iwebgate

Overview

Delivering the Value of Powerful Networking

... to Everyone

Introduction

iWebGate revolutionizes networking technology for the world. It will have a profound impact on the fabric of security and organizational capabilities everywhere.

Overcoming a series of technical uncertainties and risks, iWebGate has successfully aggregated an array of normally disparate network services in a single platform - *without* using server virtualization technologies!

The consequences of this remarkable breakthrough go far beyond just another security product. This innovation is both disruptive AND transformational technology ("transruptive") that will have a lasting impact on the way we securely and reliably connect with each other ... forever!

One security product:

a) **Introduces the world's first commercially available DMZ Platform**
   - a necessity for every organization publishing network services on the Internet

b) **Can quickly and easily turn IT from a cost base to a profit center**
   - via the ability to establish an infinite array of secure private cloud solutions from existing ICT infrastructure

c) **Introduces the world's first replacement for insecure VPN technologies**
   - securely enabling users to instantly create "private-internets" over the public Internet

d) **Impacts in a systemic and pervasive way throughout both the virtual and physical worlds**
   - Accepting status quo, when it comes to conventional networking, is no longer an option

The President of the United Sates' understands the current security situation. He made the following remarks in May 2009:

> ***"But make no mistake: this world, cyber space, is a world we depend on every single day. So cyber space is real and so are the risks that come with it. In short, America's economic prosperity in the 21st century will depend on cyber security. And this is also a matter of public safety and national security. Indeed, in today's world, acts of terror could come not only from a few extremists in suicide vests but from a few key strokes on the computer - a weapon of mass disruption"***
>
> ***President Barack Obama – May 29, 2009***

Lives put at risk with leaks of military data, millions of dollars stolen when hackers easily obtain customer credit card records and the new face of war where utilities are taken down or threatened at the click of a button are just some examples of how interwoven and reliant physical security is with the virtual world.

Copyright © iWebGate Pty Ltd, 2010. All rights reserved.

In the space of the last nine months senior independent ICT experts, business analysts and venture capitalists have awarded iWebGate for its groundbreaking technology through the judging process in some of the world's more significant security and innovation competitions including (in chronological order):

March, 2010
The Security Network - Security Summit (San Diego)
Award Winner - Information Assurance and Cyber Security

August, 2010
Australian Information Industry Association (AIIA)
National Winner - Best Security Product
(Qualified for APICTA Final in Kuala Lumpur in October, 2010)

September, 2010
Global Security Challenge
Winner - Asia Regional Final
(Qualified for Final in London - November, 2010)

October, 2010
Asia Pacific ICT Association (APICTA)
International Winner - Best of Security

November, 2010
Telstra Innovation Challenge
Winner
(Global Fortune 500 Company)

November, 2010
Global Security Challenge
Winner Worldwide
(US$300,000 TSWG – US Government agency sponsored award)

iWebGate redefines the Internet's future!

Next generation technology, adhering to security principles we use in our physical world (i.e. principle of separation, the whole and interdependence), changes network connectivity, capabilities and security forever.

Best practice security models can now be fulfilled. Outdated industry standards can get ahead of the hacker and other undesirables. Everyone can now play a vital role in creating a new fabric for generations to come.

With the iWebGate Platform there is no trade-off between security and user functionality. Security does not need to be comprised by the explosion in the multitude of technologies and appliances now demanded by users. The market maintains current ICT infrastructure and maximizes investments. This means the market can enhance existing technologies, get the maximum out of legacy systems and yet allow the agility of secure networking to take place.

Copyright © iWebGate Pty Ltd, 2010. All rights reserved.

Contents

Copyright © iWebGate Pty Ltd, 2010. All rights reserved.

