

De-perimeterized Architecture

By Ido Dubrawsky – ISSA member, Baltimore, USA Chapter

Difficulties posed by current network capabilities, protocols, applications, and business needs have resulted in a redefining of the network perimeter. This article describes the evolution to a perimeterless network architecture.

For some time now the accepted design concept for any given network architecture has been the defense-in-depth model where multiple layers of filtering, monitoring, and analysis technologies seek to identify malicious behavior and activity. Early white papers like the original Cisco SAFE series provided conceptual models whereby the network was subdivided into multiple blocks separated through network choke points utilizing firewalls and routers. This design provided for restrictions to be placed at critical junctions where network traffic can be limited to specific protocols and direction flows. In essence the firewalls played the role of policemen, separating the network topology into “trusted” and “untrusted” zones.

This architecture provides strong perimeter-based security throughout the network. Difficulties posed by current network capabilities, protocols, applications, and business needs have resulted in the reduction of the firewall as the effective tool for network security at the perimeter. In addition the emergence of cloud computing poses additional challenges to the traditional firewall design. As services move out from the enterprise network into a cloud environment the effectiveness of the firewall diminishes. In a cloud environment security must travel with the data and therefore the paradigm of perimeter defense must change – the only question to be answered is “how?”

De-perimeterization

A possible model is one based on an architecture that has been in development for the past five years within the Jericho Forum, a community of public, private, academic, and interested individuals working to define a solution or set of solutions to address shortfalls in “traditional approaches to network and system security architecture and design [that] cannot cope with some important contemporary business drivers

for collaboration and commerce.”¹ While it does not represent all possible evolutions of the defense-in-depth design, it does represent one vision of how network security could evolve to meet the security challenges of today’s networks and cloud computing environments. Some of these contemporary business drivers for collaboration and commerce include the following:

- The increasing use of on-line collaboration and trading between business entities, which can involve the sharing of high business-impact data
- A shift towards industry outsourcing and off-shoring of support services and core business processes along with the attendant skill set required to support them
- The use of low-cost, open networks to achieve collaboration and commerce

These business drivers are changing how organizations do business and how they collaborate with their partners. The end result is that today’s network perimeters are slowly being eroded and losing their effectiveness. In today’s architectures most businesses allow for partner connections to tunnel through their perimeter or bypass it altogether; applications are being designed to encapsulate their communications within HTTP to avoid being blocked by perimeter devices; and security threats are increasingly entering networks utilizing email, instant messaging, and web-delivered malware vectors.² As business drivers require greater collaboration,

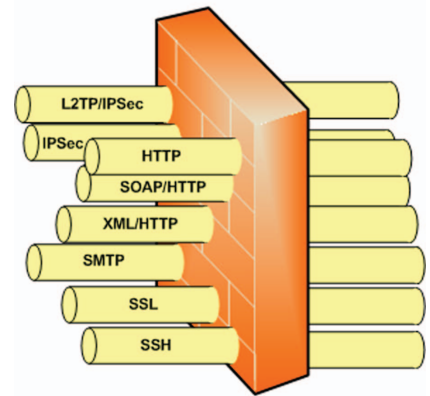


Figure 1 – The De-Perimeterization Concept

1 “Visioning White Paper,” Jericho Forum (February 2005) – http://www.opengroup.org/jericho/vision_wp.pdf (accessed May 2009).

2 “The What and Why of De-perimeterization,” Jericho Forum (2009) – <http://www.opengroup.org/jericho/deperim.htm> (accessed July 2009).

more protocols and exceptions must be made in the perimeter firewalls to accommodate the traffic. The exceptions to the firewall policy, in effect, become more ubiquitous to the point that the firewall itself loses its initial effectiveness. This overall process of erosion is what is known as *de-perimeterization*, as shown in Figure 1.

The Jericho architecture is a response to this erosion, a way to continue the evolution of the defense-in-depth network model and provide additional security to data. De-perimeterization still maintains the need for firewalls as part of a multi-layer approach to securing a network and the data that resides on it. As threats have evolved, the effectiveness of the firewall as the primary point of security for a network is being lost and a new paradigm developed.

