Security Zones

Jesse Ybarra

North American Sales

October 29, 2018

Executive Summary

As security technologies grow more complex the administrator has many tools at his or her disposal to regulate and enforce traffic in firewall devices. While security zones are not new tools, an individual may underutilize the objects in daily activities. This paper attempts to explain what a security zone function in a firewall and how it applies to modern security techniques. The key benefits to a security zone is tight control of traffic and routing functions while maintaining simplified control.

Demographics

The author assumes the audience is familiar with security terms in Information Technology. The audience should consist of those who manage, configure, or operate firewall devices. The individuals should have medium-level knowledge of security terms. Common use terms are as follows but not limited to:

- Routing – the process of selecting a path in a network to move traffic across
- Packet – a piece of information transmitted across a network
- Firewall – A device that controls traffic to and from a network
- Stateful Firewall – a technology that tracks connections through the device
- DMZ – Demilitarized Zone where traffic is regulated and shared between an external and internal network

Security Zone

As firewalls have evolved over the last couple decades, there have been many ways to implement firewall policy. The technology touched on specifically in this paper is the use of the stateful firewall. Several key firewall technologies include object-oriented firewalls, interface based firewall, and zone based firewalls. In terms of securing an environment, it is said that there is no determination on which type of firewall is most secure as there are a handful of different types.

"The Check Point firewall was one of the largest game changers in firewall history. It came along at a time when most people believed a firewall was nothing more than a piece of wood inside a wall," (Cameron, Woodberg, Giecco, Eberhard, & James, 2010). Object-oriented firewalls, such as the technology created by Check Point Software Technology, inspects traffic as it crosses the backplane of the device. The firewall processes the packet as it pertains to the security before it performs a routing query.

Interface firewalls, such as the technology that Cisco implements, inspects traffic on the interface; this allows security policy to wrap around the interface. Two policies are created in a legacy interface base model. One policy is created to allow the data packet to reach the interface and one to allow the packet through the interface.

Lastly, an alternative firewall technology is a zone-based firewall. A zone-based firewall allows an administrator to wrap a single policy from one zone to another. This is a simplified policy compared to interface based firewalls and object oriented firewalls.

Juniper Networks uses technology in their firewalls that are an example of a zone-based technology. "A security zone is a logical construct that contains one or more interfaces, and zones are used to create a direction between two different areas of the network," (Cameron, Woodberg, Giecco, Eberhard, & James, 2010). Security zones are associated with trust. "A security zone (specifically, the Sec(L3) from the preceding output, which is a Layer 3 security zone for firewalls operating in Layer 3 mode) represents a logical area of trust within the firewall," (Brunner, et al.,

2008). An interface is assigned to the zone to control routing and applies security policy as packets enter and leave the zone. When a policy is created there is a source zone and a destination zone added to the security database lookup. This predefined requirements helps streamline security policy lookup.

In object oriented firewalls and interface based firewalls, policy databases could become extremely large and highly complex. Often, this leads to administrators spending countless cycles optimizing rule bases and deleting unused policy after rigorous audits are performed. This leads to efficiency of the rule base going down as the rule count goes up. The administrator must constantly tune a large firewall database if policy maintenance is not kept up.

A zone-based firewall policy's database can grow very sizeable in scale. When accessing the rule base, a look-up is performed on the routing, zones, and other attributes. Nevertheless, if the rule base is over one thousand rules, but the zone-to-zone output reveals only ten policies the lookup is fast. This allows the administrator to look at the rule base quickly and proficiently. Zone-based firewalls, just like other firewalls have a global drop rule. A technique used by an administrator is to apply a zone-to-zone drop rule and log the output. As an example a zone-based firewall has an Internal zone and External zone. There may be several policies between Internal and External but the last policy read in the database is a drop rule with a log option. This allows the administrator to see if the packet made it through the entire zone-to-zone lookup before being dropped and logged.

With all of the positives to zone-based firewalls, they do have a couple drawbacks. In large-scale enterprises, routing must be correct and in place for zones to work. Management of zone-based firewalls will lend well to local management instead of a distributed management tool. Each zone should be unique to each firewall unless they have a common network, such as an internal network. As more zones are created on the firewall, the zone-to-zone rule grows. As an example, one rule-set exists with an Internal zone to External zone. The moment you introduce a demilitarized zone or DMZ, the zone-to-zone rule-set grows in complexity. An administrator will have to write one rule-

set from Internal to External and another rule-set from Internal to DMZ. A public DMZ will have another rule-set written for External to DMZ. If the servers in the DMZ need to talk to the Internet, another rule-set is written from the DMZ to the External zone. Therefore, just by adding one zone to the rule-set, it went from one to four in the database. Zone-based architecture must be well thought out before implementing or the administrator runs the risk of the rule base becoming very complex.

With the invention of Check Point's layer based approach, zone-based firewall technology has taken a step forward into controlling access. Check Point introduced inline layers with a concept of parent and child rules. The inline layer does not necessarily need a zone assigned to the source and destination column, but it can help. When an administrator assigns the parent rule with a source zone and a destination zone the logic becomes straightforward. The parent rule acts like a drain and sucks the packet into the inline layer. The administrator begins to create child policies that allow traffic to be permitted or dropped based upon the entity's needs. This ability brings the control and efficient lookup process to a Check Point firewall. Going a step further the administrator can assign software blades, such as Intrusion Prevention System or IPS, to these zones. One zone-to-zone communication may need an application and content software blade for Layer-7 inspection. Another zone-to-zone communication may only need Layer-4 firewall technology for machine-to-machine communication. This type of control allows a Check Point engineer to control, optimize, and accelerate the traffic on a case-by-case basis.

In closing, security zones are a logical entity that control access and allow an administrator to enhance the efficiency of the rule base. The zone is bound to an interface to allow routing decisions. There are many choices the firewall must make to process every packet. Zones are a tool used in the arsenal of an administrator to secure an entity's assets. Object oriented firewalls and zone-based firewalls alike can be implemented to provide a good solution for all organizations that choose to implement said technologies. Most manufacturers have crossed over the line to create a hybrid approach to their setup and incorporated the best of both worlds in terms of how they conduct

business. Juniper has detached from local address books and gone to global address books in their approach to allow a more object oriented view. While traditional object oriented firewalls, such as Check Point, have adopted zones in their bag of tricks. Zones are simply another tool that an administrator can put into practice to efficiently manage their security stack.

Reference

Brunner, S., Davar, V., Delcourt, D., Draper, K., Kelly, J., & Sunil, W. (2008). *ScreenOS Cookbook.* O'Reilly Media.

Cameron, R., Woodberg, B., Giecco, P., Eberhard, T., & James, Q. (2010). *Junos Security.* O'Reilly Media.

