1

Screening External Access Link (SEAL) Introductory Guide

***seal** n [ME seel, fr. OF, fr. L sigillum seal, fr. dim. of signum sig] n,seal 1a: something that confirms, ratifies, or makes secure : GUARANTEE, ASSURANCE ... 2a: something that secures (as a wax seal on a document) 2b: a closure that must be broken to be opened and that thus reveals tampering ...*

What is the Screening External Access Link?

The Screening External Access Link (henceforth referred to as “SEAL”) is a system of computer hardware and software configured to provide a highly serviceable link between a private network and an internet or another network that is not necessarily trusted. The systems which comprise the SEAL work together to provide as high a degree of security as is possible, while still providing high quality access to internet services such as electronic mail. The SEAL actually consists of three systems, known respectively as **gatekeeper**, **gate**, and **mailgate**. The role of each of the three machines is summarized briefly as follows:

Gatekeeper: is responsible for providing an external access point for electronic mail, file transfer services, internet domain name service, and other services, as well as hosting protocol gateways that permit users on the internal network to access services on the external network in a secure manner.

Gate: is responsible for implementing screening routing between the internal network and the internet, as well as potentially logging routing related events. Gate can additionally provide time service and limited other services, but generally acts as a "black box" in its role as a screen between the two networks.

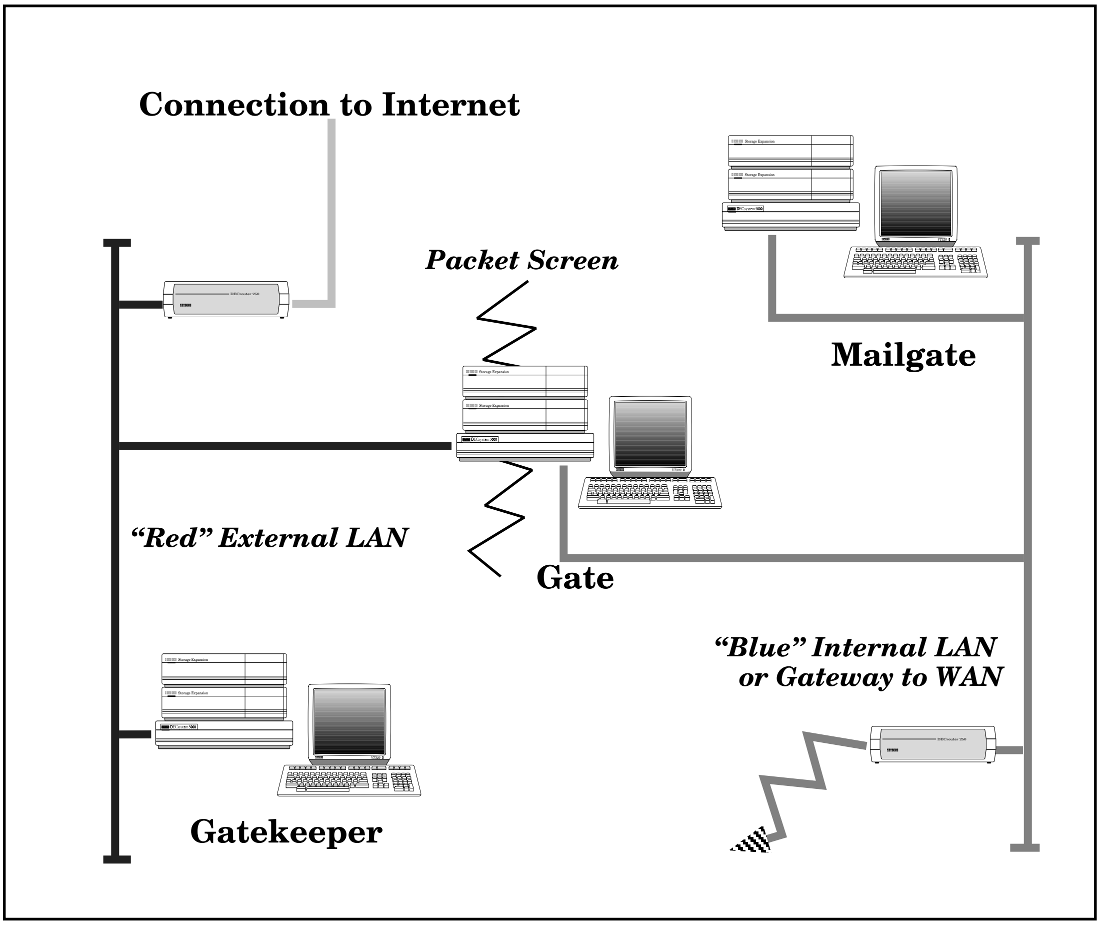
Mailgate: is responsible for acting as an internal mail drop and mail router between TCP/IP SMTP mail and DECnet mail or other mailers as well as a general purpose server for internet domain name service, user accounts, DECnet terminal login, and other services as necessary.