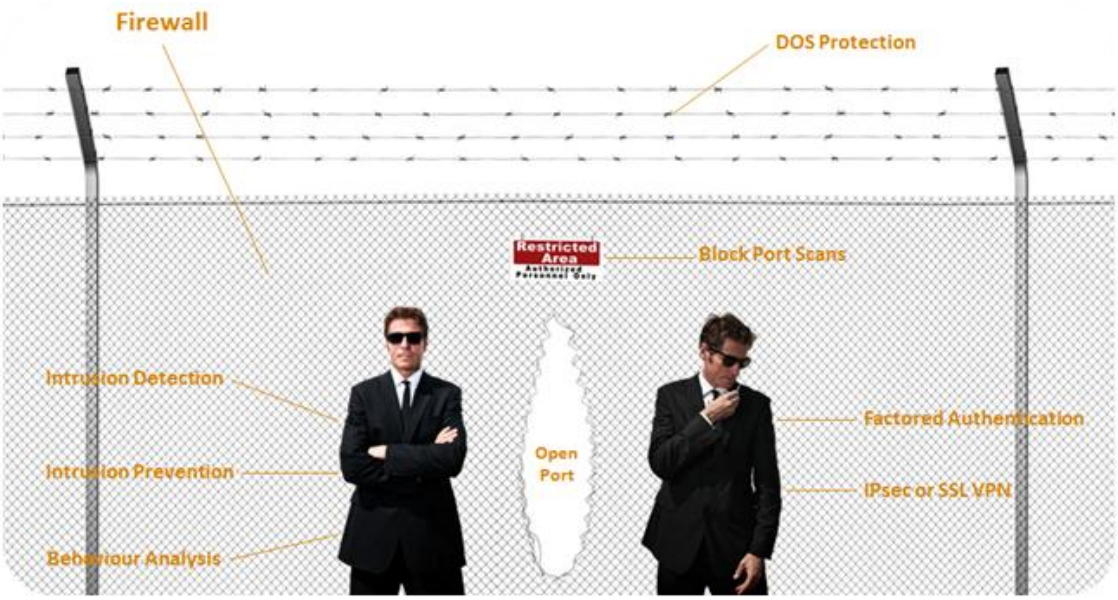
Business Description

Universal Problem

The Internet has made us more interconnected than at any time in human history. Business reliance on the Internet has exploded in the last 12 years - with most organizations rushing to get on it for the lowest cost possible.

The primary product used by most organizations to try and secure their private/trusted networks from the world's most volatile public network is a firewall.

The best way to think of a firewall is to picture a fence. Openings must be available if information/requests are to come in or out. As weaknesses appear and more threats are thrown at the fence, "band aids" are applied to try and boost security.



Firewall Fence

However firewalls have serious weaknesses associated with them, especially when it comes to:

- Zero-day vulnerabilities (i.e. unknown threats)
- Inspecting encrypted packet payloads
- Authenticating trusted users for all network services
- Poor setup and configuration

Incredibly, we find most (>90%) small to medium enterprises (SMEs) adopt this "fence" mentality when publishing network services (e.g. email, ftp, terminal server access) on the Internet.

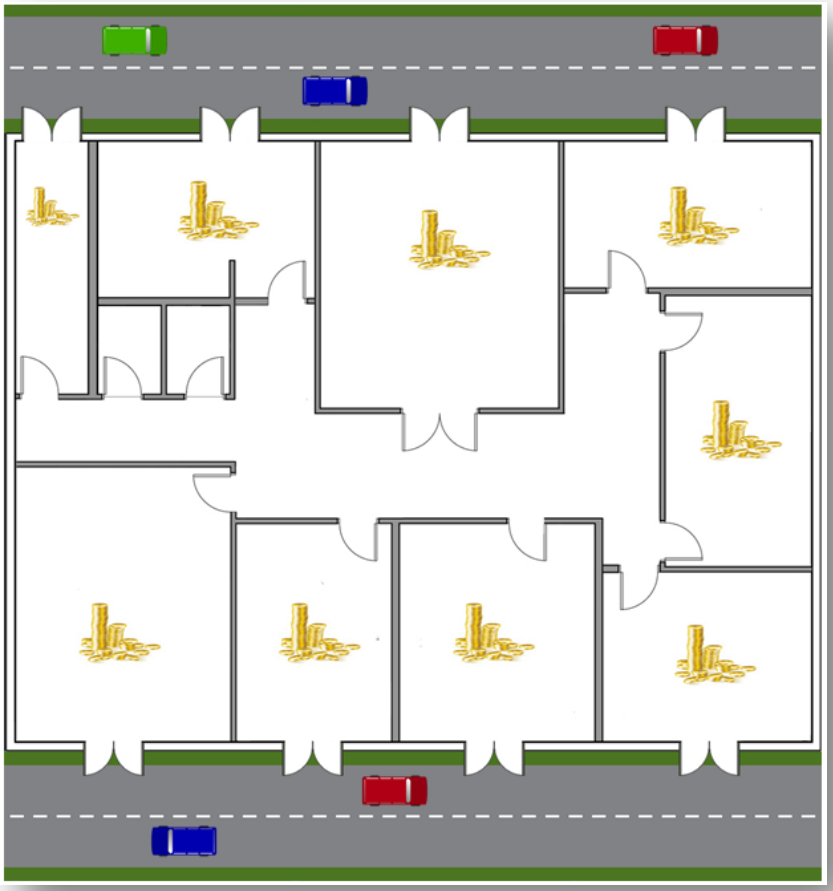
This weakness is quickly and easily exposed during a live demonstration. Management are in complete shock when they see how easy a hacker, located anywhere around the world, can reach their business systems in less than 10 seconds without being detected!

