Intermedia Secure

Statement of Work Scope for Turnkey Firewalls

Revision 1/5/99

Purpose Statement

The purpose of this document is to establish the engagement scope used with Intermedia Secure Turnkey Firewall. The scope of work provided herein is Intermedia Communications, Inc., hereafter ("Intermedia"), confidential and intended for the sole use of customers, customer prospects, or partners/agents.

This document details:

- A written explanation of all deliverables
- Essential customer requirements for full benefit of the engagement
- Customer satisfaction model and associated processes
- Use of essential documents

Table of Contents

1. Introduction

1.1 Firewall Methodology

Intermedia's Methodology for securing the private Local Area Network (LAN) from the potentially hostile or harmful Internet-borne threats is simply to drive the customer's security policy using best-of-breed firewall software. Inter-networked systems and messaging are essential to today's businesses. By limiting access only to the required services between trusted host systems or networks, the risk of internal misuse or external intrusion is dramatically decreased.

All firewall-driven security postures begin with an implicit deny or all-stop rule configuration. This means that only the data traffic that is specifically allowed by the firewall configuration will be passed. In most applications, network services that originate from the trusted network (company LAN) are allowed to pass in the least restrictive mode possible. Inbound traffic is treated much differently. Specific firewall rules or combinations of rules must be created to both allow necessary business data communications to work and to restrict access only to trusted people and/or computer systems.

The sum of all network access restrictions and/or privileges is called a “security policy.” The firewall is simply the software-driven enforcement of the company's security policy.

☛ **It is essential for all companies who have invested interest in protecting their data traffic and its resources to have a written Network Security Policy.**

1.2 Component Integration and Installation

Intermedia Communications delivers quality hardware and software, combined with the best systems integration, to achieve enhanced Return on Investment (ROI) for customers. Components systems are worthless without a responsible and comprehensive understanding of the component relationships. Moreover, every brand of firewall software requires a complete understanding of its unique features and methodologies. Essentially, each firewall implementation is a separate discipline of its own. For this reason, Intermedia maintains solid, supporting relationships with Check Point Software Technologies, Ltd., Axent Technologies, and Cisco Systems, Inc., so we can take all of the headaches out of the introduction of a firewall into the customer network.

1.2.1 Software and Operating Systems

One of the essential parts of a firewall installation is managing the details of software inter-operability. The integration technician will install the Operating System and the firewall software with the appropriate vendor-recommended patches. After the firewall installation and Acceptance Test, it shall be the customer’s on-going duty to perform routine vendor upgrades. Most of the time, customers apply upgrade through patches commonly found on the vendor’s web site.

1.2.2 Hardware and LAN Interfaces

Intermedia will obtain all hardware used with Turnkey Firewalls. For 1999, Intermedia chose the Compaq Prosignia 200 System for all Firewalls using the NT Operating System. For Unix Systems, Intermedia standardized upon Sun Microsystems Ultra 5. Intermedia will provide similar hardware platforms subject to the availability of standard hardware or to technical requirements specific to a customer network.

☛ **Special hardware configurations are available. However, Intermedia requires that all hardware either purchased by the customer or by Intermedia be approved through our custom configuration process**.

1.2.3 Required Network Components

To complete a successful Firewall Integration, Intermedia must be notified of any network deficiencies that exist before the firewall integration. E-Mail Servers, DNS servers, and other customer-administrated systems must be in a full functional capacity when upgrading network security. Otherwise, essential network services will not test properly and may extend the cost of the Turnkey Firewall.

The customer, prior to the firewall installation day, shall provide several items of hardware:

- Ante-Firewall Network Hub (Either 10/100BaseT or TokenRing), a 5 port hub will usually suffice. The firewall may not be plugged directly into customer routers.

- Post-Firewall Network Hub (Either 10/100BaseT or TokenRing). This network device is used to connect all LAN connectivity into the firewalls. Customers using LAN routers to bridge multiple LAN segments will plug the routers directly into the hub. The routers default router setting must be configured to use the IP address of the Internal Interface of the firewall.

1.3 Expectations Establishment

1.3.1 Dedicated Installation Coordinator

Intermedia provides all Business Connectivity and Security Services Customers a dedicated Installations Coordinator. This affords the customer several benefits that include: an interface to the Order Tracking Processes, a single point of contact for all pre-installation issues, and assistance in performing all of the information gathering tasks required for a successful firewall installation or "security policy establishment."