Using the business drivers outlined above, the Jericho Forum has detailed a set of commandments that are necessary to deliver on the vision of a de-perimeterized architecture. Two of these commandments are that “security mechanisms must be pervasive, simple, scalable and easy to manage” and “all devices must be capable of maintaining their security policies on an untrusted network.”³

These two commandments define a different paradigm in network security. The traditional approach has been to build a network with firewalls and other security mechanisms defining the boundaries of the system as a whole as well as internally between different network modules. However, the complexity that arises from these architectures violates the business drivers that organizations are trying to achieve today – complexity increases the cost of business and makes collaboration difficult. Additionally the threats are changing rapidly and are beginning to stress the defense-in-depth model. The question is how to rethink and rebuild the model that is in place today so that it will not only provide security and collaboration capabilities today but also into the future?

The Jericho architecture

The Jericho architecture builds on top of the traditional architecture in which boundaries are formed at distinct locations and with defined data flows. The underlying concept of the Jericho architecture is the free flow of information without hindrance between authorized clients. Rather than eliminating firewalls completely this architecture is multi-layered in design – similar to the current concept of defense in depth as shown in Figure 2.⁴

The definition of a defense-in-depth network model utilizes layers of security in the network in a perimeter fashion. The Jericho architecture is similar in approach but tries to spread the security deeper, driving security all the way down into

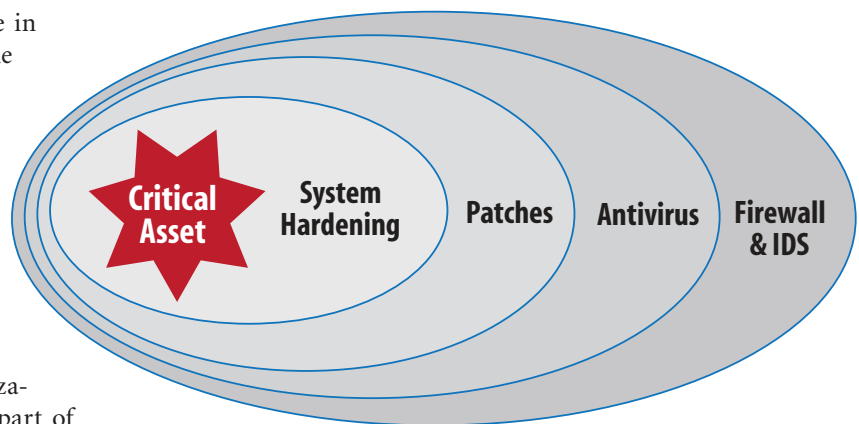


Figure 2 – Multi-Layered Architectural Approach

the resources. Looking back at the two commandments noted above, the Jericho approach is to push security into every component in the overall system, including the application and the data as well. The final vision is that every component is independently secure and uses a mixture of

- Encryption
- Inherently secure communications
- Data-level authentication

It is fairly easy to understand the need for encryption and “inherently secure communications” in this effort, but the question arises with regards to what is “data-level authentication”? Data-level authentication is defined as the data being encrypted with specific read and write privileges, and when that data is moved, those privileges are retained across the move.⁵ This is nothing new and has been a goal of every data architect and security administrator for a long time.

Technologies

Until recently the data-level authentication called for by the Jericho architecture has been elusive. When the forum was first created in 2004, the various components of the architecture were not as mature as they are today, so the ability to embed security into network architecture was considered a “future” possibility. Today many technologies exist that can be leveraged to meet most of the requirements of the Jericho architecture. These technologies include firewalls, intrusion detection systems, antivirus, and patch management, but also IPv6, server and domain isolation, digital rights management, and identity management and federation.

IPv6

IPv6 addresses many of the security shortcomings of IPv4 through the integration of IPSec as a fundamental interoperability requirement, but its widespread adoption has been very slow. As such it remains a future possibility.

The roles that the other components are not as well known and described in more detail below.

3 “Jericho Forum Commandments,” Jericho Forum (May 2007) – http://www.opengroup.org/jericho/commandments_v1.2.pdf (accessed July 2009).

4 “Jericho Forum Brochure,” Jericho Forum (2008) – <http://www.opengroup.org/jericho/brochure/F080402.pdf> (accessed July 2009).

5 P. Simmonds, “De-perimeterisation - This Decade’s Security Challenge.” Blackhat. Las Vegas: Blackhat, 2004. 21.

Server and domain isolation

Server and domain isolation (SDI) leverages IPSec and Microsoft's Windows Active Directory to allow network and security administrators to dynamically segment their networks into more secure and logically isolated environments. The segmentation is based on group policy utilizing IPSec as an enforcement agent. This allows the ability to lock down access to network resources such as data stores and applications and make their availability based on user authentication and group membership rather than access control lists in a network device. It also can be done without requiring a costly physical redesign of the network infrastructure. Another benefit of SDI is the ability to require encryption between systems – whether server-to-client or client-to-client – in order to preserve the confidentiality of the data.