Copyright © iWebGate Pty Ltd, 2010. All rights reserved.

Setting a network up in this manner resembles a corporate office not having a reception area.

Instead, each office has a door permanently opened to the street. In cyberspace, the only commodity being traded is information. Information is power and power is money.

So is it logical to store money in an office which has permanent, unrestricted street access to every room? Never ... so why does everyone accept and do this in cyber space?



The Solution

A 'Demilitarised Zone' (or DMZ for short) is a network space between a trusted network and the Internet. This best practice recommendation makes very good sense because it applies a principle we see every day when protecting valuable items – the principle of separation.

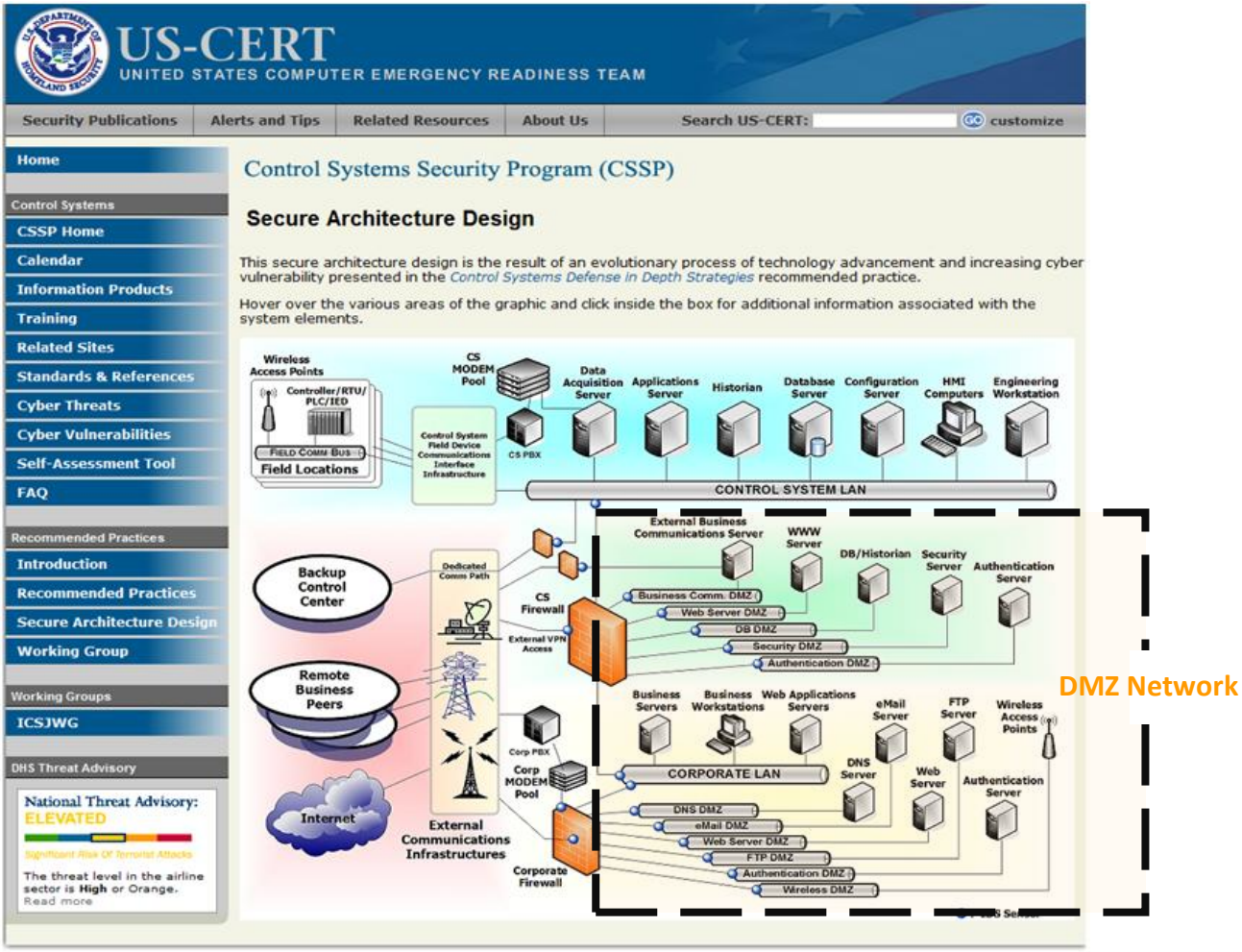
iWebGate introduces the world's first commercially available DMZ network solution ... one platform ... multiple network services ... set up and ready to go in 20 minutes