The three machines provide security through several approaches. The most important way in which the SEAL provides security is by completely isolating an external network from the internal network. This is implemented by configuring the SEAL such that no

TCP data from a host on the outside can directly reach a host on the inside. Connections from the outside are only permitted to gatekeeper, which runs a variety of protocol gateways that perform access control and logging, and then in turn pass data to machines on the inside. Connections from internal machines towards the outside operates in the same manner, though typically the site administrator will prefer to relax access controls for internal machines going out while tightly restricting or blocking access for external machines coming in.

Wherever possible, the SEAL makes network access as transparent as possible. Key services such as electronic mail are totally transparent, while file transfer (FTP) and remote terminal access (telnet) require an additional step in connecting to the protocol gateway.

SEAL Schematic and Interconnection Diagram



In this figure, the three computers comprising the SEAL, and the two local networks to which they are connected are represented. The central system is the packet screening router, and acts as the fire-wall between the trusted ("Blue") network and the untrusted ("Red") network. The routers represent generic TCP/IP routers; the one connecting the external network to the internet is typically provided and managed by the network service provider, while the internal one is simply included in the picture for representational value and can be any type of multi- or single protocol router or bridge. The zig-zag line denotes the packet screening software's effect of preventing any unauthorized data from passing between the internal and external networks.

The Packet Screen

The packet screen is a feature of the ULTRIX operating system which permits an application to have administrative veto over every TCP/IP packet that is to be sent through a host running the software. The packet screening software consists of two components: the kernel-based packet screen, and the *screend* process, which is responsible for enforcing the systems administrator's will. As *screend* is started up, it reads a configuration table that explicitly states the types of connections it is to permit or deny. The configuration rules permit exact specification based on whether the connection is TCP or UDP, what port it is originating from, what port it is destined for, originating or destination host, or originating or destination network. Thus it is feasible to specify that a given host can only communicate with another via mail, while still permitting name and time service to work between them. Logging rejected packets is supported, though tremendous amounts of log data may result.

The typical SEAL *screend* configuration is to disable any unspecified traffic ("all that is not expressly permitted is forbidden") and to then permit traffic only between the gatekeeper and any internal hosts. If the site administrator desires to, the list of internal hosts that can communicate with the gatekeeper can be further restricted. This is generally not thought to be necessary, but it's reasonable that there might be a situation in which the administrator would wish to limit access to the gatekeeper to only a specific subnet. Mail would still work, since users on other subnets could send mail via mailgate. The administrator might opt to configure *screend* such that one subnet would have unlimited access to the gatekeeper, while the rest of the internal network could only send and receive mail, and synchronize their system clocks with it.

Application Gateways

Key to the security of the SEAL is the concept of trusted application gateways. An application gateway is a protocol server for a given application, which runs on the gatekeeper machine on the external network. The application gateway is responsible for several crucial tasks:

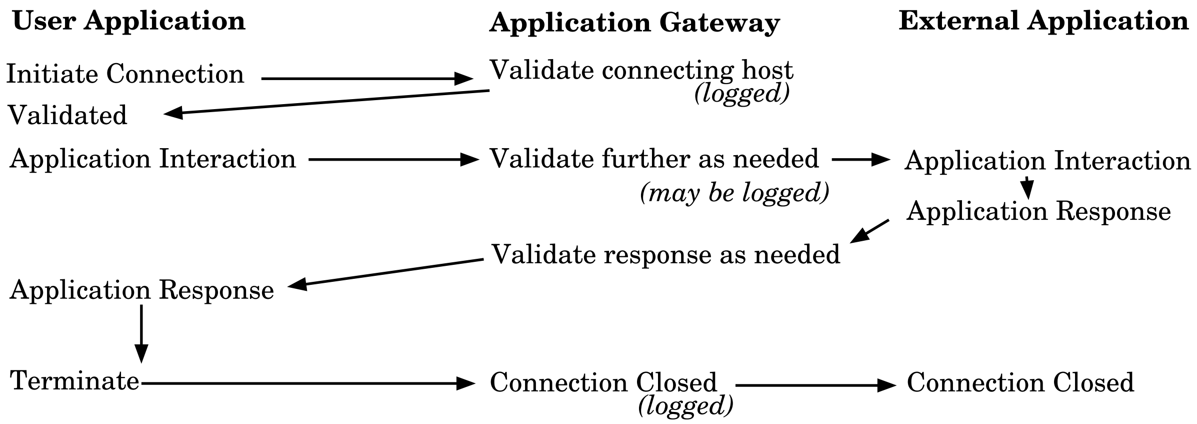
1) Validating the origin of the service request and determining if it should be permitted. This entails checking the originating host of a service request and either denying the service or permitting it based on a site specific policy defined by the administrator. This authorization is completely tailorable, and can permit (for example) the telnet protocol gateway to be limited to only a small number of hosts on the internal network.

