

The most secured gateway, based on:

ShuttleIT & SelectorIT

Background

The need to connect organization's secured network to the external network is quite common in today's interoperable era – from email connection to the world, files transfer, files updates downloads (e.g. anti-virus updates), organization's internet site uploads for updates, supplier and customers, etc.

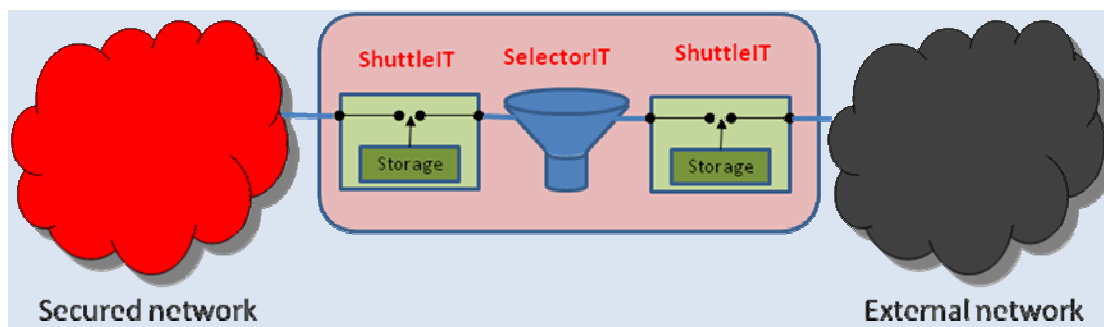
However, strict security policy eliminates direct connection between the networks.

Therefore, manual work is usually required in order to check and filter incoming files from viruses and malicious files, as well as manual censoring of outgoing files to prevent sensitive data leakage.

This results in time consuming and delayed activity, which is often not complete (hidden data not detected for example) and not effective (anti-virus update is too late).

YazamTech co. developed the advanced and most secure gateway, based on two main components:

- **ShuttleIT** - H/W based and S/W controlled solution (US Patent Pending) that enables information transfer between IT networks which are forbidden from being physically connected to each other. Automatic and secure information transfer system between isolated IT networks
- **SelectorIT** - A family of professional software tools configured to permit, block and sanitizes of files transference by different users, based upon a set of rules and other criteria. It checks certain kinds of files (structure and content), and can detect whether an unwanted structure or content is trying to move between the trusted and untrustworthy zones.



Typical ShuttleIT & SelectorIT customers include: banks, insurance companies, health organizations, military and national security, government and any other organization which is interested to compartmentalize their sensitive IT networks and secured information.

ShuttleIT

ShuttleIT is an innovative H/W based and S/W controlled solution (US Patent Pending) that enables information transfer between IT networks which are forbidden from being physically connected to each other. So far, in order to transfer digital information to and from their sensitive IT networks; organizations manually use Flash Memory, CDs or any other portable media. ShuttleIT provides continuous 24/7, automatic and controlled digital information transfer while being secure from any potential attacker.

Main Capabilities

- Full control over the transferred information.
- *ShuttleIT* Transfers any type of information which does not require On-Line connection between the sending and the receiving PCs.
- At any system switch, as many as several bytes to hundreds of GB and more can be transferred in unique session.
- *ShuttleIT* neutralizes external attack threats by using USB communication, compared to unsecured communication lines such as TCP/IP.
- *ShuttleIT* enables unidirectional or bidirectional digital information transfer.
- Easy installation - no need for special preparations.



Your Challenge

As a compartmentalized LAN user in your organization, you are obligated for a strict information security policy; you are probably disconnected from any direct digital communication with the external environment especially from the Internet.

In this case, you are limited when it comes to free and continuous delivery/reception of emails to and from your personal desktop as well as download/upload files to/from the Internet, FTP or simply transferring digital files to and from the other organizational LANs.

In order to fulfill those requirements while maintaining the strict organizational security policy, you are probably required to verify that the information you wish to transfer-in does not contain any security threat that may threaten the compartmentalized LAN, or from the other hand, verify that the information you wish to transfer-out of that LAN does not contain any sensitive information that may 'Leak' out of the organization.

