

manage
conversations
not just
the greeting

a better way to protect information

let's explode some myths

wires don't get viruses.

criminals don't want your network.

networks are a means, not the end.

information is the target.

with me so far?

good. then read on.

Contents3

Why you can't control the perimeter4

 Why conventional network security is ineffective.....4

 So what else can be done to secure an Internet facing environment?4

Application attacks: a deadly development5

 A wolf in sheep's clothing.....5

 Malicious mail payload.....5

 How could this happen?.....5

How the threat has evolved6

 The early Internet.....6

Data flow7

 Protecting the information, not just the network.....7

 Introducing internal data protection.....7

 How application firewalls work.....7

 Email protection.....7

Traffic management8

 Controlling the way an application is used.....8

 Out of band management.....8

 Everything blocked by default, including day zero threats8

Application firewalls9

 SQL Injection Attacks.....9

 Protecting the Web enabled business.....9

The Future?10

 Extending control to the perimeter.....10

 Closing the perimeter gateway.....10

About LANZen11

 Thanks for reading this white paper.....11

Why conventional network security is ineffective

Well, there are two main reasons.

First, because we still tend to think about networks the way they used to be. Protected, private cordons around our organisations, with well defined, easily managed entry points. But all that changed when the Internet arrived. Now, those entry points are all around us and are growing every day. And as they expand, we just can't retain managed access *and* run an efficient business.

But more importantly, we think our networks are secure just because we've checked the traffic type at the edge or gateway. Yet once past the perimeter firewalls, an attacker can wreak havoc to a company's web infrastructure with code injections, malformed requests and denial of service attacks.

So what else can be done to secure an Internet facing environment?

We have to start to think about security differently.

We have to realise that innocent-looking traffic arriving at the perimeter may be carrying a deadly payload we can't check until it's deployed. By then, our web infrastructure is compromised and vital customer information or product details is streaming out of our networks.

Mail is a critical business application, yet sometimes, up to 90% of the traffic can be spam, junk mail or malicious. Placing defence mechanisms on the server itself reduces operational efficiency and risks server failure by over-stressing it.

We have to not just make sure the greeting is right, we need to ensure the conversation is controlled as well.

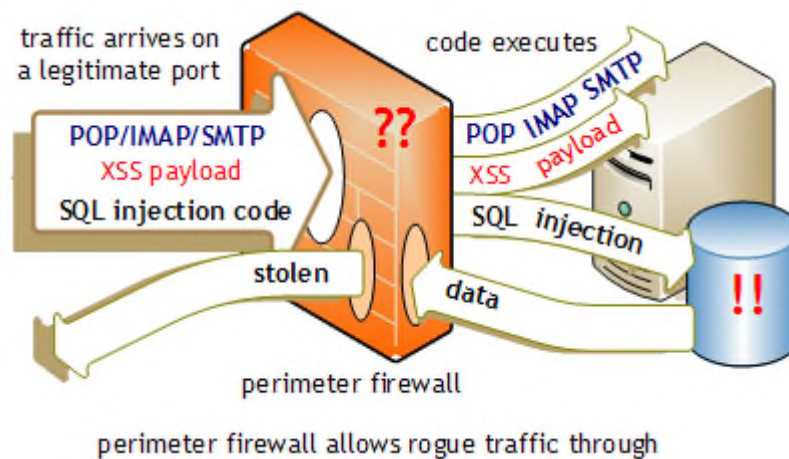
A wolf in sheep's clothing

All the traffic arriving at the perimeter appears fine. It's using the right ports, it's addressed correctly. So, it passes the perimeter firewalls without a problem.

But instead of filling in the web form fields as a normal user would, it injects a series of SQL or Cross-Site Scripting (XSS) code statements into those fields.

The code exploits vulnerabilities in SQL code programming by encapsulating the rogue code inside legitimate form data. The rogue code then executes behind the firewalls and the business's databases start to haemorrhage information.

XSS scripting adds blocks of rogue Java or other script into legitimate forms that can make illegal username and password requests which are forwarded to the attacker's site for use later. Similarly, email traffic is passed through unchecked.



