Blueprint for Cyber Security Zone Modeling

Andrew Gontarczyk, Phil McMillan, Chris Pavlovski
Digital Protection Group
Commonwealth Bank of Australia
Sydney, Australia

***Abstract*—The increasing need to implement on-line services for all industries has placed greater focus upon the security controls deployed to protect the corporate network. The demand for cyber security is further required when IT solutions are built to operate in the cloud. As more business activities are migrated to the on-line channel the security protection systems must cater for a variety of applications. This includes access for enterprise users who are mobile, working from home, or situated at business partner locations. One set of key security measures deployed to protect the enterprise perimeter include firewalls, network routers, and access gateways. In addition, a set of controls are also in place for cloud enabled IT solutions. Collectively these components make up a set of protection systems referred to as the security zones. In this paper, a security zone model that has been deployed in practice for the industry is presented. The zone model serves as a design blueprint to validate existing architectures or to assist in the design of new cyber security zone deployments.**

Keywords—Cyber security; lateral movement; firewall zones; security zone model; cyber threats

I. INTRODUCTION

The need to support an on-line presence and cloud services for many enterprises has changed the fundamental way in which consumers and businesses interact. The general public now has internet access to enterprise systems that have traditionally been accessed by support staff only. This also means that the general consumer also has a way to establish connectivity to the network and adjacent systems that are deployed within the corporate network of the business. In order to grant and control access to these on-line systems a series of firewalls, identity access management, and protection mechanisms are implemented to enable access for legitimate users, whilst denying access to accidental use by valid users, and to prevent all access to malicious users and attackers.

Firewalls are viewed as the foundation technology by which the corporate network is protected. However, the management and enforcement of legitimate access has evolved considerably and requires a complex set of models in place to accommodate the range of control mechanisms to be supported. While there are firewalls that are now designed for applications and databases, the fundamentals of grouping applications together in different security zones poses a security challenge for network designers and security architects. The security zones must cater for both external and internal access and must also protect applications from each other in the case of compromise; more recently referred to as lateral movement. This area of work is also classified under work related to Unified Threat Management (UTM) and Perimeter Security [1].

Together, with a set of principles for enabling access to corporate services, a security zone model also comprises technology, rules, and implementation guidelines for developing a set of security zones. This paper extends preliminary work that appeared in [2]. Specifically, a cyber security zone model together with case study scenarios that illustrate how this can be applied in practice is presented. The proposed security model may be used as a blueprint for security and network architects in developing and refining the zone policies and frameworks. The proposed model is based on work developing security zone frameworks in multiple industries. Hence, the main contributions of this paper are as follows.

1. Discussion of the technologies applicable to security zones, with a set of design principles and guidelines that may be used in practice when developing a security zone model.
2. A security zone model is proposed that may be useful as a design blueprint for developing security systems to protect the enterprise network, its assets, and users.
3. Working scenarios are described to show how the proposed model may be applied in practice with a classifier to assist designers in application deployment decisions.

In the next section, the literature is reviewed that relates to security zones and protection of the corporate network. This is then followed in section 3 with a brief discussion of several modeling concepts to support security zone models together with some definitions. In section 4 a set of guiding principles is then suggested that may be applied when developing a security zone model. In section 5 a security zone model is presented as a blueprint together with the security controls to be applied. This is then followed in section 6 with some case study examples that illustrate how to apply the zone model together with a classifier that can be used as a guide for security zone application deployment decisions. Finally, in section 7 we elaborate upon further work that may be explored and summarize the key points made in this paper.

II. RELATED WORK

After a review of the literature in security zones and network security it is noted that whilst there is significant work

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

in identity access management and unified threat management in terms of firewalling and network segmentation, there is less work that focuses specifically on security zone modeling. The related works are now briefly discussed.