2) Validating the protocol as necessary. In some protocols, such as remote terminal protocols like telnet, this is not necessary, but in a more complex protocol such as file transfer (FTP) it is important to actually examine the commands passing through the protocol gateway, to ensure that they are valid and cannot possibly represent a threat. In some cases such as FTP, the protocol gateway can then "know" enough about to the protocol to selectively enable or disable parts of the protocol. A common usage would be to disable the ability of users to execute shell commands over the FTP connection, or to deny users the ability to export data from the internal network to the external network.

3) Additional authorization as deemed desirable. In the case of a telnet protocol gateway, it is desirable to be able to restrict the hosts that can be destinations as well as the hosts that can access the service. Thus, the administrator can selectively specify hosts or networks that can communicate with each other to a high degree of precision.

4) Audit trail. Each protocol gateway can implement appropriate logging.

Data Flow Through Application Gateway



Forcing all transmissions to pass through the application gateway initially appears to pose a performance problem. In practice, however, the performance of the SEAL is bounded by the network connection to the internet, and since all the application gateway traffic is directly between the user and the internet only a few milliseconds are added to each operation through the gateway. For normal usage this is unnoticeable yet provides the highest possible security.

Audit Trail

The existence of an audit trail is vital for maintaining a secure system, as well as for justifying the existence of the system through usage statistics. SEAL uses a special version of the system log management utility (*syslogd*) which maintains duplicate copies of selected system log information in multiple locations on the network. System log information can be automatically sent to a hardcopy log if desired. SEAL is configured to monitor itself as much as possible, automatically searching logs daily for “interesting” patterns and mailing them to the systems administrator for evaluation. Storing the logs on multiple hosts makes it very difficult for an intruder to completely clean up all “footprints” in the event that they succeed in penetrating one of the SEAL hosts.

Every significant event that occurs on the SEAL is logged, including connection via FTP, connections over the network, repeated login failures, mail transactions, and use of the application gateways. At the administrator’s discretion, system logs can be saved for several weeks for reference if needed. Sites with an archival system may opt to never delete log information.

User Management

Users typically represent the largest security risk to an internet machine. Failure to choose “hard-to-guess” passwords and similar mistakes permit the majority of breakins. Since the SEAL uses application gateways and the notion of a “trusted” machine on the external network, there is no need to worry about managing general user accounts on the external system. Since the gatekeeper machine provides several crucial services (electronic mail and name service) that should not be spoofable or interruptable, it is best to minimize the risks by keeping users off the gatekeeper host entirely. The SEAL configuration, however, is extremely flexible, since there is no limit to the number and type of hosts on the external network. A second host can be placed on the external network with user accounts and a high degree of security, and the packet screen can be configured such that connections between the external “user account host” and internal hosts is greatly limited. The user account host can be accessed from an internal host over some one-way medium such as a LAT terminal server, so that connections cannot be originated from the exterior to the interior.

Network Access

Since the gatekeeper and gate machines are the only two hosts on the network that are "visible" from the outside, their security is of paramount importance. It is reasonable to assume that the systems are physically secured, and to assume that all attacks on the system will have to originate over the network. To secure against network attack, the gatekeeper and gate hosts both have software that allows the systems administrator to specify what hosts are trusted to perform what types of connection. Usually, SEAL systems disable telnet and remote login access from hosts that are not part of the internal network. This can be restricted still further as needed, so that the gatekeeper and gate systems will only accept login attempts from a list of trusted internal hosts. Thus, in order to log in to gatekeeper or gate, an attacker would have to be on the internal network already, *and* to know a login and password on the gatekeeper.

The network access software permits controlling access on arbitrary TCP-based services other than just login. For example, *finger* requests can be restricted only to a specific list of hosts, or to internal-only hosts. In this manner, users on the internal network can be allowed to *finger* users on the internet at large, but the privilege is not reciprocated.

Electronic Mail

One of the most important services the internet provides is electronic mail. SEAL is designed to transparently support internet-style electronic mail, with the ability to gateway mail to VAX MAIL and other SMTP-based mailers. SEAL uses the standard UNIX sendmail mail-routing agent and can be used in conjunction with the name service to provide transparent access between internal VAXMAIL nodes using a mail-exchanger record.

Electronic mail arrives from the external network at the gatekeeper machine, which examines the destination address. If the mail is destined for another host on the external network, it is forwarded directly on its way. If the mail is destined for a host running TCP/IP and SMTP-based mail on the internal network, the mail is delivered directly from the gatekeeper to the internal host. Mail destined for other types of mail systems, such as DECnet based mail is forwarded to the internal mailgate host, which can be configured to run DECnet or other protocols.