1.3.2 Communicating Your Needs

It is imperative that all customers discuss any pre-installation issues with their Service Delivery Coordinator. The ultimate objective of a firewall installation is to deliver to the customer network services similar in capacity to those uses before the introduction of the security policy. In order to achieve this objective, customers must deliver to the installation coordinator and in some cases to the actual Integration Engineer the required information about their network.

☛ **If network information is scarce or a security policy does not exist, Intermedia offers a Site Assessment product that will deliver the necessary up front consulting.**

1.3.3 Installation Process

(1) Order received in Order Tracking System. Firewall Installation Coordinator calls customer to confirm order.

(2) Firewall Installation Coordinator faxes/mails customer Welcome Kit: Pre-installation Questionnaire, Customer Readiness Checklist etc.

(3) Firewall Installation Coordinator obtains equipment & software for Installation.

(4) Firewall Installation Coordinator coordinates with Leased Line Coordinator on Leased Line FOC date from local-loop provider to schedule (preliminary) firewall install.

(5) Customer delivers to the Firewall Installation Coordinator the Network Map, Pre-Installation Questionnaire and the signed Turnkey Scope Document.

(6) Firewall Installation Coordinator and Integration Technician review the Network Map and Pre-Installation Questionnaire. A call to the customer is done if either have questions.

(7) Leased-Line is confirmed Operational

(8) Final Delivery Date for Firewall Installation is given to the customer

(9) On-Site Integration (usually 1, sometimes 2 days for enterprise networks), customer Acceptance Test

(10) Firewall Installation Coordinator calls customer for QA follow-up Conversation.

If the customer already has connectivity, omit items 4 and 7

1.3.4 Leased-Line Delivery & Firewall Scheduling

The primary task of the Firewall Installation Coordinator is to schedule and deliver timely integration to customers. Intermedia will deliver the firewall within **5 business days** of a leased-line "operational date." If the customer has not purchased a firewall in combination with connectivity, the firewall will be delivered within **10 business days** of the order's receipt in the Order Tracking System. Customer caused delay's in providing information about their network can lead to delays in the integration schedule. For this reason, it is imperative that the customer delivers the pre-installation questionnaire and network map to the Firewall Installation Coordinator as soon as the information can be collected. The final installation date is not established until these documents have been received.

1.3.5 Customer Required Deliverables

Please pay careful attention to the information detailed in this section. Intermedia's desire is to deliver absolute customer satisfaction. The process of installing a firewall is a participatory one on the customer's part. Information regarding the network and its components are crucial to the success of the endeavor.

1.3.6 Network Map

A network map is essential for planning all electronic infrastructure improvements. Using a network map is helpful in isolating network topology, and from a security perspective, understanding any weaknesses. A network map is required before performing any

firewall integration. If a customer does not have a network map, the Firewall Installation Coordinator will provide an example map for them. Network maps must detail all network entities by IP Address. It should identify all servers, switches, routers and workstations.

1.3.7 IP Address Assignments & NAT

Customers that were assigned their own network blocks directly from the IANA must provide Intermedia with their CIDR Block information, that is, the number of contiguous networks assigned.

Customers who have Intermedia assigned IP numbering will provide the Firewall Installation Coordinator with their Leased Line Number. The Firewall Installation Coordinator will verify the IP assignment with the customer.

It is common practice to use firewall driven NAT (Network Address Translation) in anticipation of future network growth. NAT is a optional part of the firewall integration. Its function is based on two requirements.

- Customers must either provide their existing network numbering topology as part of their pre-install questionnaire or network map or re-number the network before the integration of the firewall**.** Host and Server renumbering is NOT part of a Turnkey Firewall.

- Customers not using NAT are only affected by these requirements if they are changing service providers and require new IP Address space from Intermedia.

1.3.8 Current Routed Networks

Customers must declare all network sub-networks or separate Local Area Network (LAN) segments on the Network Map. This information is used to coordinate any routing changes required for a functional firewall implementation. It is also useful in establishing security policies for different company divisions - separating access privileges for finance systems etc.

1.3.9 Shared Connectivity of Business Partner Connectivity

Intermedia may address the risk of additional out-bound connections to Business Partners or Back-up Internet connections if the work can be confined to configuration on the single Turnkey Firewall. Additional engagements will be recommended when applicable.