... AND we introduce Virtual Invisible Networking to the world. It eliminates the need for insecure IPsec and SSL VPN forever.

Copyright © iWebGate Pty Ltd, 2010. All rights reserved.

Problems with Today's Best Practice Recommendations

The United States Department of Homeland Security recommends establishing a secure network zone between an organization's trusted/private network and the Internet as best practice.



US-CERT Secure Architecture Design Model

However, this recommendation demonstrates with a self-built security network the challenges, technical complexities and high costs associated with achieving and maintaining this best practice in an organization's Demilitarized Zone (DMZ).

Reasons associated with the technical challenges and costs include:

- A requirement to essentially double-up on network services
- Networks typically consist of a number of servers with affiliated software
- Uncertainties with getting all network services to work together and seamlessly with network services residing in the trusted/private network without compromising network security, performance and reliability
- Network security is weakened for a self-built DMZ solution the minute Virtual Private Network (VPN) connections are introduced for remote access (i.e. IPsec and SSL) because they increase the surface attack area by "extending" the network to the remote user

Copyright © iWebGate Pty Ltd, 2010. All rights reserved.

The PCI DSS, was developed by the founding payment brands of the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures on a global basis. Only now (Oct, 2010) does the standard mention the need to implement a DMZ network security zone but it doesn't emphasize the requirement to protect all network services.

iWebGate's Technology

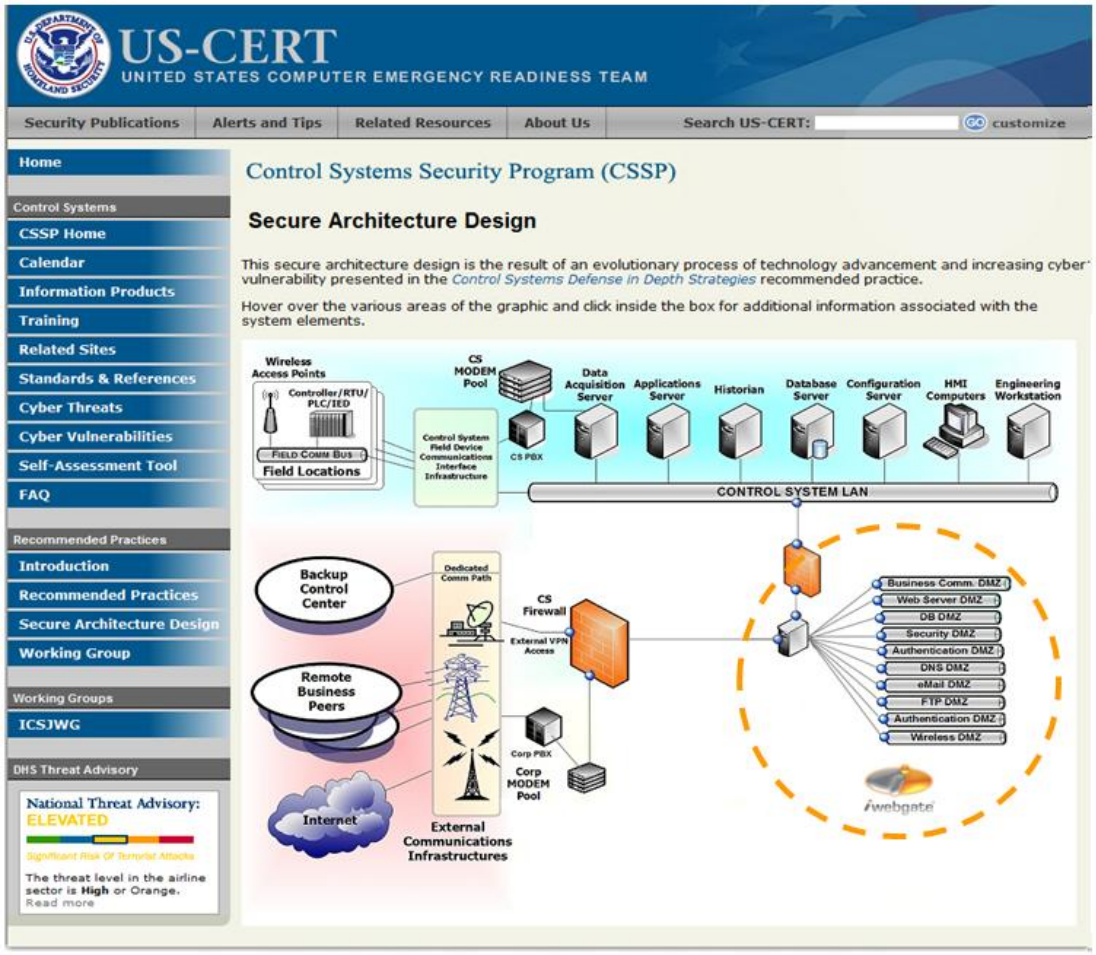
iWebGate originates from the world's most isolated capital city – Perth, Western Australia. Remotely connecting to the office is a must for any organization trying to prosper in one of the world's largest mining, oil and gas regions. Dealing with customer problems in this unique region provided us to with the experience to see things differently and attempt to rectify a universal problem ... the way to operate safely, optimally and reliably on the world's most volatile public network - the Internet.