Electronic mail leaving the internal network follows the same route in reverse. DECnet mail is sent to the mailgate host (usually named with a mnemonic like "**INET::**") which examines the destination address and forwards it appropriately. If the destination is an internal TCP/IP and SMTP-based system, it will forward the mail directly, thereby acting as an internal DECnet to TCP/IP mail gateway. If the destination is outside of the internal network, the mail is transferred to the gatekeeper, which then delivers it. Outgoing mail for networks like BITNET or the UUCP networks can be forwarded by the gatekeeper to specific BITNET or UUCP gateways. Each delivery transaction on the gatekeeper or mailgate is logged.

SEAL is a highly configurable and reliable mail gateway, providing transparent service with the maximum amount of security. Security is enhanced further by the fact that internal-only mail *never* leaves the internal network; only mail that is inbound or outbound goes through the gateway. SEAL also acts as a central email locus of authority, so that mail aliases and mailing lists can be defined and maintained on the mailgate system. This can be very convenient as a mechanism for providing transparent mailboxes for individual users or groups of users.

Other Services

SEAL can support a large variety of other services as needed. USENET news is a typical application that users might want to run on the gatekeeper system, or the mailgate system using an application gateway to permit an external news server to send articles to the internal news server. This permits access to news with a maximum of security, and minimizes the risk of external users accessing internal news groups, by keeping the news articles on the internal network. Accessing the news at the internal mailgate system is a more efficient use of network bandwidth and can also permit DECnet users to access news directly.

Many sites support guest, or anonymous file transfer directories as a means of large-scale distribution of public files. The gatekeeper machine is an excellent place to support anonymous FTP, since it can be reached from both internal and external machines. By combining NFS-shared file systems between the gate and mailgate systems, combinations of read-only file systems or internally-visible-only file systems can be presented.

Since the SEAL hosts effectively straddle two networks, they are an ideal location for supporting services such as X.400 mail routers, network time service, and other services as needed. Network time service is typically configured on the SEAL, with the three hosts acting as peers to keep each other accurate, getting their time from satellite clocks on the network. Internal hosts can then set their time based on the SEAL machines clocks.

Security Risks of SEAL

Computer security is a matter of degree, and SEAL provides a high degree of security, while permitting service to be as transparent as possible. An attack against a network can be considered in terms of increasing domains of threat. Once a system is penetrated, it often opens toeholds into other systems, until eventually it is no longer possible to even quantify the level of risk an arbitrary system on the network faces. SEAL can be considered in terms of its initial vulnerabilities: gatekeeper and gate. Only these two systems are visible to the outside world, and of the two, gate can be eliminated completely as a possible initial point-of-attack, since it does not accept logins over the network from any hosts on the outside network. Gate runs no services that can give an attacker a login or a shell. Gatekeeper is somewhat more at risk, but the risk is limited to only the services the administrator wishes to configure. Typically, gatekeeper will also not permit logins from any untrusted host, and since there will only be administrative accounts on the system, one can at least hope they will choose complex passwords.

In the worst case, if a break-in occurs on gatekeeper, the attacker still cannot change the configuration of the packet screen, but does gain access to attempt to connect to any internal hosts that gatekeeper is allowed to talk to. While this would be a serious problem, it's not considered likely. There would be a good chance that the systems administrator could recover a lot of information about the attack from the system logs.

Internet sites that are not running SEAL typically enforce security through one of several methods:

None. This means that either all systems are at risk, or all systems run in a highly secure configuration. The former is unadvisable, and the latter impacts the usability of the systems, often to an unacceptable degree.

Single Host, Dual Ethers. A single host is put in place and has one interface on the internet, and the other on the internal network. TCP/IP gateway forwarding is disabled, so it acts somewhat like a packet screen with all filtering prohibited. The problem with this approach is that if the system is penetrated, and the attacker can gain systems management privileges, the TCP/IP gateway forwarding can be enabled, and suddenly the internal network is totally open to anyone on the internet, and there is no way of telling that this access has been enabled until someone happens to notice.

Commercial Routers with Screening. Commercial routers can implement something similar to the packet filter, but do not permit the kinds of security SEAL provides with its trusted application gateways. Routers can filter packets based on destination and port, but cannot do the level of fine-grained access control of the application gateways, and cannot support logging.

SEAL provides a high level of security while being as transparent to users as possible. The SEAL configuration is built on top of UNIX, so it presents no extra management burden and will integrate easily with existing UNIX networks. Digital supports a mailing list of SEAL systems managers that consists of both customers and Digital's own gateway managers, where relevant topics and concerns can be discussed.