The majority of previous work has focused on firewall designs and architecture [3–6]. Conventional firewall technologies are suggested to protect the organization from threats from external entities over the Internet. The idea of a distributed firewall to extend this protection system against new threats that originate from insider attacks was first introduced by Bellovin [3]. Several papers have extended this approach. Markham and Payne discuss the notion of network edge security that also counters threats from within the organization [4]. The authors define 1st generation firewalls as focusing on threats from the internet and outline a distributed firewall architecture suggesting that protecting from internal threats is the focus of 2nd generation firewalls. There is further work that discusses a distributed firewall architecture where several problematic areas of distributed deployments are addressed with improvements suggested in rule tampering, insider attack, packet sniffing, address spoofing, and denial of service [5]. A more specific application of firewalling is treated in [6] where a reference architecture and model for a database firewall is presented. The paper observes the more recent trend of application level attacks such as those targeting databases, with the purpose of a database firewall to protect against such application-specific attacks. The presented model segments the firewall into several layers including network, schematic, and semantic layer. The paper makes the claim that an improvement in security may be achieved through this layered approach. There is also extended work in devising a firewall design that is applied to grid architectures [7]. The authors note that traditional firewall techniques to accommodate grid networked applications are to relax firewall rules. In their work, they propose a firewall traversal approach using proxies to preserve firewall integrity.

There is some work on security zones, in [8] two case studies are discussed where security zones are modeled using a set of routers and firewalls. The techniques apply the Policy Description Language (PDL) [9] to specify firewall routing policies. Moreover, the policy language is extended with additional declarations that support zones, hosts, and interfaces that enable the definition of security zones; the revised scripting language is thus referred to as PDL zones (PDLz). There is more zone related research in [10] where network partitioning is applied to established protected zones. The authors apply their work to specifically address the issue of malicious code and propose security zones to aid in detection and to prevent the spreading of these threats. It is finally noted that the collective use of network routers, firewalls, and several other security functions is referred to as Unified Threat Management [11]. The UTM security functions and nodes are also applied to establish security zones, the application of these technologies to offer a zoned based monitoring and control system is also observed in [12].

The existing research in security protection mechanisms for the corporate network, its assets, and users has treated a broad range of topics. However, the topic of security zones modeling has received less direct attention. Furthermore, industry offers a range of network zoning appliances that are highly configurable but do not necessarily prescribe a particular zone model to adopt. As such, this paper builds upon the previous work to develop a security zone model design template that may be used for building security systems that protect applications, devices and assets of the enterprise in private data centers or the cloud.

III. Security Zone and Trust Level

The key concepts that directly apply to security zone modeling are now briefly described. This includes the notion of trust level and communications channel with respect to security zones.

Security zones represent a level of trust, with the outermost zone being the uncontrolled and most un-trusted domain. The zone levels progress through to the enterprise network providing maximum trust, with access to protected resources. Referring to Fig. 1, each security zone is associated with a level of trust (with Trust Level 1 the lowest). A robust security zone model will consist of several security zone layers with increasing level of trust that increases towards the most secured area of the corporate network.

In a security model, connecting zones are attached to each other via a communication channel. Fig. 1 shows the three general classes of communication channels as unmanaged, externally managed and managed. The communication channel classifications will typically align with specific security zone labels, and may be viewed as follows:

- *Unmanaged*: These are any communication channels which the enterprise has no physical control over; a typical example would be the Internet.
- *Externally Managed*: The communication channels that are managed by 3rd parties on behalf of the enterprise, e.g. external telecommunication providers, public cloud environments, or virtual private networks (e.g. MPLS).
- *Directly Managed*: These are all communication channels directly managed by the enterprise. Examples include data center networks, local and wide area networks.

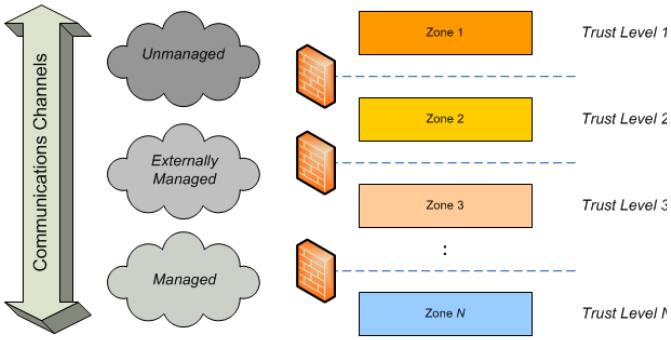

Fig. 1. Security Zones, Communication Channel & Trust Level

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

IV. Design Principles

Before describing the proposed security zone model, a set of design principles by which the zone model is to address is given. The defined principles may be considered as guiding standards in order to accommodate situations that arise where an exception is sought on specific technology decisions.