Transruptive Solution

iWebGate's breakthrough invention is based on principles we see every day when trying to protect valuable items. The principles of

1. Separation
2. The Whole
3. Interdependence

While the existing market practice and knowledge is to install a number of servers in a network, iWebGate's DMZ Platform is a "network in a single server" as portrayed in the following diagram:



iWebGate Secure Architecture Design Model

Copyright © iWebGate Pty Ltd, 2010. All rights reserved.

The world's first commercially available DMZ network solution

After 5 years of research and development (R&D), the Company created a way to securely setup an array of normally disparate network services – each in isolation - on a single Operating System without using server virtualization technologies. Background information to develop the innovation was non-existent or at best unreliable. As a consequence we had to establish a body of original thinking!

Server virtualization technologies could not be used on the basis they:

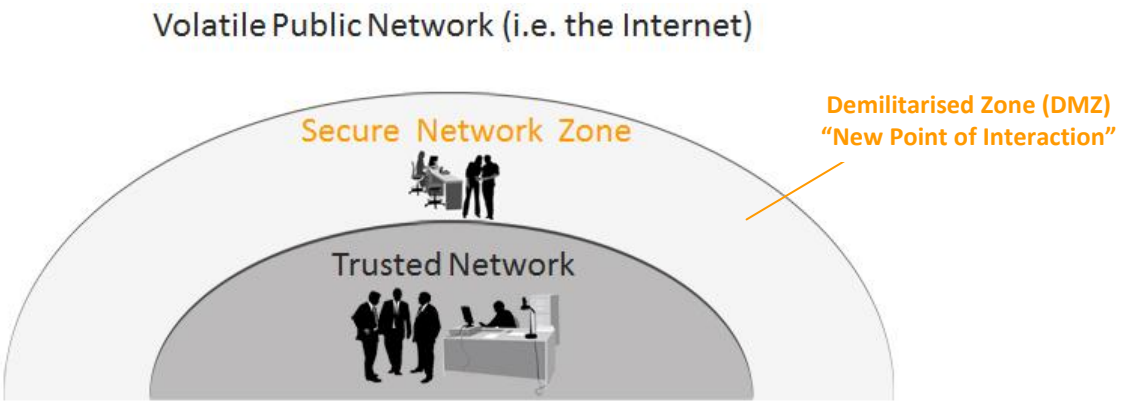
- Require an Operating System to be installed and maintained for each network service in order to maintain a level of distrust between services;
- Significantly increase the complexity and costs associated with the setup and maintenance of the solution;
- Load a burden on already limited hardware resources;
- Might compromise the commercial accessibility of the solution to major sectors of the market; and
- Potentially weaken the security of the network due to;
  - Multiple points of attack on a number of Operating Systems
  - An increased surface attack area provided by the Hypervisor if not properly protected (a risk is eliminated in the best possible way when it's not created in the first place).