One of the big benefits to server and domain isolation is that it can provide inherently secure communications by requiring authentication of end users and systems attempting to communicate with each other and by providing optional encryption. As more and more businesses adopt IPv6, in the long term they will be able to leverage their existing SDI implementation to continue to apply connection-security policy in the IPv6 environment.

Digital rights management

Digital rights management (DRM) is a technology that is applied to data to restrict access or use of digital information to authorized individuals. Unlike many other technologies DRM has the distinct advantage that the security applied to the data travels with the data no matter where it resides. DRM can be used to partially meet the data-level authentication requirement directed by the Jericho architecture. DRM encrypts information and applies a specific policy as to who can access the information and for how long. Those authenticated individuals who have the appropriate authorization to consume the data are able to access it while those who do not have the appropriate credentials are not. In essence DRM provides the ability that security remains attached to the data wherever it may be.

Identity management and federation

Another key component needed is identity management and federation. Without a strong identity management system in place it will be difficult to manage the data rights of those users who are authorized to view information that is protected with DRM. In addition a strong identity federation model is necessary in order to provide access to business partners and other business vendors. The

identity federation will tie the external partners and vendors into the DRM system of the organization, allowing for secure, managed sharing of information.

Example network design

An example network design is useful in order to understand the difference between the Jericho architecture and traditional security architectures. A network using a defense-in-depth model utilizes firewalls as choke points and gateways to control and determine which traffic should be allowed through and which should be denied. Connection-oriented security is the main stay of today's design. As more applications shift towards utilizing HTTP as an underlying transport protocol for communication, the firewall's job becomes more critical and the intrusion detection system more essential. The Jericho Forum's premise that the security should travel with the resource approaches the problem from a different perspective. As such a Jericho architecture is different – not necessarily better automatically, but different. The Jericho architecture shifts the basis of the network design from a "secure connection-oriented" design to a "secure resource" design.

The original Cisco SAFE architecture broke down the network into various modules which include the following:

- E-commerce
- Corporate Internet
- VPN and remote access
- Extranet
- Edge distribution
- Building
- Building distribution
- Core
- Management
- Server

A graphic representation of the original Cisco SAFE architecture is provided in Figure 3.