A. Traversing Security Zones

When access is requested by any applications or user the associated data traffic can only increase by one trust level when moving across a security zone boundary. This principle applies to traffic in both directions, inbound and outbound, across a zone boundary.

The rationale of this principle is to mitigate risk against the threats that originate from a less trusted zone by allowing the trust of a session to be increased in discrete and predefined amounts. The approach facilitates the defense in depth principle [13] from a security policy perspective.

The implication of this principle is that hardware infrastructure will need to exist in each zone to support the transmission of applications data over multiple zones. In addition, connections from a low trust zone to a high trust zone will need to traverse multiple zones which may increase transaction latency.

B. Earning Zone Trust

All connections must earn the level of trust for the zone they are accessing, in order to interact with any asset hosted within that zone. The level of trust is earned by meeting the security controls and mechanisms in place for that zone, this may include (see next principle) adhering to boundary port restrictions, network address restrictions, authentication, authorization, proxies, and passing access controls policies.

The rationale of this principle is to classify data connections appropriately, to treat them on a least-privilege basis, and to mitigate threats that originate from a less trusted zone.

The implication of this principle is that application capability will need to exist in each zone to support the transmission of applications data over multiple zones. In addition, connections from a low trust zone to a higher order trust zone will need to traverse multiple zones. This will increase the number of interactive-hops that a connection needs to establish in order to gain access to protected assets.

C. Zone Interaction

In order to transit through a zone implies that there is some form of interaction with a device or system in that zone to be able to earn the level of trust associated with that zone. This is achieved through mechanisms such as authentication and authorization, application processing, and application proxies. It is noted that security encryption between zones does not mean that the trust of the traversed zone(s) is inherited.

The rationale of this principle is to ensure support of the first principle of traversing security zones. Specifically, each zone must implement some security measure to alter the trust level of connections passing through the zone to a trust level commensurate of the zone. This principle helps enforce the first principle by ensuring a session cannot accidentally pass transparently through a zone; hence maintaining the defense in depth model [13].

There are two key implications of this principle. Infrastructure will need to exist in each zone to support the transmission of applications data over multiple zones, and connections from a low trust zone to a high trust zone will need to traverse multiple zones

D. Zone Security Requirements

The placement of data and systems in any particular zone will be driven by the relevant Confidentiality, Integrity, and Availability (CIA) requirements for those systems. For example, mission critical systems that require a higher level of security and availability are likely to be deposited in a more secure zone.

The rationale of this principle is to facilitate the consistent application of CIA requirements across all zones. Since confidentially and integrity are fundamental security requirements, this will help to provide a close link to the IT security policy through system and data classification.

The implication of this design principle is that the requirements for confidentiality and integrity will need to be determined and agreed upon during the design of the IT solution. The security zone model will also drive the logical and physical deployment of business application systems and components.

E. Zone Communication

In general, all communications between physically controlled security zones is to be carried out over managed communications networks. There are some exceptions where data emanating from an externally controlled environment (such as the cloud) may gain direct access to a zone. That is, there is no need to travel all zones where the externally controlled environment has suitable security measures in place that satisfy the security zone policy being accessed.

The rationale of this principle is in the importance to consider communication in the overall zone model because the boundaries between communication technology and the security zones will drive specific control requirements at the zone boundaries. This will also mean that controls are in place to protect data travelling across networks and zones.

The implication of this principle is that a trusted relationship between external suppliers (i.e. cloud service providers) needs to be established prior to connection establishment.

V. A Security Zone Model

Security zones are a key high-level design construct within the security architecture, providing a clear and efficient way of organizing IT solutions when building a logical deployment model for sub-components. The security zone enforces security policies and protects assets. This helps to make the locations and access to information more intuitive to understand, justifying application placement and maintenance when deployed. A basic tenet of the security zone is to group

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

protected assets that have a similar level of trust to facilitate consistent security policy decisions for access. The trust designation for a zone is determined by the lowest common denominator, in terms of trust associated with the zone, specifically this is a combination of the following.

- Threats within the zone: This is driven mainly by physical considerations as well as a combination of users and systems.
- Systems deployed to the zone: The level of trust and system mission criticality associated with infrastructure deployed to the zone.
- Users accessing the zone: The level of trust associated with the users of the zone.
- Data stored within the zone: The security classification of data at rest in the zone.