Malicious mail payload

Mail is also be affected in this way. malicious mail comes in waves and can sometimes be up to 90% of all mail processed. Standard firewalls can't help.

How could this happen?

It happens because of sloppy coding practices, often by developers pushed to release web applications without proper testing, poor coding practices, when applications are outsourced to developers whose work isn't properly checked or simply by exploiting vulnerabilities on unpatched systems.

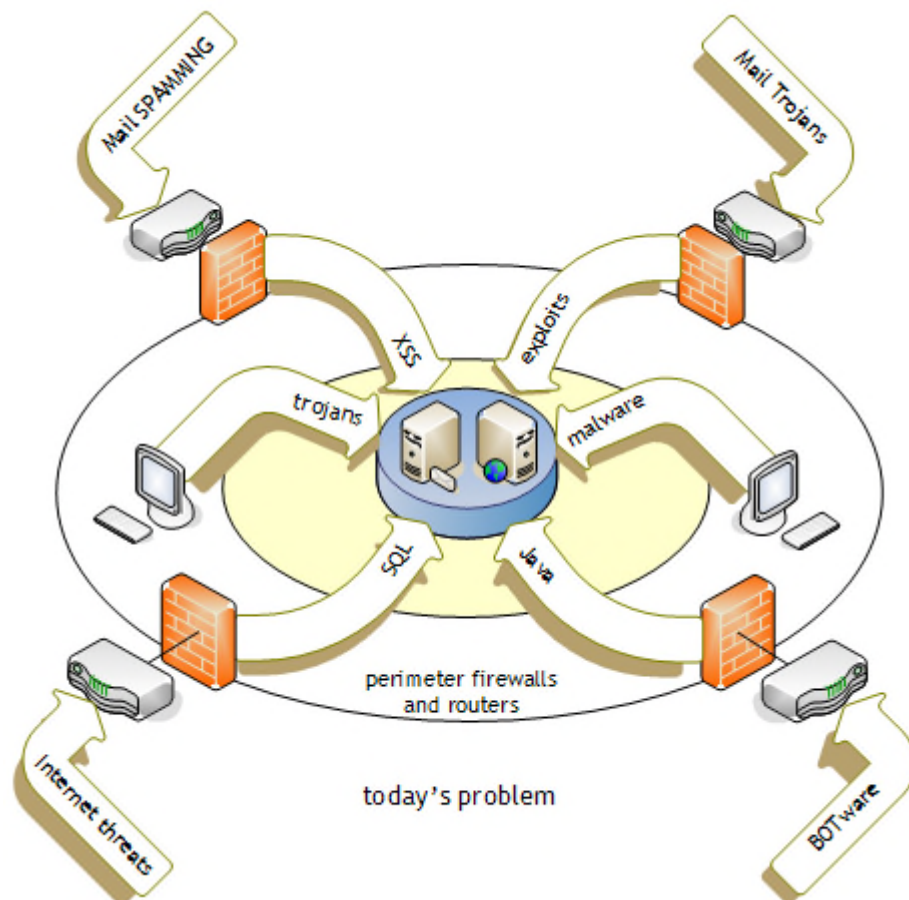
Nor can perimeter firewalls cannot protect against internally-borne attacks, from compromised workstations infected with malware, or used by criminal employees.

Perimeter firewalls still have a place; but clearly the threat has now evolved so that they can't now fully protect any organisation that runs a database-driven application, particularly one sitting behind a website.

The early Internet

When company websites first appeared they were simple brochure sites. They showed potential customers what the business did and provided contact information, or a look at products or services.

As businesses became more confident about the sites, they added transactional abilities, the ability to buy on line or to query stock levels or client details. This meant that information was placed within reach of the outside world. If someone could figure out a way of getting at it.

