DMZ in a box

iwebgate®

New Weapon in Cyber Security and Business Capability

" Your New Point of Interaction "

Problem

Security check points, corporate reception areas and residential entrances act as a point of demarcation to prevent an intruder from directly accessing areas containing items of value.

When it comes to network setup and security, some government and defense force contractors, professional service firms and small to medium size organizations dealing with sensitive information innocently ignore this same "principle of separation". Incredibly they open and directly link numerous peripheral firewall ports to primary business systems residing on their trusted networks!

Ultimately these organizations conveniently provide both their users and hackers with remote access to an array of primary business services based on the misconception their firewall and/or software is 100% secure. This is a courageous approach to network security especially when:

- Firewalls frequently experience difficulties discriminating authenticated and untrusted users
- Firewalls often have troubles inspecting encrypted packet payloads
- Software vulnerability provides easy hacker penetrations

A disturbing process, taking less than 20 seconds, demonstrates how easy an external intruder can breach firewalls to directly access primary business system like Email, File, Reporting, VOIP, VPN and Terminal Services. Time to crack these services can take milliseconds via known vulnerabilities to weeks using an array of attack vectors.

Compounding the problem, these organizations frequently allow internal users and network services to directly interact with the Internet from within their trusted/corporate network without authentication or filtering services.

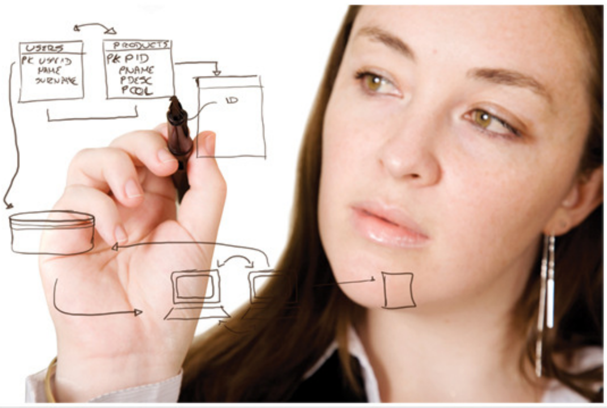
This network setup can have catastrophic results with infected host devices residing on an organization's trusted network. In such a situation, external intruders are equipped with the tools needed to launch a full scale attack on systems, applications and information residing in an organization's trusted network and/or against other remote networks.

Solution

Adhering to the principle of separation to boost defense-in-depth strategies, iWebGate has developed a novel Ghost Network Platform which resides in an organization's Demilitarized Zone (DMZ).

Whilst the perimeter firewall remains as a crucial "front door" security component, the Ghost Network Platform acts as a segregated phantom network which mirrors the trusted network and intelligently supplies all the key services normally provided and located in the trusted network.

iWebGate's Ghost Network Platform removes the technical complexities and costs associated with establishing self-built DMZ services by delivering a commercially available DMZ solution for every small, medium and large organization connected to the Internet.



I can have a secure private cloud?

Opportunities

Importantly the Ghost Network Platform moves the primary "point of interaction" between an organization's trusted network and a volatile public network (e.g. the Internet) into a DMZ protected space. This new point of interaction enables every organization to extract significant value by:

1. Seamlessly establishing "private cloud" solutions
2. Protecting primary business systems, applications and information
3. Transforming business capabilities

For example:

✓ **Say Goodbye to Business-Sapping VPN Services**
Contrary to corporate belief, traditional VPN services (e.g. IPsec, SSL) do not strengthen network security because they inherently extend the private/trusted network and increase an organization's surface attack area. iWebGate's Bridging and VLAN services are designed to resolve this problem and eliminate every day complaints where users struggle with VPN services - especially when working abroad or connecting over slow data, 3G and satellite connections (e.g. too slow, cannot connect, keeps dropping out).

✓ **Private Cloud Reporting Services**
From a single iWebGate platform, in the professional service industry for example, accounting firms can automatically and securely collect information from their clients' data sources residing in remote networks and deliver a range of business intelligence reports (e.g. financial, operational, inventory, assets and carbon assessments).

✓ **Establish Private "Internets"**
Industry, government agencies and defense forces can rapidly establish a private "internet" which leverages off public infrastructure - resulting in extremely secure and efficient communication with networks irrespective of physical location. iWebGate's ability to "layer" a mesh network also enables these groups to securely and efficiently interact in seconds with other networks and devices belonging to contractors, allied defense forces, suppliers and a wide multitude of organizations!