The above points must be considered when defining and using security zones. As mentioned, the overall level of trust associated with a zone (and the residual risk) will be that of the least trusted component. The security zones can be represented logically as illustrated in Fig. 2. Each zone has its own security characteristics and is separated from other zones with boundary security systems such as firewalls, proxies, and access control mechanisms.

Referring to Fig. 2, it can be seen that there are effectively three main classes of security zones, where the key differentiator is the level of physical control the enterprise will exercise over them, these are as follows.

No Physical Measures: Any zone in this category is completely beyond the direct physical measures that can be applied by the enterprise. Moreover, it is largely difficult to implement any tangible form of physical control in these environments that may be used to secure the users and systems within them from external threat agents.

Limited Physical Measures: In these zones the enterprise has direct physical measures in place, however due to the nature of these environments (e.g. general office space), the effectiveness of these measures is limited to enable an effective and efficient working environment. For example, external consultants, maintenance, and other parties are able to enter these environments and move around relatively unsupervised.

Strong Physical Measures: In these zones the physical measures are very restrictive. They typically have a very limited number of people that have access, and where access is granted it is generally under a rigorous control process. Typically the users external to business in these zones are also supervised.

Before describing each of the defined security zones, it is necessary to illustrate how the level of trust, asset criticality and the need for a managed communication channel are situated with respect to the security zone and communication channels. This is depicted in Fig. 3, which also shows the permissible traffic and data flows between the security zones.

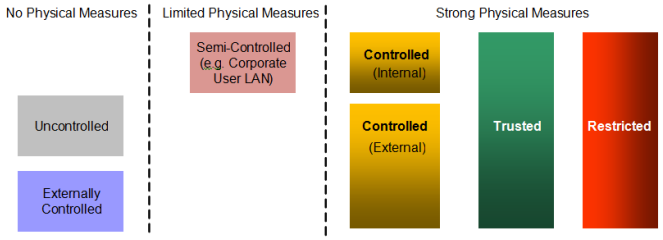

Fig. 2. Logical View of Security Zones

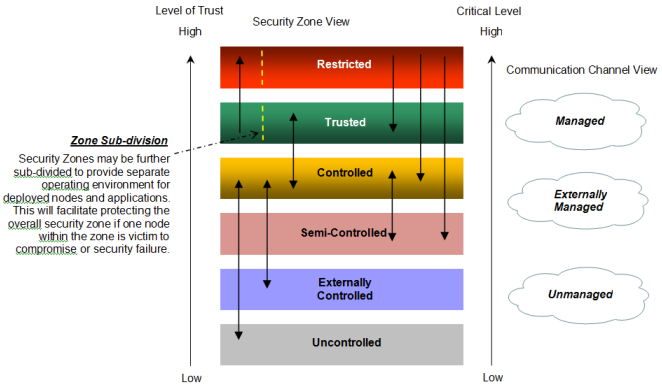

Fig. 3. Physical Security Zone with Transit Permission

An object with access to one zone is not necessarily granted access to other zones. In order to maintain the trust model, zones must be traversed sequentially when moving between the non-adjacent security zones. That is, it is not possible to leapfrog or skip a zone. For example, if moving from an externally controlled zone to the restricted zone it is mandatory to move through the controlled and trusted zones. While this is consistent with the design principle, there are some exceptions. For example, where an interacting entity originates from an external entity, such as a business partner that has previously established the necessary level of trust, access can be granted directly into the semi-controlled zone. The level of trust can be maintained by communicating over an unmanaged or externally managed communication channel using a virtual private network.

From Fig. 3 it can also be observed that the trust level needs to be incrementally increased by moving or transiting through each zone. By moving through each zone, a user or system session is subject to security mechanisms that enforce the trust model. Examples of this include stronger levels of authentications, intrusion prevention, increased logging and differing levels of message protection such as encryption and integrity controls. When moving between different communication channel management levels, for example, between a semi-controlled LAN segment and a management network used for the restricted zone, the connections must terminate both in the controlled and trusted zones before access to restricted services is available.

Security Zones may be further sub-divided into separate operating environments (micro-segmenting) for deployed applications and appliances. This will facilitate protecting the

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

overall security zone if one component within the zone is victim to compromise or security failure (i.e. minimize the possibility of an attack exploiting lateral movement within the zone). This can be achieved with techniques such as host based firewalls, hypervisor firewalling, or VLANs.