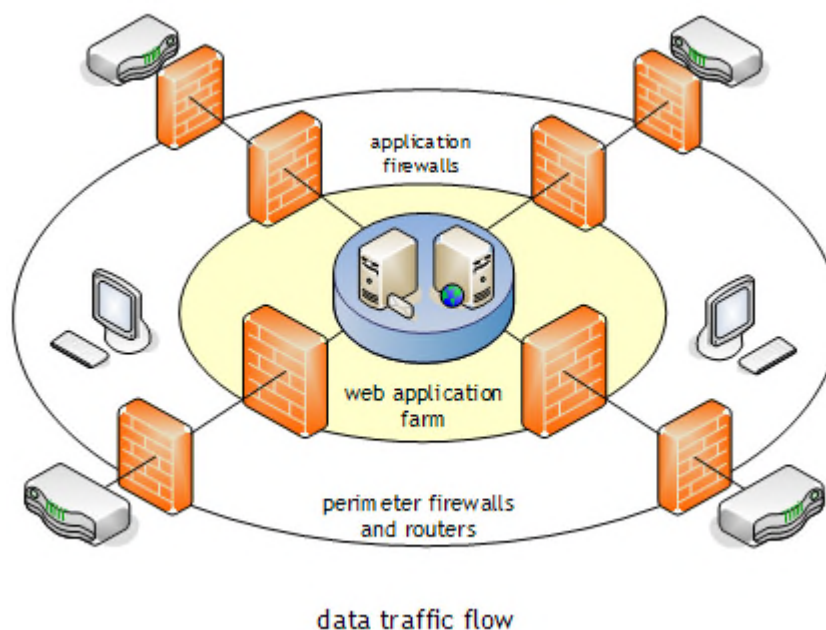


Conventional firewalls were designed to address early Internet-style threats. They controlled ports and IP addresses. Opening and closing access based on port numbers and machine IDs. While effective when these were the only threat, they're useless when the threat is of unknown origin, like the Internet today.

Perimeter firewalls still play a vital role, offering basic protection against many common attack signatures, But they can't defend against the sophisticated attack signature of today's cyber-criminal. Nor can they protect from threats from inside the company network. Few organisations are really sure their workstations or laptops are 100% safe.

Protecting the information, not just the network

This view introduces the concept of the application firewall. Wherever there's a route to the company's information, a firewall confronts it. Wherever an attack may come from, the firewall monitors it. It's ever vigilant, pro-actively and reactively managing the company's security.



Introducing internal data protection

Application firewalls don't simply protect against Internet borne threats. They protect against internal ones as well. Research has shown that companies are at a much greater risk from within. From known and unmonitored workstations on internal networks, employees or contracted agents rather than the Internet. Yet most investment still goes on perimeter-based security. Crazy!

How application firewalls work

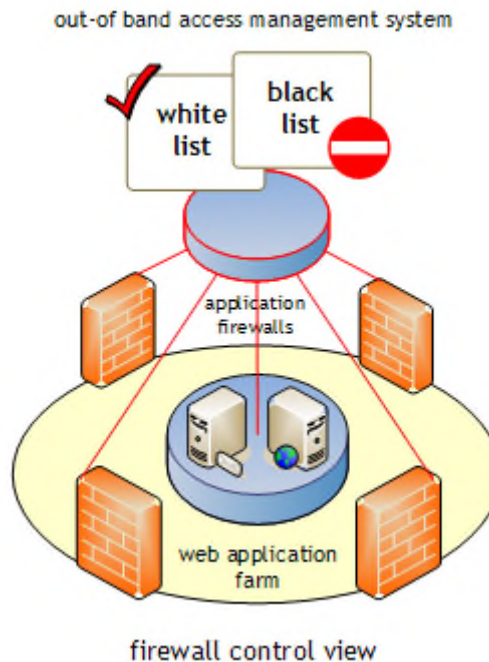
Application firewalls are intelligent devices. They contain processing logic that allows them to interrogate packets in real time and compare the results against code statements held in Web Access Control Lists (WACL's) and SQL expression lists. The better ones also adapt to the applications they manage. This technique is known is given a a number of names, such as Dynamic Application Profiling.

Email protection

Because of their ability to check packet protocols and data, application firewalls can reduce spam and other email borne threats. By stopping rogue traffic before the servers, throughput and server performance is greatly improved.