Customers must depict these kinds of connections on the Network Map. Modem Banks, Desktop Fax Modems, and ISDN Lines can be harmful back-doors that reduce the firewall's ability to manage the risks of direct Internet connectivity.

1.3.10 Pre-Installation Questionnaire

The Intermedia Pre-Installation Questionnaire is a critical document in performing a firewall installation. Pointed questions are delivered to find out information used in developing firewall rules, firewall network configurations and so forth. Customers are

urged to deliver this document as soon as possible so the information will be reviewed with time for installation technicians to ask questions.

1.3.11 Site Assessment Options

Intermedia maintains a group of on-site assessment products for occasions when the customer requires additional assistance in discovering their risk & vulnerabilities or needs more complex analysis of their network security needs.

2. Customer Prerequisites

2.1 Addressing Network Failures First

It is difficult to deliver security for systems that are already malfunctioning or broken. It is important to address any network failures or improper configurations before introducing a firewall into the networked environment. Intermedia's purposes to leave networks as operational as they were before the firewall's installation. This objective will not be achieved to everyone's satisfaction unless precautions are taken to make sure that the network is at complete operational status.

2.2 Network Renumbering Requirements

A fundamental concept of networking is that each interface on a device that performs routing of IP traffic must be on a different network. A firewall is a device that routes IP traffic. Therefore, each interface on a firewall must be assigned to a different logical network. There are several options available to customers.

1. First, the customer may use the allocation of IP space that they have been granted by their Internet Provider on the external interface of the firewall and use Network Address Translation (NAT) on the internal interface of the firewall. Security Product Operations will assist customers with Network Address Translation at the time of the installation. Additionally, Security Support Technicians can assist customers with NAT after the installation.

2. Second, if the customer has a large enough block of address space, the customer may subnet the address space to accommodate two separate networks on each side of the firewall. Security Product Operations views the sub-netting of address space to be part of the normal duties of a Network Administrator. Intermedia is not responsible for assisting customers with the sub-netting of their allocated IP space.

Intermedia policy dictates that a customer must be using 60% of their IP space before an additional allocation will be made. In the event that a customer is using more than 60% of their allocated block, a final option may be to request additional IP space from Leased Line Customer Service.

☛ **Security Product Operations can not assist customers in their request for additional address space. It is the customer's responsibility to request additional address space before the installation of the firewall.**

2.3 Announce the Configuration Window

One item that IT/MIS personnel typically forget to announce is the configuration window in which network connectivity will be down. Intermedia recommends that the responsible IT person announce the introduction of additional network security prior to the day of installation. Network traffic on the day of installation will be down for periods as the firewall is implemented and security policies are adjusted.

☛ **Please see Figure 10.1 for a summary of additional customer prerequisites.**

3. Network Connectivity

3.1 Routed Networks & LAN Segments

All networks on the customer's LAN must be routed by default to the firewall. This usually is achieved by making configuration adjustments on LAN routers or client systems. Configurations of TCP/IP configurations on Internal/LAN routers, client systems or servers are beyond the scope of work for a turnkey firewall. IT Managers must be present during the installation of the firewall in order to provide configuration changes, if needed, to network dependent devices (mostly routers).

3.2 Internal Routers/Routing Topology

If no internal (LAN-side) routers are in use, then the default router configuration for all network entities should be the LAN-side interface of the firewall. If internal routers are in use, then the routing topology of the entire network should be reviewed before the firewall installation.

3.3 Recommended DNS & IP Transition Procedures

For customers who change their Internet Access to Intermedia, the following network transition procedures are strongly recommended:

1. Intermedia conducts a zone transfer or all domains owned by the customer – out of the past providers DNS servers.

2. Customer sends Intermedia written (company letterhead with a principle's signature) authorization to become Primary for the customer's domain.

3. The customer renumbers their network by either:

    A. Renumbering the NAT (Network Address Translation) functions on their firewalls or routers.

    B. Renumber their router configurations to use Intermedia assigned IP Addresses. [If Intermedia Provides the CPE, then this step is not necessary]

    C. Consult with the Firewall Installation Coordinator for addressing complex renumbering issues.

Intermedia strongly recommends the use of RFC 1918 reserved address blocks for all firewall-protected networks. Customers are responsible for the renumbering of all client systems, servers or

routers. Intermedia is always happy to give advice on renumbering strategies before a firewall installation.

4. Nameservice

4.1 Protocols Included

DNS is the only supported network naming convention, protocol etc. as part of a standard Turnkey Installation.

