Listenless Unhackable Servers

What cant’t be accessed, cant be hacked

SMARTFIREWALL REFLECTOR

What is of supreme importance in { **Cyber }** war is to attack the enemy’s strategy.

Sun Tzu - Art of War

ALL CYBERATTACKS HAVE THE SAME OBJECTIVE

100% of all corporate cyberattacks have a single end goal – connect to and steal data or otherwise compromise a secure backend corporate server.

This is called a Cyber “killchain”. Whether it is Malware, Spear Fishing, or Password Theft - All are just different paths to same end goal.

What is the **CYBER KILL CHAIN?**

The cyber kill chain, created by Lookheed Martin, describes the phases or stages of a targeted attack. Each stage presents an opportunity to detect and react to an attack.

THE CORE PROBLEM
DESIGN OF THE TCP/IP PROTOCOL

TCP/IP CAN'T PREVENT HACKING OF DATA

TCP/IP which is the core protocol for all modern network communications was designed in 1972.

The first computer virus was written in 1986 – called The Brain.

The problem is that TCP/IP was designed in an age when cyberattacks were unknown, and consequently has no security built into the core protocol.

TCP/IP requires that any server which needs to provide information, must be listening on an open port which anyone who can access that network, can then connect to. If a server doesn't listen and allow incoming connections, then it can't participate in communications.

Anything which is accessible, is by definition hackable.

What if there was another way? A server which could serve data yet not be open to any incoming connections?

Listenless Servers

Listenless servers are servers which don't listen on any TCP/IP port to the outside world. Servers that don't allow any incoming connection to them at all, while still serving data and information out to the clients.

YOU CAN'T HACK WHAT YOU CAN'T ACCESS!

SmartFirewall Reflection Network is a patented technology created by TekMonks which allows for operating Listenless servers. These Listenless servers are not listening on any external ports, nor accepting any traffic, they are completely isolated, and by definition un-hackable, however by participating in the reflection network, they are still able to serve data to external clients.

Smart Firewall Reflection Network

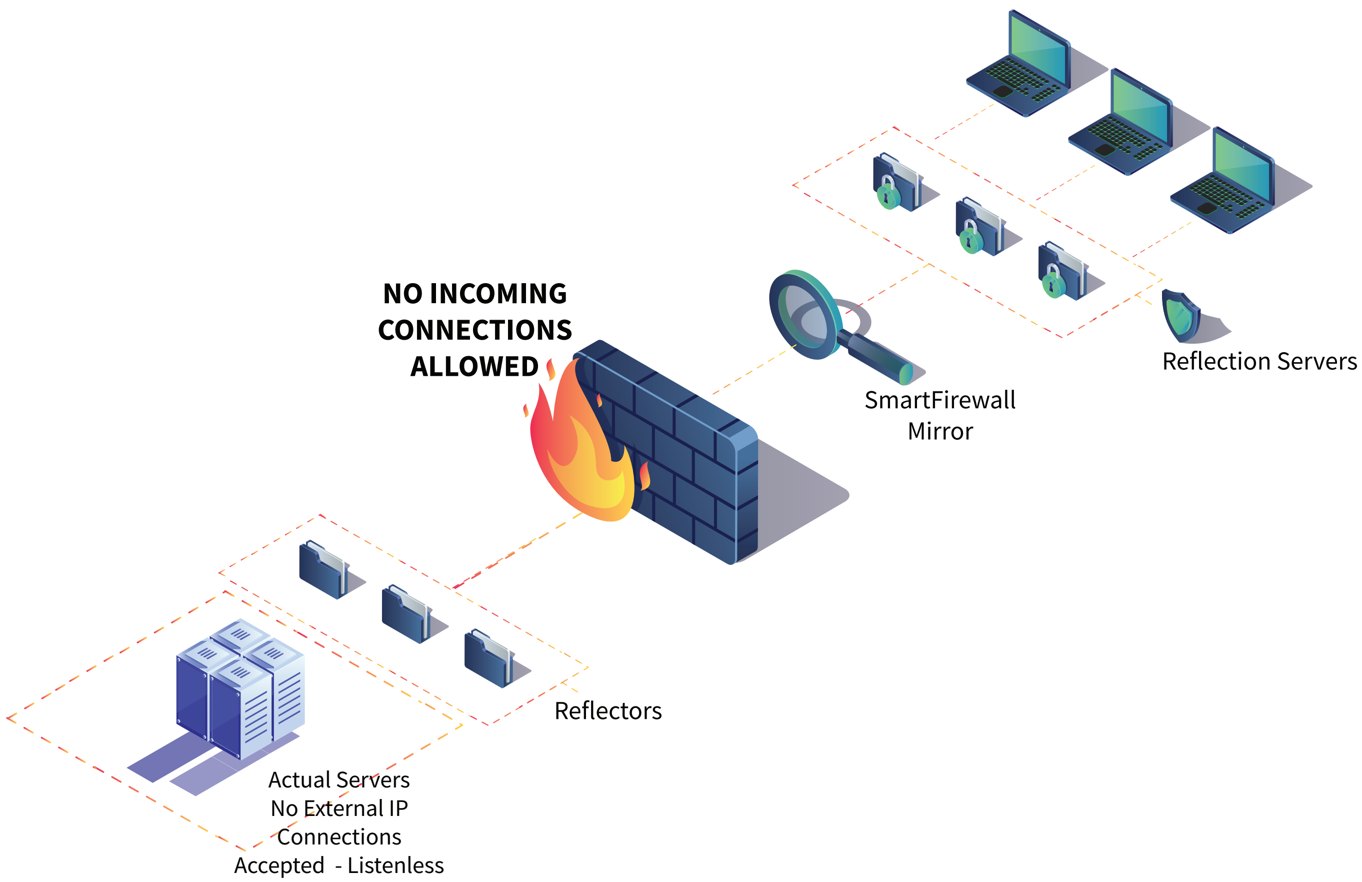
SmartFirewall Reflector is a TCP/IP protocol level reflection-based network. Just as in real life, a mirror image of a person, act and behaves identically to the real person, a SmartFirewall reflection server, acts and behaves just as the actual server.

