between FireWall-1 and best-of-class, leading edge security applications. Intermedia is a strong advocate of the OPSEC program because it assures the absolute best tools to provide security services to our customer. The advent of OPSEC is a significant milestone in the path to build active, secure networks that do not constrain users and allow people to securely and ubiquitously conduct business in the new information economy.

3 Benefits of Managed Firewalls

- The cost of having Intermedia manage your firewall is much less than staffing, training and maintaining in-house security expertise.
- Intermedia is a strong partner of multiple firewall software vendors and has access to new technologies before they are widely available to the market. This knowledge and cooperation is used for our customer's benefit for new product releases and product upgrades.
- The implementation of a firewall is a discipline of it own, separate from the type of skills required to install and maintain most common networking systems. Intermedia staffs professionals who are trained to manage firewalls.
- The Security Management Center (SMC) is a facility designed specifically for the purpose of providing monitoring and management services to firewall customers.
- This service allows customers to focus on their policies and access controls rather than figuring out how to implement them on the firewall.
- Intermedia archives log files from the firewall and delivers comprehensive monthly reports based on the data.

3.1 Cost Estimate of Providing In-House Secure Access

The following cost analysis shows the cost to a moderate enterprise for in-house comprehensive security to protect their Internet access. If these numbers look exorbitant, think about the fact that most companies spend more money on coffee annually than on protection for their networked information assets.

Item	Cost
Firewall Software Market Price including Encryption	$ 15,000
Cost of Quality Hardware to Service T-1 Speed (Estimated)	$ 5,500
Network Security Engineers to provide 24x7x365 Management	$220,000 (55K/ea.) (Annual Cost)
Quarterly Penetration Tests (Out-sourced Market Price)	$ 4,500 (Annual Cost)
Firewall Training for Engineers	$ 24,000 (6K/ea.) (Annual Cost)
Reporting Software & Annual Training for Engineers	$ 3,000 (Annual Cost)
Total:	**$ 272,000**

Assumptions:

1.) A minimum headcount of 4 Engineers is required for 24x7x365 Coverage
2.) Security Technology/Software changes at least twice a year, requiring additional training for engineers.
3.) Reporting software is required to compare use of the network against the corporate Acceptable Usage Policy (AUP).
4.) Firewall Software Cost is based on a typical software user license for T-1 Access

3.2 Cost Benefit of Choosing a Managed Service Provider

Item	Total 1 Year Fees from Intermedia	Total 2 Year Fees from Intermedia	**1 Year Savings to Customer**	**2 Year Savings to Customer**
Managed Firewall	$ 33,588	$55,176	**$ 238,412**	**$ 444,324**

Assumptions:

1.) Firewall Software Cost is based on a typical software license.
2.) Cost Savings are based on above Estimated Customer Costs to provide an in-house Managed Firewall minus Fees
3.) Intermedia Fees Totals based on Average List Pricing

4 Scope of Managed Firewall Service

Intermedia provides quality "Risk Management" for Managed Firewall Customers.

While no network can be absolutely secure, closing off all unguarded entry-points into a private network dramatically decreases the risk of conducting business over the Internet. Also, tightly controlling communications in-bound from the Internet based on source with destination entities (hosts or networks) with strong user authentication is crucial to electronic peace of mind.

Using this "implicitly deny all electronic communications not specifically permitted" methodology, the risk of connecting your business to the Internet is greatly decreased. Indeed, the sum of all allowable communications to and from the Internet is the customer's *security policy*.

If a customer is unclear as to what their security policy is or how to develop their security strategy, Intermedia recommends they invest in the Site Assessment. This is a two-day on-site assessment of security needs coupled with an exit briefing that delivers recommended security policies and applicable next steps.

The Intermedia Managed Firewall Service is simply using sophisticated firewall technology to enforce the customer's security policy and maintain reliable network capabilities for trusted LAN/WAN users and user groups.

Intermedia takes managed security to a new level and maintains the Security Management Center (SMC) to provide both the electronic infrastructure and a professional service organization to deliver comprehensive IP Security. Our mission is complete customer satisfaction.

5 Service Description

5.1 Managed Hardware and Software

Intermedia delivers best-of-breed Customer Premise Equipment (CPE) and software by identifying strong vendor partnerships with industry leaders. Available hardware platforms include the Nokia IP300, IP400 and IP600 series firewall appliances. Pricing varies based on the size of firewall license and Nokia platform. Intermedia selected Nokia's platform because of its ability to provide a feature-rich, repeatable, and highly available solution in diverse networking environments. Nokia appliances provide the most scaleable firewall appliance on the market. Features include: dynamic routing protocols, built-in high availability functions, and a small, efficient operating system.

5.2 Firewall Monitoring

The software framework used in the SMC is designed to monitor uptime for a variety of firewalls. If a Firewall is detected to be down escalation begins immediately to identify the source of the problems. Intermedia Security Technicians follow strict procedures for documentation when responding to network outages.