The following sections now describe further the zones in Fig. 2 and 3. These zones provide a high-level framework for defining network segments.

A. Zones with No Physical Measure

Two zones are classified with no physical measures, the uncontrolled and externally controlled zones. The uncontrolled security zone is any domain that is outside of the physical and logical control of the enterprise. Key examples include kiosks, touchscreens, or any device connected to the Internet such as personal computers. Access from an uncontrolled zone to systems in the controlled zone would typically be via the Internet, which is an unmanaged communications channel. Organizations and persons in the uncontrolled zone include those who would be legitimately accessing corporate systems or exchanging information with the enterprise on an ad-hoc basis and for which there are no specific agreements in place. Typical threats sources in this zone include hacking attempts, organized crime, rogue software, and malicious external users.

The externally controlled security zone contains business partner environments (primarily commercial) which connect to the protected enterprise for the exchange of information in order to provide or deliver services. This zone may include third-party hosted networks or websites and differs from the uncontrolled zone in that there is some level of trust established with the partner.

The protection of data by the business partner would be based on the use of secure communications and a range of security controls implemented within the third party's IT environment (for example, virus scanning of exchanged files). Entities that operate within this zone include retail service provider environment, ICT vendors, and system integrators internal environment. The enterprise will normally have a formal contractual relationship with these partner organizations to exchange information up to a certain data classification. This agreement would define a minimum level of security controls the external organization must have in place to protect data so as to obtain the required level of trust. The typical threats sources in this zone include rogue software, compromised systems, and malicious users from relevant organization.

B. Zones with Weak Physical Measures

A definition is given for the single zone that falls into the weak physical category. This is the semi-controlled zone, which may be considered the least trusted security zone within the enterprise's environment. This zone is effectively a controlled zone as it is owned, implemented, and managed by the enterprise, however due to the general physical access granted to users and systems it is the least trusted internal zone. An example of this is the corporate LAN where general staff, consultants, and end-user laptops can gain access to the network. Typical threats sources in this zone include rogue software, compromised systems, malicious users who are physically present on the premises, theft and malicious use by internal staff.

C. Zones with Strong Physical Measures

There are several zones that are situated under the direct control of the enterprise with strong physical measures. This includes the restricted, trusted, and controlled security zones. The controlled zone enables access from parties situated within the uncontrolled, externally controlled or semi-controlled zones to the protected business systems of the enterprise. The zone exists to allow legitimate external access to the corporate systems on a controlled basis while stopping access from non-legitimate parties. This zone can also further segregated on a per application or protocol basis, meaning that applications can be isolated from each other within this zone using routers or intermediate firewalls. This limits an attacker's use of one compromised platform/protocol to attack other systems. Systems in this zone should be considered as being vulnerable to attack and have appropriate controls and alarms in place.

Information assets in this zone will generally be limited to data of low sensitivity, which have a balanced requirement for confidentiality, integrity, and availability. The controlled zone also manages access from within the enterprise environment to outside networks and systems. There are effectively two main interfaces that the controlled zone has to less trusted zones; these are to uncontrolled zones and semi-controlled zones. Because these have significantly different trust levels, it is necessary to have multiple instances of the controlled zone, one for internal boundaries and one for external ones. The threats sources in this zone include hacking, organized crime, rogue software, and compromised systems.

The trusted zone is used to accommodate applications and systems that perform sensitive or an essential core business function. It is where most processing will occur and where frequently accessed data is stored. These applications use and store enterprise data and are accessed by internal staff via the controlled zone. Salient examples include business and operational support systems, management systems, and security controls. Connections to the trusted zone may originate from within the controlled or restricted zones. No access should be allowed directly from the uncontrolled, externally controlled and semi-controlled zones. Actors in this zone will include processes acting on behalf of authorized users, various corporate system, and application administrators. Threats to this zone typically include rogue software, incorrectly configured applications and systems, application design errors, data entry errors, some environmental threats and non-compliance with enterprise security policies. Assets within this zone may include the authentication processes and databases, the application processing of some of the web-based systems and most frequently used and accessed IT applications. Critical business data may remain in this zone for the period of time required to support an active session.