For end-users, each of the network services appear to work together seamlessly on one Operating System residing on a single server. This outcome has been achieved by:

a) Emulating network engineering through software on a single appliance; and

b) Isolating each and every service in the platform individually without affecting the performance and reliability of the service AND without preventing communication with other "co-hosted" services within the appliance.

Deploying this technology in an organization's Demilitarized Zone (DMZ) is 'best practice'. A DMZ is a network space/zone between a private/trusted network and the Internet as illustrated below. The principle of establishing a DMZ is to ensure the private/trusted network is never directly exposed to the Internet.



iWebGate's patented DMZ Platform resembles a highly secure and incredibly powerful reception area between an organizations' trusted/private network and the Internet.

Copyright © iWebGate Pty Ltd, 2010. All rights reserved.

Private cloud solutions from existing ICT infrastructure – IT business units generate profit

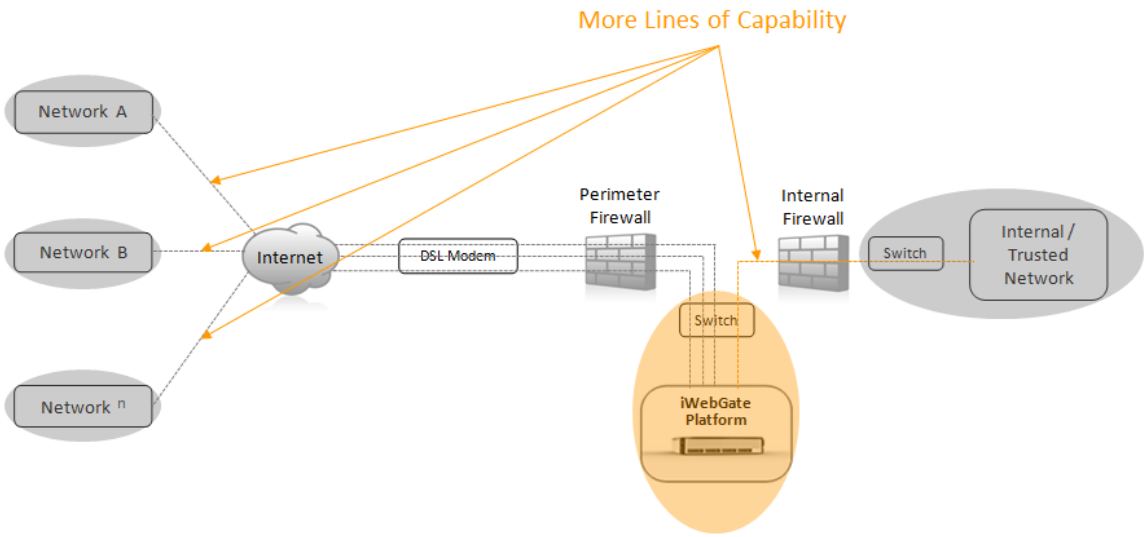
> **"Creativity is the power to connect the seemingly unconnected"**
>
> **(William Plomer)**

What's really clever about the iWebGate Platform is it treats its own private/trusted network as completely alien and untrusted but it has design capabilities allowing it to still seamlessly work with its own private/trusted network over local area network (LAN) infrastructure.

We leveraged off this capability so the DMZ Platform has the same seamless capacity to work with any and multiple alien networks located in remote locations (i.e. securely over the Internet).

This was not possible until we overcame the technical challenges associated with developing each of the network services to seamlessly and securely work in isolation whilst accommodating the need to provide multi-tenant capabilities!

We live in an interconnected world so the technology has been designed to recognize the importance of dealing with any combination and type of network and the endless spectrum of user demands regardless of location. As an example, a software vendor is currently providing business intelligence reporting services for over 160 individual remote locations, each using different point of sale software, from a single iWebGate Platform.



Replacement for insecure VPN

Virtual Private Network (VPN) connections (i.e. IPsec, SSL) are frequently used by organizations of all sizes to provide users with remote access to private/trusted networks, using an encrypted connection, over public network infrastructure. VPN services are a band aid response in the firewall to provide authentication for remote access.

> **VPN services are commercially and universally accepted as resolving risks associated with remote access. In reality, it's an unintended but very real violation of network security!**

Copyright © iWebGate Pty Ltd, 2010. All rights reserved.