Reflections Are Inherently Safe

A reflection of a person is not actually that person. If someone tried to touch the reflection, all they will touch is the mirror. If they tried to attack it, actual person will be unharmed.

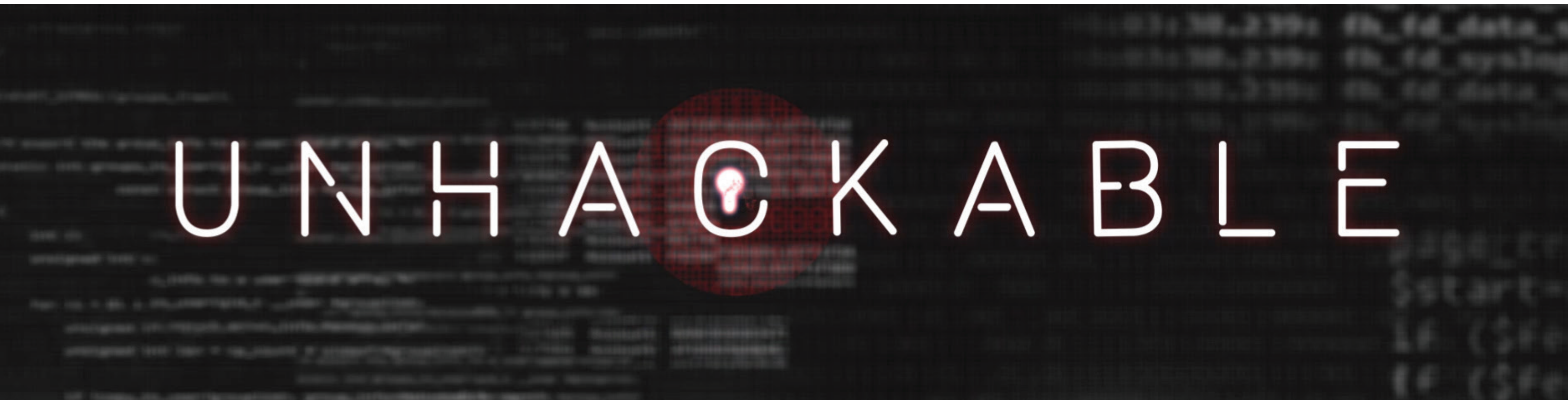
A SmartFirewall Reflection server works the same - for example, it may look like an HTTP server but will contain no real HTML files. It may look like a Database server but will contain no real filesystem with actual data. Anyone who tries a known hack on a reflection server will find it is immune, as it is actually not even running the HTTP or Database or other software.

Reflections can be setup quickly, and are immune to all attacks, as they are not real, they just look and behave as if real.



The Holy Grail of Cybersecurity – Listenless Servers Fixing the TCP/IP Security Issues

With a reflection network in place, reflectors can be setup to reflect any server. The actual server itself will not be connecting to the clients, only the refection will. Therefore, the actual server doesn't need to listen on any ports or allow any incoming connections. It is the reflector which opens an outbound connection to the reflection server. As the external clients connect to the reflection server, it then reuses these pre-existing connections to serve the clients. All communications are AES-256 encrypted. There is no incoming network path from the reflection servers or the clients to the actual servers. Not only does the reflection server contain no real data, it can't even open a path to the actual servers. Unhackable!



Produced/printed in the UK 05/07

IMPORTANT PRIVACY INFORMATION: If you would like to request access to or correction of your details, or if you would prefer you or your organization not to receive further information on TekMonks products and services please contact us at:

privacy@tekmonks.com

TekMonks Ltd.

Kemp House, 152 City Road
London. EC1V 2NX.
UK.