5.3 Automated Data Archiving

Log files are created by the firewall for several reasons. In general, log files account for the in-bound and out-bound communications that pass through the firewall. This information is helpful in determining network usage etc. Firewall logs are often helpful in providing information useful to identifying patterns of misuse. The off-site collection and backup of this data is a particularly important benefit of this managed firewall offering.

Data archiving of firewall logs is performed during standard configuration windows. Usual configuration windows are scheduled between 12AM and 6AM Eastern Standard Time (EST).

The data is preserved in a customer management infrastructure system. Log data is stored in a high-capacity disk array for easy processing. Log files are saved on disk for one month and then moved to more permanent media storage.

5.4 Monthly Log Report

The log data collected in section 5.4 of this document is used to create an aggregated monthly view of network activity and a summary of the most common events on the network. Intermedia maintains a standard report format designed to structure important data into an easy-to-read deliverable for network administrators.

The following items are included in a standard report:

- Top Ten Web Sites Contacted
- Total Bandwidth Utilization by TCP / IP Service
- Total Bandwidth Consumption by IP Network (where applicable)
- Summary of Change Request for the last month
- Snap Shot of Firewalls Rules Base

Reports are maintained in disk for one year. Reports more than one year old are saved on permanent media for storage.

5.5 Configuration Management

Using the customer's security policy, Intermedia manages all changes to the firewall's configuration. After Intermedia completes the firewall installation, the firewall properties and account information are included in the software framework used to manage the SMC. This software creates a new account for the firewall, which contains all of the necessary contact information reports and configuration filing structures. Essentially, Intermedia has automated the art of providing quality attention to each and every firewall under the care of the Security Management Staff.

5.6 Uptime, Performance, and Capacity Planning

Intermedia proactively monitors firewall performance based on log data, our own router statistics reporting tools, and other network management tools like the Intermedia NetScanner^{tm}. Intermedia is a leading provider of quality metrics for Business Connectivity Customers. Also, we deliver standard hardware that is already satisfactory for the growth of a customer's bandwidth needs. In most cases, the access line size is an issue long before a firewall's capacity is consumed. Intermedia is developing additional features to this basic offering that will deliver real-time performance information directly from the firewall platform.

5.6.1 Redundant Hard Drive Configurations

Uptime is a primary concern for all companies doing business on the Internet. Intermedia has found that disk drive failures are the most common cause of system downtime. For this reason, two internal hard drives are offered as an option on the IP440 managed firewall platform.

5.6.2 Out of Band (OOB) Solution

Out of Band (OOB) access to the firewall is very important in troubleshooting network problems or defending against network-based attacks. If a network connection is flooded or down, Intermedia connects to customer premise firewalls using secure modems. This methodology allows a second management interface to the firewall and provides an extra measure of redundancy. Customers must provide a dedicated phone line as part of this product component.

5.7 Virtual Private Networks

There are two basic types of VPN capabilities supported by Intermedia.

5.7.1 Point to Point VPNs (Office-to-Office)

Management of firewall driven VPN is included in this offering as long as Intermedia has sole administrative control to all tunnel end-points. Special considerations may be made using the pre-sale "Customer Configuration" process. In order to maintain a high quality of service, it is strongly recommended that all VPN installation and equipment be purchased through Intermedia.

Management of Virtual Private Networks includes key & configuration management as well as bi-directional filtering of VPN electronic traffic where applicable.

5.7.2 Remote Access VPNs (Dial-Up-to-Office)

Intermedia provides support for remote access VPN customers at consistent commercial rates. Clients are encouraged to deliver remote access over the Internet with strong user authentication. Indeed, modem pools are common targets of hackers since passwords are usually weak.

The Customer's MIS/IT personnel are charged with supporting VPN access customers by installing mobile security software. Intermedia manages client setup for key-exchange, password preference, and network access control. Intermedia interfaces directly with customer IT Professionals. All customer client-side issues are routed through the appropriate MIS staff to qualify client difficulties or errors specific to the mobile workstation's method of connectivity. The Service Level Agreement (SLA) for Mobile VPN/Remote Access VPN is a "Best Effort Support Guarantee" since the work involves supporting client software delivered on customer-owned and operated mobile equipment.

5.8 Quarterly Remote Scanning

At the end of every quarter, Intermedia scans each firewall using ISS Scanner Software to validate the host security of the Firewall System. Intermedia may also opt to scan the Firewall when major patches, operation system revisions or other upgrades are performed.

6 Security Management Center (SMC)

6.1 Facilities

Security and surveillance are necessary to maintain the privacy of all customer information. This is why Intermedia's management facility is accessible to properly authorized employees only. The entire building is protected by an electronic key-card entry system using an alarm response and logging method. Intermedia is also continuously protected by uniformed guards and has 24-hour per day Closed Circuit Video monitoring. All of these methods are used to ensure the complete security of your information from physical threats.

6.2 Power Supply

Power protection should be viewed as an insurance policy. The entire Security Management Center's power supply is backed up by an Uninterruptable Power Supply (UPS) battery-based system, providing extra fault tolerance for our managed security framework and software. The UPS system has enough power to operate the entire facility until the Diesel Generator comes up (within 90 seconds), allowing us to manage customer security without interruption.