In order to gain remote access, a user must establish a connection with a VPN service typically residing on an organization's trusted network. Once connected, the VPN service *extends* the trusted network to the remote user – thus extending the surface attack area of the network to the hacker if the VPN service is breached due to poor configuration or known vulnerabilities.

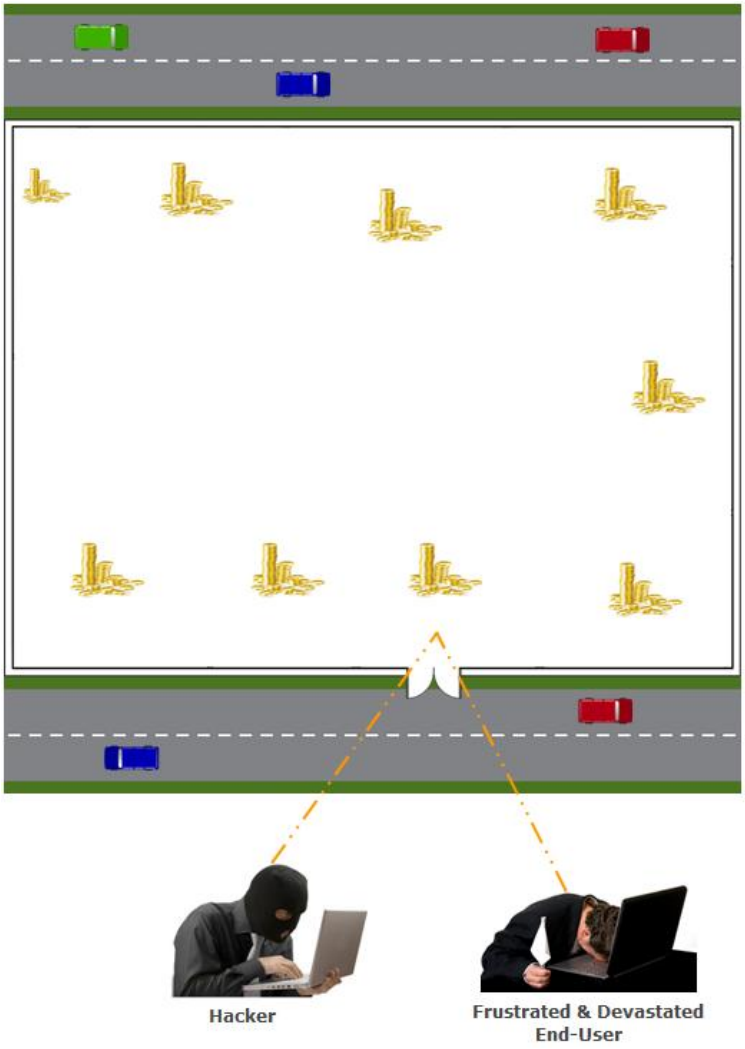
We had great difficulty identifying where VPN services should reside in the DMZ network model. For example:

a) If the VPN service resides in the DMZ network and provide remote access to host machines residing on the private / trusted network, both the DMZ and private networks can be breached because they have all been extended to the remote user

b) If the VPN service resides in the private / trusted network and provides remote access to host machines residing on that network, a port in the perimeter firewall needs to be opened and mapped to the VPN service resulting in the user bypassing and defying the purpose of the DMZ network

In addition to insecurity, users often complain of poor connection speeds, constant drop outs and/or inabilities to connect when using VPN services

The VPN framework resembles a user walking into an open office plan. If these VPN services are breached due to poor configuration or known vulnerabilities they can extend the private and/or DMZ network to the hacker.



Copyright © iWebGate Pty Ltd, 2010. All rights reserved.

It's important these VPN services should not reside in a DMZ or for that matter in a private network.

Instead of extending remote access services we have invented the ability to layer networks using Virtual Local Area Network (VLAN) parameters over a multi Peer-to-Peer framework at a layer 2 network level.

Layering a network resembles an office building with many secure and separate rooms. In a pin point way these rooms are isolated and difficult to identify from the outside as containing any particular service or asset. These rooms are removed as a target because they are never directly exposed to the street (i.e. public network).