The restricted zone is characterized by allowing data access to only a small number of authorized users and services and is the most protected domain within the secured environment. Most critical assets are retained in this zone. This may include systems that play a master control or mission critical function

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

for the business. For example, this includes regulatory controls to private information, core banking systems, billing systems, payroll systems, network management systems, and security management systems. The restricted zone is a special class of zone as it needs to span control over all other zones that are deemed to be zones for management purposes. For instance, this zone will host the common security services required to support and administer security resources across all the other zones.

An object which has access to one secured area within the restricted zone is not necessarily granted access to other restricted zone areas. Access is also limited to a small group of highly trusted users and processes. Connections to and from this zone are intended to only originate from within the trusted zone. The actors in this zone include processes that operate on behalf of users, administrators and system operators and a controlled set of employees. Typical threats sources in this zone include rogue software, misconfigured applications, data entry error, application design errors, and internal threats.

VI. Scenarios in Practice

The proposed security zone model is analyzed further by applying several scenarios that are typical in practical deployments for the broader industry. Together with the classifier shown in Table I, these scenarios also demonstrate the typical deployment of technologies and business functions to the various security zones.

A. *Enterprise Web Application Access from the Internet*

In this scenario, users access a web application that is situated within the enterprise environment from over the internet. The zone in which users are located when initiating a connection is by default deemed to be uncontrolled or externally controlled. Communication will be via an SSL channel. The user experience commences with the user selecting a link or URL; they are then prompted with a login form. After entering their user ID and password, the credentials are validated. Upon successful validation, the user is permitted to interact with the desired application. By referring to Fig. 4, the following security controls and services are shown that are typically deployed to the zone or zone interface.

The inbound internet traffic enters the semi-controlled security zone (A) and is intercepted by the first security measure, a firewall gateway. At this point, scalable infrastructure to deal with expected load is deployed. Port and IP filtering is applied to allow connections to specified hosts n the controlled zone, with stateful inspection of all traffic. Quality of service is enforced to mitigate denial of service attacks. Explicit routing to user authentication proxies together with audit and logging is also carried out at this point.

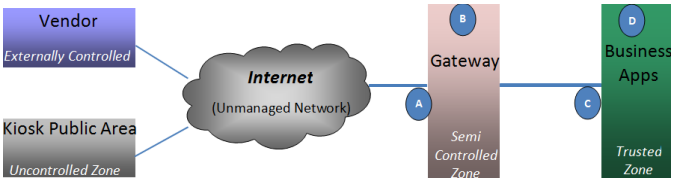

Fig. 4. Web Application Access: Externally Controlled to Semi-Controlled

Several gateways that carry out SSL termination, load balancing, Web application firewalling, user authentication, and application proxies are deployed at the semi-controlled zone (B). These security controls intercept all incoming traffic. Secure application code is also deployed and integrity controls for both application and platforms are engaged during access. Quality of service is also enforced to ensure that a compromised authentication node does not impact the availability of other shared infrastructure. Additional security mechanisms deployed include intrusion prevention, platform hardening, explicit traffic routing, and audit & logging systems.

At zone interface (C) appropriately sizes infrastructure to deal with expected load is deployed with port and IP filtering enabled to allow connection to specified hosts within the controlled zone. The stateful inspection of traffic is carried out with measures to ensure a quality of service to mitigate compromise to shared infrastructure. Explicit routing of traffic is managed between the user authentication node and backend application servers with connections granted only from known sources in the semi-controlled zone. Application audit and logging is also carried out.

The business applications within the trusted zone (D) will only accept connections from the recognized authentication node deployed to the semi-controlled zone (B). Platforms are hardened and accessed via the default gateway at the interface (C). Application platforms are generally deployed in a manner that segregates them from other applications in this zone to manage any potential compromise. Authentication services are also deployed in this zone such as directories (i.e. LDAP) together with audit and logging.

B. *Web Application Access from Internal Network*

In this scenario, an application in the trusted zone is being accessed by an actor on a network situated within a semi-controlled zone. Referring to see Fig. 5, a connection to an application will traverse both a managed network (e.g. a third party network) and an externally managed channel (i.e. the Internet). Although the zone in which users initiate a connection from is a managed network with a level of trust, since all users are accessing the enterprise application over the internet, the default trust level is uncontrolled.

