Firewall Complexity and Governance – Dealing with the increasing impact of firewall proliferation

July 2012

Introduction

Over the past 15 years the rationale for firewall deployment has changed from being primarily a perimeter security defence solution to a pervasively deployed security zoning technology. This is as a result of the realisation that the hard shell approach to information security and protection is no longer adequate where third party collaborative connectivity, consumerisation and always on mobile communications are common.

However, with this expansion of firewall deployment comes added complexity with multiple layers of firewalls and complicated firewall rulesets, separating customers, partners, users, applications and data repositories. Any misconfiguration could result in a loss of system functionality, or worse, the accidental opening up of systems and information to the wrong audience. This paper looks at the causes and impact of firewall proliferation and the tools available to support the control and governance of firewall and ACL estates.

Drivers of Firewall Proliferation

1. De-perimeterisation

Since organisations first started to become Internet connected in the early 1990’s, firewalls have been the primary line of defence against a malicious third party gaining access to a company’s network attached information and systems. As the scope of connectivity has expanded in the subsequent two decades additional security controls have been implemented including Content Management, Data Loss Prevention, Intrusion Detection and Prevention, Anti Virus:Spyware:Spam:Malware.

Firewalls however, including less intelligent non-stateful router based ACLs, have continued to be the major security defence implemented by organisations to restrict logical access to corporate systems.
The Jericho Forum, now part of The Open Group\(^1\), has long championed the de-perimeterisation agenda which can offer significant financial and operational benefits to those organisations willing to reduce or remove the traditional corporate hard security shell, however with this comes a need to provide new levels of protection for the corporate data assets.

One strategy that companies have adopted to achieve this has been the creation of secure enclaves for corporate data and systems. This effectively shrinks the hard outer shell and focuses the protection at the data/system level rather than the complete corporate IT estate. However this isn't fully aligned with the Jericho Forum's objectives which is predominantly focused on protection of information at the application level.

The consequence of this approach is that each enclave requires its own security defences including its own set of firewalls, whether physical or virtual. With that comes the creation of additional rulebase complexity for intra-enclave communication.

2. Governance, Risk and Compliance

The Governance, Risk and Compliance (GRC) requirements of SOX, FSA, PCI DSS, HIPAA and others has resulted in ACLs and Firewalls becoming a defacto and mandated technology deployed to enforce and protect the multiple zones required to maintain the security of the information assets encompassed by these regulatory and industry bodies. This results in multiple network security zones being created with firewalls enforcing the access into and out of these zones. As with the multiple enclave approach the complexity of firewall rulebases increases as a result of the extension of firewall from an external to internal communications control technology.

3. Corporate Acquisition

An additional driver of firewall proliferation is a consequence of corporate growth being achieved through acquisition. In most circumstances the acquired company will already have its own firewall security infrastructure protecting the corporate perimeter, extranets and internal network zones. Additionally there is often a perceived need to not trust the acquired/acquiring companies IT infrastructure so firewalls are often placed between the two organisations to maintain the security boundaries. Additionally, in many cases, firewalls are implemented to facilitate Network Address Translation between the two organisations due to overlapping use of RFC 1918\(^2\) private IP address spaces. In this case, the business requirements to enable integration can then lead to complex end to end firewall rulebases.

---


Rulebase Management Issues

Rulebase End to End Application Requirements

The underlying principle when implementing firewalls is to automatically deny all traffic and to open up specific traffic types to/from specific locations. This is easy to understand in a simple perimeter firewall environment, however once there are multiple firewall complexes sitting between the users, applications and underlying data this picture becomes more complex. It is more likely in modern network infrastructures that to enable a specific group of users access to a new application or web service multiple firewalls will be involved and all will require specific rules to be implemented for successful deployment of the service.

Ensuring that all necessary firewalls have rules implemented requires the firewall administration team, or in many cases multiple firewall administration teams to have an end to end holistic view of the network and firewall infrastructure in question. Problems occur when this view doesn't exist due to lack of formalised documentation. This leads to delayed deployments of applications due to troubleshooting, identification, and remediation of the missed firewall components in the end to end deployment.

Rulebase Proliferation

As an organisation’s IT infrastructure becomes increasingly segregated by firewalls, more firewall rules are added. This trend is exacerbated by the drive to dynamic service hosting infrastructures being enabled through on demand provisioning cloud based virtualization environments. Firewall administration teams are having to cope with ever increasing loads covering firewall management activities with little or no increase in headcount.

Rulebase Optimisation

Firewall rulebases can, over time, grow to become extremely complicated. It is not uncommon for some systems to have rulebases that are many thousands of lines long. Over time, this can result in two undesirable consequences:

- **Prioritised Rules**

  Most firewalls process firewall rulebases from top to bottom, looking to identify a rule that matches the traffic type being processed. Once a matching rule has been identified the traffic is dealt with according to the matching rule and further processing of the rulebase stops. Thus, if the highest volume traffic types match rules at the start of the rulebase then the processing of firewall traffic will be optimized, leading to faster processing of high volume traffic and also a reduction in CPU utilisation on the firewall as traversal of the rulebase is considerably reduced.

  However this level of intelligence is not regularly applied when implementing new firewall rules into an existing rulebase. This is quite often due to a lack of resources within firewall administration teams to monitor firewall performance and in particularly regular monitoring of the rulebase hit counts to identify the “top talker” rules. That combined with a lack of knowledge of how frequently new rules will be processed, whether through forecasts, or indeed the ongoing organic growth/reduction of traffic as services are introduced, withdrawn or subject to seasonal changes regularly results in firewall rulebases often being implemented in a sub-optimal manner.