Controlling the way an application is used

This view shows the controlling infrastructure for an application firewall cluster. Like traditional perimeter firewalls, traffic is managed using an allowed and disallowed traffic policy using white and black listing. This is known as a *positive and negative security policy*.



Out of band management

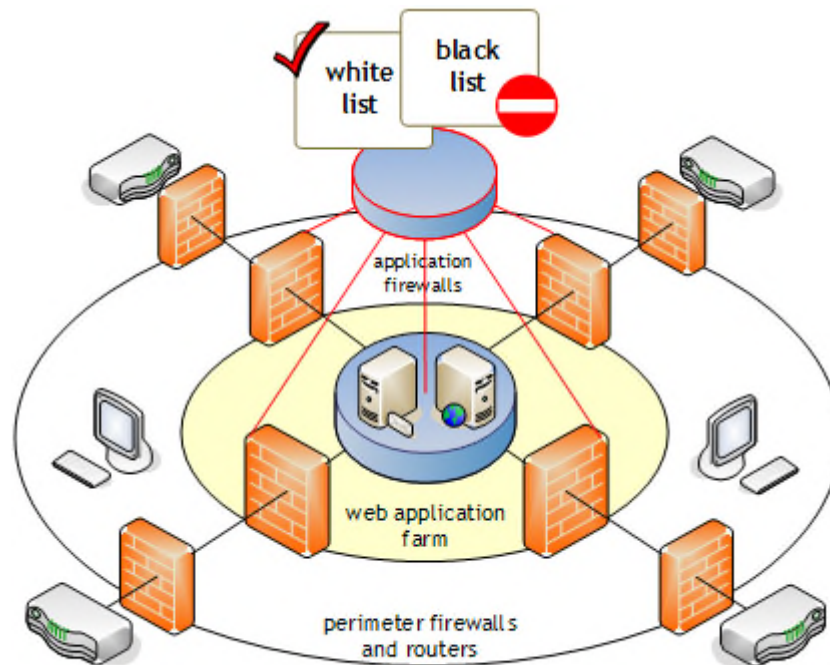
The firewalls are controlled *out of band*. This means outside of the route network traffic follows. This denies unauthorised traffic access to the firewall policies. In this example, the firewalls can *learn* the valid queries from the applications themselves. This is a feature of the better application firewalls.

Everything blocked by default, including day zero threats

By default, all database queries are blocked unless specifically allowed. Good application firewalls use *adaptive technology*. This allows them to actually learn the applications dynamically, building a specific policy while continuing to blocking anything falling outside of the existing policy.

In other words if the code looks unusual, the assumption is that it's bad, so it's blocked. This protects against day zero attacks, the worst threat of all.

This is a view of an application firewall environment. In this case, there are four routers representing the various access points to the servers.



an application firewall environment

By closely coupling application firewalls to the application servers, they will monitor all traffic, internal and external. Monitoring internal traffic is vital; compromised workstations can lead to propagation of trojans or other malware.

The application firewalls check that code passing across them is expected by the applications behind. Any unusual code is stopped at the firewall. It's important to note that there's no route to the servers other than through the application firewalls. This is a key difference between perimeter and application firewalls.

SQL Injection Attacks

SQL injection attacks exploit weaknesses in SQL coding to crash or extract data from the servers. The code is embedded in legitimate SQL queries that perimeter firewalls allow to pass. As standard firewall policies render conventional attacks ineffective, SQL injection is used more and more to bypass network security.