The user experience is similar to the previous scenario where they are prompted for username and password for authentication. Communication will be conducted over an SSL encrypted link.

Since the users accessing the business application will operate from a semi-controlled zone, there are controls that can normally be deployed at the interface to the semi-controlled zone (A) to establish a certain level of trust. Similar to the previous scenario, physically separated gateway devices are deployed to deal with inbound connections from the Internet with appropriately sized computer hardware infrastructure to deal with projected load. Port and IP filtering is deployed to allow connections to specified hosts in the controlled zone, with stateful inspection of inbound traffic. Quality of service measures are in place to mitigate against denial of service attacks, with explicit routing to the authenticated node, together with audit and logging.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

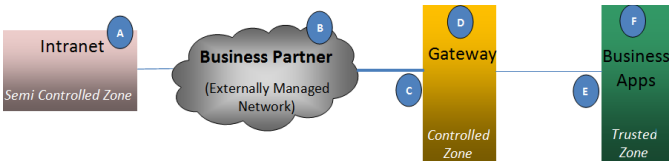

Fig. 5. Web Application Access: Semi-Controlled to Trusted Zone

Traffic is routed through the third party network and via the Internet, shown at (B). Controls may be in place at the external managed third party network; however, as mentioned previously since this shall travel via the Intranet the default level of trust is assumed to be uncontrolled.

At interface (C), inbound Internet traffic enters the controlled zone and is intercepted by a firewall gateway. Port and IP filtering is carried out with deep packet inspection. Routing rules are also applied to enable connections to the specified hosts in the controlled zone. Similar enforcement for quality of service and preventing denial of service attacks apply.

Security controls deployed to the controlled zone (D) are extensive and include SSL termination, load balancing, web application firewalling, intrusion prevention, user authentication service, application, and platform integrity controls. In addition, quality of service mechanisms will be present to ensure that a compromised authentication node or proxy cannot impact the availability of other shared infrastructure. Other typical measures will also include hardened platforms, explicit routing, secured application code, and audit and logging.

At interface (E) technology is deployed for managing inbound traffic. This includes infrastructure to deal with load, port and IP filtering to allow connections to specified hosts in the controlled zone, stateful inspection of traffic, quality of service to mitigate compromise to shared infrastructure, explicit routing between user authentication node or proxy and backend application servers. In addition, connections only from known sources are permitted in controlled zone.

Within the trusted zone (F), security and network controls are configured to only accept connections from the designated authentication node via the default gateway at the interface (E). Applications are segregated from other application within this zone with other security services deployed such as audit and logging.

C. Security Zone Classifier

In this section, a security zone classifier is proposed that can be used to assist security architects when determining which security zone to deploy IT applications and network appliances. The classifier is not intended to be prescriptive but rather a guide for the overall decision making process in deployment. Table 1 shows where a class of business applications may be deployed in the security zone. For example, a self-service web application can be deployed to the uncontrolled, semi-controlled, and externally controlled zones. The table can also be used to view applications from a technology or vulnerability perspective to determine security zone. For instance, an application that is vulnerable to insider attack may be deployed to the trusted or restricted zones, offering a higher level of protection from network access.

VII. Discussion and Further Work

In this paper, a security zone model is presented that may be used as a blueprint for security architects and engineers when designing threat management strategies. Also illustrated is how to apply the blueprint in practice, with several case study scenarios given, together with a classifier that can assist architects in the zone placement of IT applications. With the escalating demand for mobile access to corporate services and greater adoption of cloud technologies, the importance of secure access to systems will increase. We have observed that in some instances the development and classification of new

TABLE I. Security Zone Classifier

	Mission Critical	*Regulatory influence*	*Security System*	*Core Infrastructure*	*Pilot*	*Business Partner*	*Business Support*	*Operational Support*	*Data Sensitivity*	*Commercial Sensitive*	*Self Service Web App*	*Proxy/Gateway*	*Vulnerable to Attack*	*Service Denial*	*Insider Attack*	*Failover Protection*	*Strict Service Level*	*Physically Secured*	*Mobile Technology*
Zone	*Business Application Classifiers*												*Technology & Vulnerability*						
Restricted	✓	✓	✓	✓			✓	✓	✓	✓			✓			✓	✓	✓	
Trusted			✓	✓		✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	
Controlled			✓	✓	✓	✓	✓	✓	✓	✓			✓	✓		✓			✓
Semi-Controlled			✓	✓	✓	✓					✓	✓	✓	✓		✓			✓
External Control			✓		✓	✓					✓	✓							✓
Uncontrolled			✓		✓						✓	✓							✓