You probably use manual means such as portable media (Flash Memory, CDs) in order to transfer that information, a process which consumes precious time and efforts.

Our Solution

ShuttleIT was developed in order to execute an H/W based system that enables secure information transfer to and from a compartmentalized environment while maintaining a full physical separation between several LANs. *ShuttleIT* protects those compartmentalized LANs from external attacks sourced from the other LANs and it provides those compartmentalized LANs protection from sensitive information 'Leakage' as well.

How does it work?

ShuttleIT implementation is quick and easy. The system is located between the compartmentalized LAN and the other organizational LANs while being connected from both sides using standard USB cables.

The *ShuttleIT* control software is installed twice: on the compartmentalized LAN and on the other LAN, it contains a user friendly GUI which presents the system's status and the information which is being transferred. The control software was developed using Microsoft .NET™ and it is deployed in Client-Server formation, so the system can be remotely controlled.

The control software organizes the information which is about to be transferred as well as the information which is received on the other side. The control software orders the system for a switch operation with the internal storage unit, while assuring that at any given time, there will be no direct physical connection between the two LANs.

The system provides unidirectional or bi-directional transfer mode. As the transfer mode is set on the H/W itself, it cannot be bypassed or controlled by any potential external attacker.

ShuttleIT can be synchronized to automatically transfer the information between the source and destination PCs based on 24/7 operation according to pre-defined parameters such as immediately as information is accepted by the source PC, or by predefined time schedule.

As the control software calls the *ShuttleIT* internal storage unit to connect to one of the LANs that is interested to upload information, the *ShuttleIT* physical switches connect to that LAN, upload the requested information into the *ShuttleIT* internal storage, disconnect from the source LAN, then connect and download the information from the *ShuttleIT* internal storage to the destination LAN. Once the information was successfully downloaded in the destination LAN, the system enables an automatic execution of commands supplied by the customer in order to immediately benefit from the information that was just downloaded. For example: Auto-run an Anti-Virus update that was just downloaded from the internet.



YazamTech

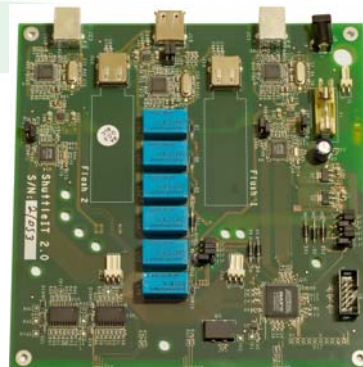


33 Arlozorov st. Raanana, 43607, Israel | **Cell:** +972 54 4326621 **Fax:** +972 9 7439326

www.YazamTech.com | info@YazamTech.com

ShuttleIT Single Board

This *ShuttleIT* model contains a single cover and a single switch board; it enables a secured information transfer between two LAN networks that have no physical connection between each other.



ShuttleIT Double Board

ShuttleIT customers who are interested to control and scan the transferred information use this *ShuttleIT* model.

ShuttleIT Double Board model contains two switch boards that actually create a 'Sterile' zone between each other, in this zone the customer operates content filtering systems such as: Anti-Virus, Content Filter and Content Checker.

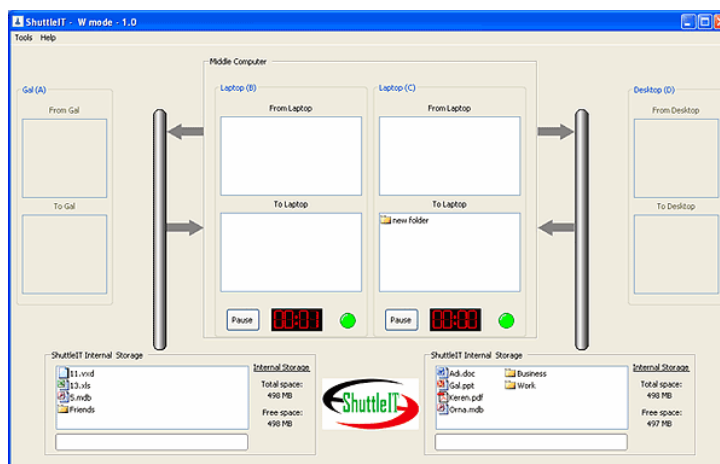
Thanks to *ShuttleIT* Double Board, the creation of such 'Sterile' zone enables the customer from one hand to filter the transferred information in a location where it is not accessible to potential external attackers and from the other hand it is done safely away from the sensitive environment that it was required to protect.