- **Redundant Rules**
As applications and services traversing firewalls are introduced, the project implementation team will request new firewall rules to be implemented to support the new environment. However, unless there is strong programme governance in place it is less likely that when the service/application is retired a corresponding rule deletion request will be made, and even if there is there can sometimes be unforeseen consequences of deleting firewall rules where additional applications or services have “piggy backed” onto the existing firewall rule. Without per rule based utilisation metrics, covering all eventualities including seasonal usage (e.g. end of financial year processing) the default posture is one of not deleting rules “just in case”.

The result is an ever growing rule base with redundant rules being unnecessarily processed by the firewall and in some cases resulting in firewall performance being adversely impacted, or a maximum capacity being reached for the number of rules that can be implemented.

Even worse is the potential that a previously redundant rule may result in the unexpected exposure of a new application/service installed on a server utilizing the retired IP address of an old server with the potential for data or services to be unintentionally made available to un-authorised systems or users.

Rulebase Compliance

With the growth of the segregated network zone approach has also come the concept of Inter-zonal communication policies, the definition of allowed and denied traffic flows between various zones. A typical policy could include items such as:

- No direct communication from the internet to the internal network zone
- Citrix/VDI traffic allowed inbound to secure hosting service
- No FTP traffic allowed
- SFTP traffic allowed
- No telnet traffic allowed from internet
- Telnet traffic allowed from Network Operations Centre
- Access to particular services restricted to a department or user group

To ensure that these policies are implemented, with exceptions escalated appropriately, requires a process that enables segregation of duties to perform pre-implementation and post-implementation checks. However the resourcing of this can easily double the manpower required to implement even the simplest one line firewall rulebase update. And even this level of process cannot prevent the following:

- Existing firewall rulebases may not be compliant due to lack of checks prior to introduction of process, or because what was once a compliant rule is no longer so due to a change in policy
- Policy compliance or otherwise can be a subjective decision leading to inconsistent application of policy
- A firewall administrator may make a mistake during the rulebase deployment process which could temporarily (or permanently if not detected during checks) expose the organisation’s information to unauthorized parties
Firewall administrators could maliciously implement a non compliant rulebase outside of the formal process – without detective systems in place these could go undetected.

The result of all the rulebase management issues discussed so far is that many organisations are unable to understand, control and ultimately accurately report on the end to end risk posture of their corporate security environments. This is especially important where regulatory requirements need to be enforced.

Solutions for Firewall Governance & Management

An ever expanding manual approach to this problem is no longer satisfactory. Gartner have stated that “More than 95% of firewall breaches are caused by firewall misconfigurations, not firewall flaws” whilst Forrester concede that “Performing a manual firewall audit in today’s network environment has become nearly impossible”.

Given these statements organizations need to be looking at new ways of regaining and retaining long term control of their firewall rulebases. A number of vendors have been working in this field for the past 5+ years and now have products that are maturing rapidly. The leading vendors are Algosec, Tufin, Skybox and Firemon, each of which have different strengths and weaknesses. These tools integrate into an organisations firewall infrastructure to provide varying levels of functionality covering:

- Definition of approved traffic policies to comply with regulatory & corporate standards.
- End to end change management workflow including policy exception approval routing & automated scheduled policy deployment where appropriate.
- Automatic pre & post change policy audits, including escalation of unauthorized changes.
- Automated rule base optimisation.
- Ongoing tracking of obsolete rules.
- Automated and on demand compliance reporting.

The benefits that these tools can bring are:

- A serviced based view of applications and associated firewalls.
- Organisations are now able to achieve security device compliance through:
  - Ability to prove real time and retrospective compliance,
  - Enabling auditors to quickly satisfy compliance attestation requirements.
- Enable technical resources to focus on technical activities and not bureaucratic processes,
- Automatically & proactively identify & stop non-compliant rules being implemented,
- Support in the region of >= 50% reduction in security resource requirements for each firewall change request,
- Release technical resources to perform additional activities or if desired support a reduction in head-count,

---

3 See Gartner Article ID : G00208704 “Q&A: Is It More Secure to Use Firewalls From Two Different Vendors?” published November 4th 2010 (Subscription required)
4 See http://www.forrester.com/rb/Research/market_overview_firewall_auditing_tools/q/id/54663/t/2/
In addition to enabling organisations improve their own management, another area that these tools can add value is the Managed Security Service Provider space. By using these tools the MSSP can enable a customer to:

- Define and control policy and exception handling.
- Maintain assurance that firewalls are always compliant to policy.

This may also lead to a reduction in customer audit requirements through automated reporting and increase the customer confidence in the MSSP and supporting potential opportunities to extend the MSSP relationship.

Conclusion

Although firewalls are now an ubiquitous network and security tool, with organisations increasing their deployments and day to day use, there are now effective technical solutions that can enhance security posture, maintain and report on compliance. Additionally, where these tools are deployed to their full potential, there is the promise of operational returns on investment and freeing up of highly skilled technical resources from the burden of governance paperwork. This provides security organisations with an attractive proposition that not only makes security sense, it also makes business sense.

DMW Information Security is a professional services practice to help organisations solve high risk information security challenges and counter the real and growing threats to the security and integrity of their information systems. All of our consultants are trusted advisors and experienced experts that have industry leading reputations.