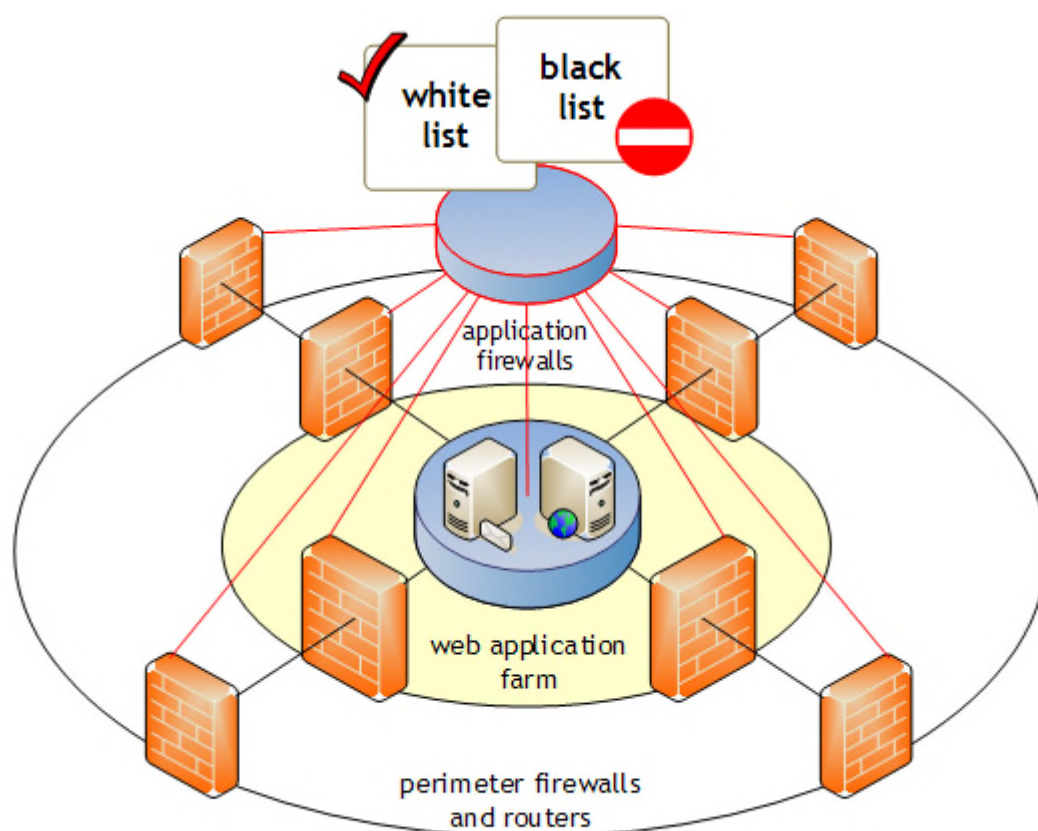
Protecting the Web enabled business

Application firewalls are the only way to ensure enterprises can compete in today's mobile market. They safeguard vital business data and by doing that, protect an enterprises's good business reputation. *And that's priceless.*

Extending control to the perimeter

I hope I've shown that application firewalls are essential for the modern web-enabled business. But application firewalls are an expensive proposition and should be deployed efficiently.

Perimeter firewalls are moving towards the commodity end of the market but could be used to reduce the load on application firewalls by taking the load of them by clever out of band linking. This technique would also provide a 2nd layer of defence, should the application firewalls fail. Here's how...



Perimeter firewalls controlled by application rules

Closing the perimeter gateway

Application firewalls could be developed to provide out-of-band management of the ruleset of perimeter firewalls. Once the application firewalls had identified rogue traffic, its ability to enter the perimeter could be blocked by adding its IP address to the perimeter firewall's black list.

This would substantially reduce application firewall load and at the same time increase throughput. Co-ordination of perimeter and application firewalls would give organisations a far broader security environment. Maybe some time soon?

Thanks for reading this white paper

I'm Neil Robinson and LANZen is my information technology strategy and design consultancy. I'm in Cheshire, in the North West UK. I've helped many clients, like City banks, Jamie Oliver, smaller and start up companies, even one-man operations discover new business IT strategies that work for them.

If you're looking to move your business forward, there is probably something I can help you with. Please take a moment to visit the LANZen website, or the LANZen strategy and design blog.

You'll be in good company, the blog is visited by most of the world's top banks and companies every day.

Neil Robinson

email neil.robinson@lanzen.co.uk

website <http://www.lanzen.co.uk>

blog <http://www.blog.lanzen.co.uk>