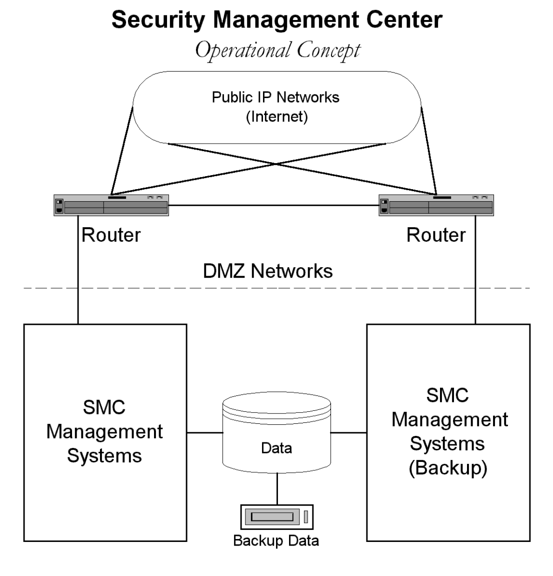
A Diesel Generator provides additional backup power protection should a power outage last more than a few minutes. This Diesel Generator can supply all of the power necessary for the Security Management Center and can be refueled to power the facility indefinitely.

6.3 Staff

Trained professionals staff the Intermedia. Their #1 Mission is customer satisfaction. They are approachable and follow strict escalation procedures to quickly address attempts to enter or deny service to customer networks.

6.4 Network Approach

The SMC was designed from the ground-up with redundancy as the cornerstone. The facility is designed to take advantage of the Intermedia Gold Ring fiber optic backbone, with multiple routes to the major NAPs (Network Access Points).



7 Service Level Agreements & Customer Support

7.1 Upgrading Hardware and Software

Intermedia will provide all major firewall software enhancements for the term of the contract. Hardware upgrades for performance and network growth issues shall be contracted separately. The customer and Intermedia will agree upon an Upgrade Proposal & Statement of Additional Work document before on-site work will be performed. Customers may be called upon to assist in performing "walk through" software enhancements periodically.

7.2 Configuration Windows

All major modifications to Firewall Software or Operating Systems are done during a pre-announced configuration window. The standard configuration for such changes will be announced to customers via email. Occasions that require additional configuration windows are discussed with customers and then scheduled for completion. The IT Professionals (Point of Contacts) will receive e-mail prior to the execution of a configuration window.

7.3 Network Access Control Change Request

Network access control changes are performed on the day the requested change is received from the customer. Customers send e-mail to a special role account for entering the request. Network access control changes are made within six hours.

7.4 User Preference Change Request

User preference change requests are typically less critical than changes in network access controls. Although these changes are handled through the standard role account, lower-priority is given to these types of requests. User Preference Changes are made within twelve hours. A special escalation process is available for termination or removal of access rights for employees that no longer work for the customer. Termination for Accounts of fired employees is handled immediately.

8 Summary of Scope & Service Deliverable

COMPONENT DESCRIPTION	INTERMEDIA SERVICE DELIVERABLES	CAVEATS / PREREQUISITES
Managed Hardware & Software	Intermedia managed service turnkey = lower entry level cost, no large capital expenditure. Software and Hardware provided.	None
Configuration Management	Installation of initial security policies for both user and network preferences, maintenance of backup configuration files for disaster recovery. Firewall driven authentication account changes for user and group properties.	Well-defined Security Policy, recommend Intermedia Secure Site Assessment to customers who have no security policy.
Firewall Monitoring	Monitoring of Firewall Uptime and Availability	None
Security Analyst Escalation	On-call experts for handling particularly complex hacking or Denial-of-Service (DOS) attempts.	On-call 24x7
Monthly Log Reports	Full report based on one-month aggregate firewall log data.	Customer provided Point-of-Contact (POC) to receive reports.
Automated Data Archiving	Daily process initiated by the firewall to deliver firewall logs back to a collection facility in the DSMC. Includes backup of firewall configuration for disaster recovery.	None
Performance & Capacity Planning	Use of standard Intermedia tools for monitoring performance of leased line and firewall throughput. Analysis of log data and other system measurements to recommend improvements as network growth occurs.	Intermedia is developing real-time CPU utilization and other benchmark information tools to use in real-time monitoring.
Virtual Private Networking (Point to Point /Branch Office)	Key and Tunnel Management between Intermedia operated Firewalls.	VPNs must use the same Firewall on both ends.
Virtual Private Networking (Remote Access/ Mobile Users)	Provide client and user access rights/configuration management.	MIS/IT Director responsible for client systems support. Escalates to SMC for security specific issues.
Quarterly Remote Scan	ISS Scanner is used to Validate the Host Security of the Firewall System Quarterly.	None
Service Level Agreements	Major Configuration changes through standard, pre-announced Config Windows. Same day response for all configuration modifications for network and user access rights. 24 hour (best-effort after 3PM EST)replacement on hardware/equipment.	Customer sends e-mail to initiate change. Intermedia Authenticates change requests.

Note: This is a working document that may change at any time at the discretion of Intermedia for service improvements and or changes in security technology and product definition.