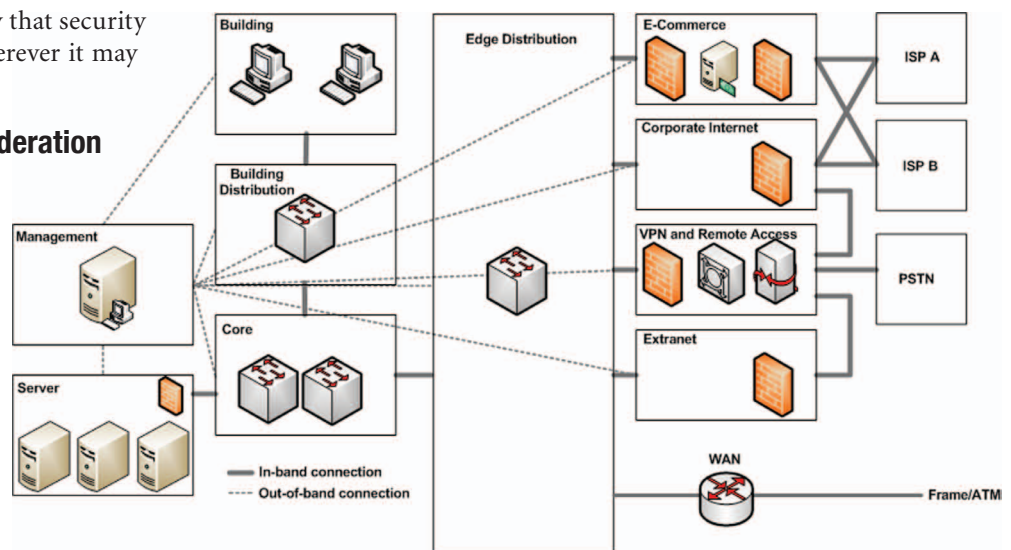


Figure 3 – Original Cisco SAFE Architecture

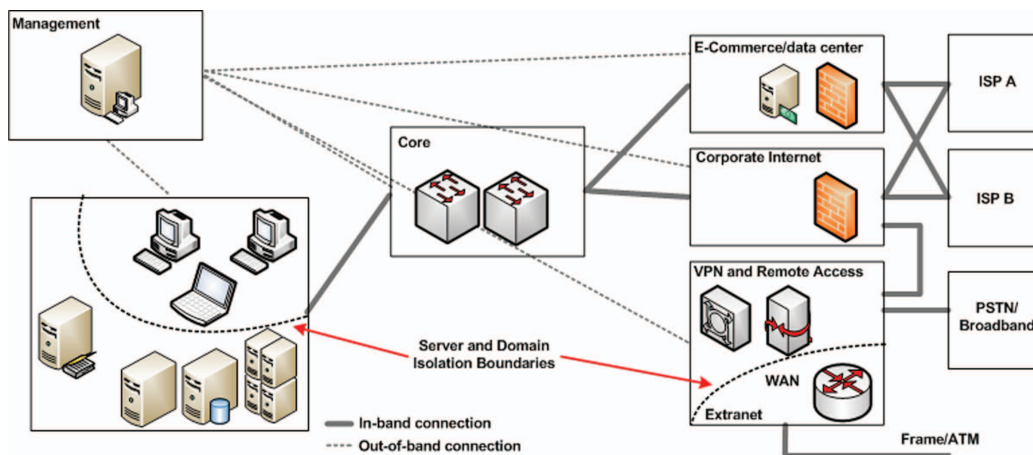


Figure 4 – Jericho Architecture

Most module demarcation is achieved through physical controls – firewalls as well as through access control lists in the switches (except, of course, at the core). Data resource access is controlled via connection-level authentication as well. To date this design has been the mainstay of enterprise-level security in the business world. This design is based on the concept of connection-level access being the control level for users and guests on the network. In many cases this is necessary and sufficient to provide a high level of security on the resources.

The Jericho architecture takes this design and continues its evolution towards secure data (or resource) level authentication. This design can accommodate the firewalls already in the network as the architects and administrators migrate towards a de-perimeterized model. Leveraging server and domain isolation, the network administrators can control access to various resources through group policy and user-group membership. One conceptual design is provided in Figure 4

In this design the controls between many of the modules are based on group policy and identity and SDI. SDI provides the architects and administrators the ability to collapse the architecture to a simpler physical design while leveraging greater control on access to systems based on user identity and authorization. In addition utilizing digital rights management, the security travels with the data wherever it may be. Partners access resources on the extranet, relying on identity federation for authentication (control is based on SDI) and access (controlled through digital rights management). All unauthenticated traffic is ignored and any traffic that is authenticated but attempting to access an unauthorized resource is similarly ignored. Users have access only to those systems and applications that they are authorized to use, based on group policy. This centralizes the management of access control even further and helps reduce the possibility of error.

Drawbacks

There are several drawbacks to the Jericho architecture, which make widespread deployment difficult for many orga-

nizations. In the example design provided the ability to enforce resource access based on group policy assumes a homogeneous network operating system environment such as Microsoft Windows. Today, few organizations have networks that are so homogeneous to the point that they don't include alternate operating systems such as Solaris, HP-UX, Mac OS X, or Linux. How these operating platforms

can be included in the design so that they can benefit from technologies like server and domain isolation is a non-trivial problem to be resolved.

Another drawback is that the concept of data-level authentication is not as widely available as called for by the vision paper. DRM goes a long way to fill this gap but does not provide complete coverage of all data resource formats.

Conclusion

The Jericho architecture may not appeal to everyone and it is not the only possible security architecture out there that could meet the needs of enterprises today – it represents one possible design in the evolution of network security and may not be appropriate for everyone. The architecture was created in response to changes in the threat landscape and the business needs of organizations. It calls for embedding security beyond the network or connection layer and pushing it all the way into the data. To this end technologies exist today that allow for many of the original Jericho architecture concepts to be deployed. These technologies include firewalls, IDS, anti-virus, and patch management as well as server and domain isolation, digital rights management, and IPv6. In combination these technologies can help organizations re-design their networks to begin incorporating concepts of the Jericho architecture that extends defense-in-depth further, thus providing organizations with the ability to ensure the security of their data no matter where it resides. In the long run this could help organizations reduce their business costs while increasing their ability to collaborate with business partners and to take advantage of new opportunities.

About the Author

Ido Dubrawsky is currently the security advisor for Microsoft's communication sector district. He has focused on network security for nearly 15 years and is an avid beekeeper as well. He lives with his family in the Washington, D.C. metro area and may be contacted at idubraws@dubrawsky.org.