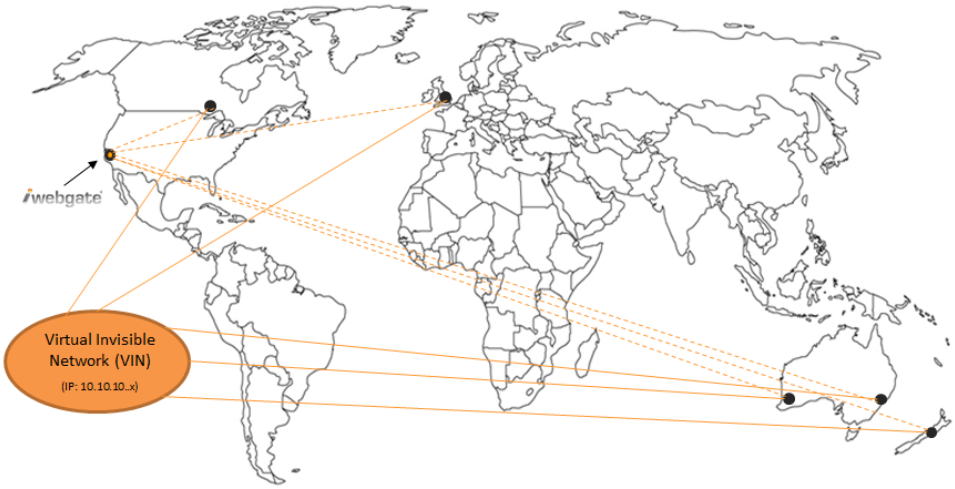
The utilisation of a P2P framework means an office in one building can securely communicate with an office in a remote and disparate building using a communication framework that cannot be seen from the street (i.e. it's invisible to the hacker because firewall ports are not directly exposed to the public network).

This also means all LAN-based software is now P2P enabled without changing a single line of code. Virtual networks can be instantly established over the Internet. Life is made extremely difficult for the hacker because of network invisibility. For trusted users, performance is outstanding – 10 months and still counting without a single drop out.

The breakthrough is so powerful it enables anyone to instantly establish private internets over the Internet. Virtual Invisible Networking (VIN) provides is a replacement for insecure VPN technologies and transforms the way we securely and reliably network on the Internet.

This patent pending technology provides the seamless ability to securely mesh up independent peers residing in disparate networks anywhere around the world, to multiple invisible Virtual Local Area Networks (VLANs) over public network infrastructure (i.e. the Internet).

Copyright © iWebGate Pty Ltd, 2010. All rights reserved.



Our world is transforming with the ability to virtualize servers and desktops. iWebGate introduces the ability to "Virtualize Networks" to the point customers can securely create private-internets over the Internet in seconds!

Copyright © iWebGate Pty Ltd, 2010. All rights reserved.

Availability

iWebGate's DMZ technology is available in a variety of formats to cater for the needs of partners, resellers and end-customers. These formats include:

"Roll Your Own" Software Version

- ✓ Ideal for end-customers wanting to install iWebGate's technology on the hardware platform of their choice
- ✓ Ideal for customers utilizing server virtualization technologies (i.e. they create a virtual machine and install DMZ Platform – eliminating the need to purchase additional hardware)
- ✓ Ideal for resellers and partners wanting to bundle iWebGate's DMZ technology in a ready-to-go appliance for clients
- ✓ Consistently proven to be setup and ready to go in less than 20 minutes
- ✓ Reliability of software version indicates outstanding performance in the following iWebGate customer experiences:
  - 500 days+ without reboot required
  - 9 months remote access connection without a single drop out
  - 370 companies and 145,000 users on a single DMZ Platform growing at 1,500 users per week without a single need to reboot for 500+ days

"VMware" Software Version

- ✓ Ideal for end-customers utilizing VMware (server virtualization) technologies
- ✓ No need to purchase additional hardware to implement DMZ Platform (i.e. reduces costs)
- ✓ Consistently proven to be setup and ready to go in less than 20 minutes
- ✓ Outstanding performance customer experiences (see above)
- ✓ Citrix and Hyper-V versions coming soon!

"Ready-To-Go" Appliance

- ✓ We have a number of resellers who obtain a copy of the "Roll Your Own" Software Version, install it on a hardware device of their (i.e. HP workstation) in less than 20 minutes and seamlessly install a Ready-To-Go-Appliance on their client's network in less than 10 minutes!
- ✓ White label and OEM branded options available
- ✓ Outstanding performance
  - HP Workstation (CPU: Intel Core 2 Duo, 2GB RAM, 200GB HDD) tested to handle 150 companies and 15,000 users

As a result, in line with best practice recommendations, iWebGate now makes DMZ technology available as a standard for organizations of all sizes!

Copyright © iWebGate Pty Ltd, 2010. All rights reserved.