4.2 Protocols Excluded

Applications using NIS, NIS+, or WINS **do not** provide proper methods of securing electronic data. From a border-gateway perspective, only DNS is necessary. In the rare event that the customer requires the installation of a stand-alone DNS server, or documents requirements for one of the above excluded methodologies, the networking approach will need to be reviewed/validated by Intermedia.

The Customer shall provide, as part of their network map, information on all Internal DNS or other naming services used on their LAN**.**

5. Virtual Private Networking

5.1 Point-to-Point Virtual Private Networking (VPNs)

Virtual Private Networking is a powerful technology that is built-in to most modern firewalls. However, due to the varying nature of VPN technologies, Intermedia's commitment to customers is structured via the below approach.

☛ **Customized integration of VPNs with Firewalls previously procured from Intermedia or with firewalls maintained by third parties is handled on a case-by-case basis.**

5.1.1 Heterogeneous Virtual Networking

This refers to encrypting and encapsulating packets between two firewalls that are not manufactured by the same vendor. Example: creating a VPN between a Guantlet and a Raptor Firewall.

Since Key Exchange is not standard among firewall vendors, Intermedia does not offer a predictable, 100% satisfactory result as part of a standard Turnkey setup. Creating VPNs between different firewalls is possible, yet the qualification of network elements, establishment of software techniques and other processes are out of scope for our standard service. Special consulting is available through our custom configuration process

5.1.2 Homogenous Virtual Networking

The setup of Inter-office/Inter-firewall Virtual Private Networking is included in a standard contract if both tunnel-endpoints are procured as part of the same integration service. Essentially, if both end-points are turnkey firewalls of the same type.

5.2 Remote Access VPN Setup

The Integration Technician will demonstrate the establishment of VPN Tunnels to Secure Remote or Eagle Mobile Clients. This includes setup of client software and initial key exchange.

☛ **A laptop or workstation shall be required of the customer for this exercise. The Configuration of Mobile VPN Software is limited to the demonstration of client setup procedures on either Eagle Mobile or SecuRemote Software.**

Note: Cisco does not provide client software for PIX.

6. Network Authentication

6.1 Firewall Driven Authentication

The Firewall Integration Technician will demonstrate the establishment of user and group authentication accounts that are part of the firewall's user and group database. This includes S/key, if the customer's security policy calls for its use.

6.2 Customer Provided Authentication Servers

Integration of Radius, Tacacs+, Kerberos or other authentication mechanisms are provided with a Turnkey Installation as long as both vendors support them. Intermedia will be responsible for the forwarding of proper electronic dialogue between the firewall and the authentication server.

Customers must provide operational authentication servers with appropriate software revision levels. Customers may contract with Intermedia on a time and materials (T&M) basis to resolve any authentication server related difficulties.

6.3 Policies on User Specific Access Preferences

User account preferences for secure network access from the Internet to the corporate LAN are the responsibility of the customer's IT Staff.

The integration technician will provide consistent and applicable demonstrations of firewall authentication and account setup. Turnkey Firewall installations are focused on providing integration of all network components into a cohesive security policy delivery function. User preferences are simple administrative tasks.

7. Alerts & Notifications

7.1 Making the most of Alerting Mechanisms

IT personnel benefit from firewall notifications only if they understand what to do with them. Firewalls are manufactured to report suspicious activity based on exceptions to the firewall rule base. The next step is to establish house procedures on how to respond and escalate based on the alerts. This is part of the overall security policy for any organization.

7.2 E-mail Alerts

E-mail based alerts are useful alarms for system administrator's. Since the firewall should be located in a secure facility, such as a telecom closet, e-mail driven alerts are helpful in keeping

touch with the firewall. In addition, some administrator's keep a second management GUI running on their own workstation, so they may connect to the firewall and evaluate the alerts that they receive by e-mail.

7.3 Modem Required Alerts

For security reasons, Intermedia will not provide a modem with its standard hardware configuration. The preferred method of performing paging is by an email assisted paging service.

7.4 Audio Alarms

Audio alarms typically are based on .wav or .au file types. These sounds are played to notify system administrators that a alert has been logged on the firewall. The integration technician will test the standard sound capabilities of both the machine and the firewall as part of the Intermedia Acceptance Test even if audio alarms are not used as part of the initial configuration.

The integration technician will demonstrate the configuration of notifications using the Firewall's Graphical User Interface (GUI).