Compared to *ShuttleIT*, existing content filtering systems available today, usually operate in the Gateway and within the internal LAN itself (Main Server and the end points).

This fact places 2 major security disadvantages: 1) It exposes those systems to potential external attackers who may want to neutralize them in order to access the sensitive information 2) When those systems operate within the internal LAN, once again they may get exposed to potential external attackers and the way to access the sensitive information is short.

Other Advantages

- Significant reduction of external attacks and information 'Leakage' threats.
- Reduction of human errors.
- Enables various uses that were forbidden so far or that there was concern to use them following the lack of a technological solution.
- Saving expensive human resources and other resources while significantly increasing the interior organizational productivity.



SelectorIT

The *SelectorIT* is a family of professional software tools configured to permit, block and sanitize file transference by different users, based upon a set of rules and other criteria.

Typical examples are:

- Receiving untrustworthy files (e.g. infected files by virus/malware) from the Internet which is an untrusted zone, to be used by users in an internal network which is a zone of higher trust.
- Transferring sensitive files (e.g. files contain classified information) from the internal network which is a zone with high trust, to use by external users which are located in a zone of lower trust.

SelectorIT is based on a "default-deny" ruleset, in which only files which are accepted are the ones that have been explicitly allowed.

In the developing process of the *SelectorIT*, a team of experts in data security integrates detailed understanding in file vulnerabilities, while to operate the *SelectorIT* the security administrator needs to configure its operation by set of rules.

The key benefit of *SelectorIT* is that it can "understand" certain kinds of files (structure and content), and can detect whether an unwanted structure or content is trying to move between the trusted and untrustworthy zones.



***SelectorIT* managing**

The administrator (*admin*) is the manager of the engine. The *admin* determines which rules and parameters to activate. The engine is provided by the developer with pre determined default parameters while the *admin* could harden or weaken the default configuration.

The *admin* must maintain the principle of "default-deny" *SelectorIT* ruleset, in which the only files which are allowed are those that have been explicitly allowed.

***SelectorIT* console**

The *console* is the tool that presents the information collected in the logs. The *console* screen show any information required about both the block files and the allowed files.

The *console* is the place to locate the ability to release blocked files if the chief security officer believes that there isn't a real reason to block a specific file that is block by the *SelectorIT* engine.

SelectorIT Engine

The *engine* of *SelectorIT* is the heart of his operation. It contains the knowledge base and the security rules.

The *engine* has a wide range of embedded abilities, which are updated continuously by the developers.

There are some general searching abilities achieved by deep content inspection functionality by the *SelectorIT engine*, e.g.:

- Determine which directories will serve as:
 - Source directories to receive from the pre checked files.
 - Target directories to allocate allowed files after successful checking.
 - Quarantine directory to allocate blocked files that failed the checking.
 - Log directory to locate the log files with the results.
- Determine the allowed file types, by checking the "magic bytes" (the first couple of bytes in a file) and not only the extensions of the files.
- Forbidden words in the file, using wildcards and regular-expressions.
- "Must Appear" words in the file, using wildcards and regular-expressions.

There are dedicated fields for searching in each file. Here are some examples:

- In Office family files: searching in: header, footer, notes, foot notes, track changes (reviewing) etc.
- In E-mail family files: searching the sender address, the sender domain, the recipients address, the recipient's domains, and the subject of the E-mail.
- In xml family files: searching in the names and values of fields.
- In html family files: searching in links, sources, comments, scripts, tags.

There are some actions could be performed by the *SelectorIT engine*, e.g.:

- Blocking files that are too large.
- Blocking transference of files during "not allowed time of the day".
- Blocking files not compatible to a reference schema.
- Cleaning slacks from allowed files.
- Cleaning/blocking infected files by viruses, worms, malwares etc.