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

security zones within an organization may become unbounded, with numerous zone model variations appearing. This makes deployment decisions more difficult without clear understanding for the co-deployment of IT Applications and security controls. By establishing a set of principles and a cyber security zone model blueprint, the basis for extending and refining the security protection zones may be conducted on a technical basis to support zoning decisions. This will help to stabilize the proliferation of security zones into a more manageable set of discrete domains

There is further work to classify the full range of IT technologies deployable to security zones. In addition, the range of security controls that extend the capabilities of the security zone requires further consideration as to their placement. It is also suggested that further zoning scenarios may be documented as design patterns to assist security architects in building protection systems. Finally, the corollary to implementing multiple security zones is that too many zone increments, for traversing applications, may impact business workflow and performance. Hence, the deployment of security controls and IT applications requires consideration with respect to the overall security posture desired and business need for application performance.

ACKNOWLEDGMENT

We wish to thank Mark Roeder for his helpful feedback and discussion on this paper. Any views or opinions expressed in this article are the author's own and do not necessarily reflect the view of the Commonwealth Bank of Australia.

REFERENCES

[1] A. Gontarczyk, P. Watson, et al., "Towards an Enterprise Security Architecture for Broadband Network Providers," *Journal of Enterprise Architecture*, The Open Group, Vol. 8, No. 3, 2012.

[2] A. Gontarczyk, P. McMillan, and C. Pavlovski "Cyber Security Zone Modeling in Practice", *Proceedings of the 10th International Conference on Information Technology and Applications* (ICITA), Sydney, Australia, 2015.

[3] S. M. Bellovin, "Distributed firewalls", *Journal of Login, Special Issue on Security*, pp. 37–39, November 1999.

[4] T. Markham and C. Payne, "Security at the Network Edge: A Distributed Firewall Architecture", *Proceedings of DARPA Information Survivability Conference & Exposition II (DISCEX '01)*, 2001, pp. 279–286.

[5] V. Ramsurrun and K. M. S. Soyjaudah, "A Stateful CSG-based Distributed Firewall Architecture for Robust Distributed Security", *Proceedings of the 1st Communication Systems and Networks and Workshops (COMSNETS 2009)*, IEEE, Jan 2009, pp. 1–10.

[6] L. Cai and X. Yang, "A Reference Model and System Architecture for Database Firewall", *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*, Oct 2005, pp. 504–509.

[7] J. Tan, D. Abramson, and C. Enticott, "Firewall Traversal in the Grid Architecture", *Proceedings of the 12th IEEE International Conference on High Performance Computing and Communications*, Sept 2010, pp. 189–196.

[8] J. Lobo, M. Marchi,and A. Provetti, "Firewall Configuration Policies for the Specification and Implementation of Private Zones", *Proceedings of IEEE Symposium on Policies for Distributed Systems and Networks*, July 2012, pp. 78–85.

[9] J. Chomicki, J. Lobo, and S. Naqvi, "Conflict Resolution Using Logic Programming", IEEE Transactions on Knowledge and Data Engineering, 2003, pp. 244–249.

[10] J. Jee, J. Jang, I. Jo, and Y. Shin, "Network Partition Scheme to Protect Secure Zone for Malicious Code", *Proceedings of the International Conference on Information Networking (ICOIN)*, Jan 2013, pp. 476–480.

[11] Y. Chao, C. Bingyao, D. Jiaying, and G. Wei, "The Research and Implementation of UTM", *Proceedings of IET International Communication Conference on Wireless Mobile and Computing (CCWMC)*, Dec 2009, pp. 389–392.

[12] S. Ali, M. H. A. Lawati, and S. J. Naqvi, "Unified Threat Management System Approach for Securing SME's Network Infrastructure", *Proceedings of the International Conference on e-Business Engineering*, IEEE, Sep 2012, pp. 170–176.

[13] Defense in Depth, National Security Agency, http://www.nsa.gov/ia/_files/support/defenseindepth.pdf.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731