8. The Intermedia Acceptance Test & Data Backup

8.1 Acceptance Test

Intermedia designed the Acceptance Test to be fundamental to the satisfaction of customers. This document establishes the configuration and measures the success of a typical firewall implementation. It is also Intermedia's written method of delivering confirmation that a customer's firewall is operational. Billing process are initiated upon receipt of the Acceptance Test.

8.2 Data Backup

At the time of installation, a backup copy of the customer's firewall configuration using a floppy disk is generated. This disk is sent to Intermedia where Customer Service stores it. This provides an off-site copy of the original configuration in case of catastrophic damage to the firewall system.

9. Summary of Turnkey Firewall Service

Figure 9.1: Summary of Components & Responsibilities

COMPONENT DESCRIPTION	INTERMEDIA PROVIDES	CUSTOMER PROVIDES
Hardware	Procurement of all hardware according to the documented specification, installation of RAM and other hardware components	Customer Provides all network hubs or bridges. A Hub before and after the firewall is recommended
Software	Procurement and installs og all Operating System (OS) Software, Firewall Software and any required Vendor or Manufacturer Patches recommended at the time of Installation.	No Customer Prerequisite
Security Policy Pre-Installation Evaluation	Intermedia provides a dedicated Installation Coordinator to facilitate the collection of information about the customer's network and security policy. They deliver standard documents and follow standard processes to maintain quality of installation and integration	Customer responds to the requests of their Installation Coordinator by returning 3 key documents: ☛ Customer Network Map ☛ Pre-Installation Questionnaire Front-End Consulting Products are available to assist customers with data collection
Network Address Translation	Intermedia configures Network Address Translation using the standard mechanisms included in the firewall software	Customer provides Intermedia with any special NAT needs prior to installation.
Renumbering of IP Addresses	In most cases, Intermedia configures NAT to eliminate the need for customer renumbering of clients. If renumbering is required, Intermedia only renumbers the firewall and its configuration. Intermedia is glad to assist the customer decide upon a renumbering strategy.	If needed, Customer renumbers all of internal routers and/or internal client systems & servers. Customer provides Intermedia with their IP Address scheme as part of their network map.
Network Routing	Intermedia provides configuration of firewall routing components. Based on the Network Map or Site Assessment data, Intermedia will recommend routing changes.	Customer configures LAN routers and/or clients to use the firewall as the default router
E-Mail Communications	Intermedia changes MX record from current e-mail system to firewall for proxy purposes. See section 4.0	No Customer Prerequisite
DNS (If changing to DIGEX Connectivity)	Intermedia provides a standard process outlined in section 3.1.3. Example wording is available.	Customer documents approval of DNS Authority change to Intermedia from former provider. Customer identifies all internal DSN servers or other naming services on the Network Map.
Virtual Private Networking (VPN)	Point-to-Point: Establishment of Homogenous VPNs between the same Firewalls. Custom Configurations must be priced and scoped on a case-by-case Basis.	No Customer Prerequisite

	Remote Access: The Installation technician will demonstrate the firewall configuration setup procedures for activating of SecuRemote or Raptor Mobile accounts as well as the client software setup. The demonstration is limited to no more than 2 clients.	Customer provides Laptop or Workstation for the VPN Client Demonstration.
Authorization	Review of acceptance test and consults with customer on the day of integration to establish access controls for inbound and outbound communications to the Internet. Intermedia enforces the customer provided security policy via the firewall software.	Customer communicates the services, applications and data allowed to pass through the firewall to and from the Internet. Intermedia assists the customer based on the data provided in the Pre-Installation Questionnaire and on the day of Installation.
Alerts & Notifications	Configuration of e-mail and audio alerts	No Customer Prerequisite
Data Backup Service	Intermedia provides a complete backup of all Firewall Configuration Files on the date of integration.	No Customer Prerequisite
Authentication	Intermedia demonstrates/configures user and group accounts using the firewall GUI. Intermedia also provides integration with Vendor Supported Authentication Servers as long as they are fully functional and operational. The Installation Technician will demonstrate authentication account setup on the firewall to the customer's satisfaction with limited support for user specific data; See Section 6.1.2	Customer identifies all Authentication Servers on the Network Map. (Needed only when the customer desires inbound access for partners or mobile workers etc..)
Acceptance Test	Quality Assurance (QA) through a standard script of operations to confirm a firewall's operational state.	Customer must be present for the testing of network components, connectivity and access controls.