The searching for forbidden information inside the files must include also the hidden areas which are invisible to regular computer user. The searching areas include:

- The file body.
- The metadata.
- The hidden-data.
- The file properties, including: title, subject, category, keyword, comments, author, application name, company, date created, date last save, edit time etc.
- The file name.



To succeed in its operation, the *SelectorIT engine* can:

- Block encrypted files, if it hasn't the ability to decrypt them.
- Search inside compressed files, and block those files which are locked by a password.

SelectorIT Gateway

Function

A *SelectorIT-Gateway* is located between networks/computers, where it could controls files transference to and from a trusted network/computer, respectively from and to untrustworthy network/computer, permitting or denying file transference based on a security policy.

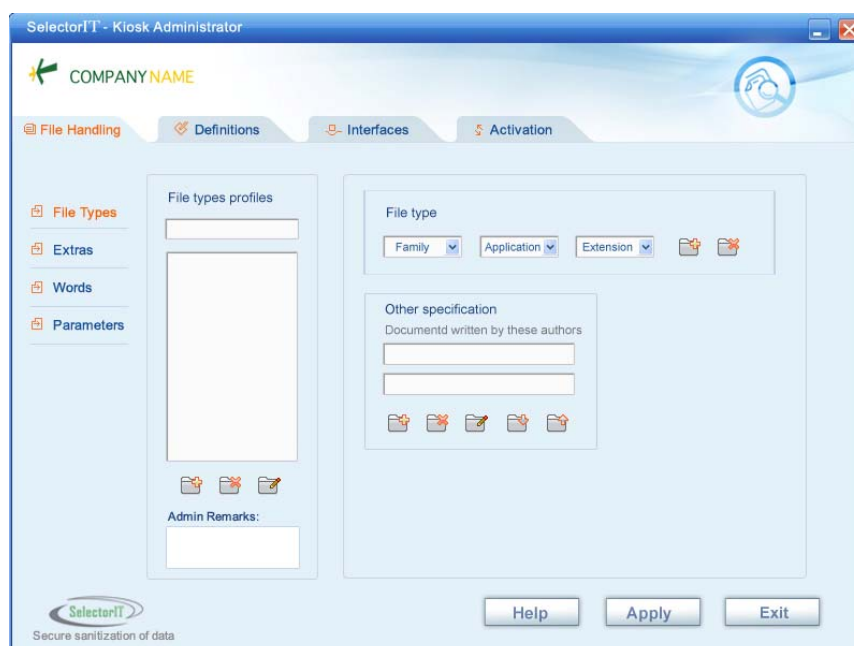
The *SelectorIT-Gateway* works automatically continuously in the *gateway*. As it is based on software it operates continuously as a service.

The user who requires the *SelectorIT* services doesn't have permission to change/update/adapt the security policy according his transference of files. The security policy to the *SelectorIT-Gateway* is determined by the administrator.

Features

Common *SelectorIT-Gateway* features:

- Allows the user to control which files will be checked by the *SelectorIT-Gateway*.
- Could alert the user about blocking incoming and/or outgoing files.
- Could provide the user with detailed information about each blocked file.



YazamTech



SelectorIT-Kiosk

Function

A *SelectorIT-Kiosk* is a station which controls file transference to and from a trusted network/computer, permitting or denying file transference is based on a security policy.

One of the most popular usages of the *SelectorIT-Kiosk* is to import and export files by removable media, to and from trusted network/computer respectively.

SelectorIT-Kiosks are typically designed for use by end-users, while the *SelectorIT-Gateway* is operating automatically continuously.

The *SelectorIT-Kiosk* is based on the same engine as the *SelectorIT-Gateway*,

In the *SelectorIT-Kiosk* the operator doesn't have permission to change/update/adapt the security policy according his transference of files. The security policy to the *SelectorIT-Kiosk* is determined by the administrator, as in the *SelectorIT-Gateway*.

Features

Common *SelectorIT-Kiosk* features:

- Allows the user to control from which device the files will be taken to the checking and in which device to save the allowed files after the checking.
- Allows the user to control which files will be checked by the *SelectorIT-Kiosk*.
- Alerts the user about blocking of incoming and/or outgoing files.
- Provides the user with detailed information about each blocked file.

