Replacing Abstract Zones with Real Application Security Policy

Abstract zones have evolved as a way to reduce the difficulty of managing a complex and expanding set of firewall rules.

White Paper

Introduction

As the number of firewall rules used by many IT organizations has grown over time, abstract zones have evolved as a way of reducing the complexity of managing those rules. Yet zones do not prevent the accretion of orphaned firewall rules; they merely mask it to the point where the global rule set is eventually littered with "junk DNA" that may or may not still have a purpose.

At the same time, today's IT organizations are recognizing the benefits of differentiating in-bound application traffic from out-bound user traffic. Next-generation firewalls have enjoyed widespread deployment to provide management of user-initiated, out-bound connections. In the other direction, Application Delivery Controllers (ADCs) have specialized in providing the intelligence to route, load balance, inspect, analyze (secure), and modify in-bound application traffic.

The advent of the application delivery firewall, with its deep integration within an organization's business and e-commerce applications, is the logical evolution of an application-centric, in-bound approach. As organizations have attached intelligent policies—regarding rate-shaping, load balancing, network optimization, and acceleration—to their applications at the ADC, the ADC has become the de facto gatekeeper for access to those applications.

The final step in this evolution is the attachment of firewall policy directly to the application configuration at the ADC. This new approach to managing firewall policy at the in-bound application level approach is called application-centric firewall policy management, and it offers surprising benefits compared with traditional zone-based firewall policy management. Organizations embracing the application delivery firewall solution, either for use in a split-traffic model or for a purely inbound, unmanned data center, are finding that an application-centric firewall policy is superior to traditional zone-based policy when manageability, performance, and granularity are priority issues for a data center's inbound traffic management.

What Is Application-Centric Firewall Policy Management?

The application-centric firewall policy management approach is a method of attaching firewall policies directly to the application. It may be defined as a logical collection of virtual addresses, server pools, and communication profiles that comprise all the configuration necessary for optimal application delivery. This approach delivers the most benefits when the application configuration is created by a template that leverages a recommended security policy, such as might be developed by the organization's own security team.

The configuration of the application-centric (or app-centric) firewall policy is relatively familiar because the policy is defined against a context. For conventional firewalls, the context is a zone and/or a 5-tuple. For app-centric policy, the context is the application itself. The application context, richer in attributes and objects than a 5-tuple, enables a richer network security policy.

In the web application firewall (WAF) market, there is no controversy in attaching WAF security policy to the application. Application-centric firewall policy management can work the same way for network security (that is, security at layers 3 and 4 of the OSI model).

Why an App-Centric Policy Trumps Zone-Based Policy Management

Applications running across networks encounter a wide range of performance, security, and availability challenges. These problems cost organizations an enormous amount in lost productivity, missed opportunities, and damage to reputation. Fortunately, the application-centric approach can reduce these challenges and streamline firewall policy management by enhancing manageability, improving performance, and delivering more granular visibility.

Manageability

As data centers have grown to encompass hundreds and thousands of applications, so have the complexities of managing firewall policies. The situation has become complex enough that a team of policy operators cannot easily manage the rules for so many in-bound objects. Traditional firewalls initially solved this problem by introducing zones, with rules set for a zone and then objects (applications) grouped into these zones based on their firewall needs. Over time, however, zones are prone to the accretion of orphaned firewall rules—rules that linger in the security configuration even after their associated applications are retired, since removing rules is always harder than adding them. A security policy focused on applications is a better approach.

Unlike zones, which are artificial abstractions, applications are concrete groupings of firewall objects where the real business logic, commerce, and day-to-day communication of the organization take place. When each application includes the definition of its own security policy, there is no need for an extra abstraction layer that needs its own management and maintenance, as a traditional zone does. Herein lies the intrinsic value of an app-centric policy management approach: firewall policies are attached to the business application already being managed for its own sake, rather than to an artificial construct that imposes its own management burden and more easily becomes outdated.

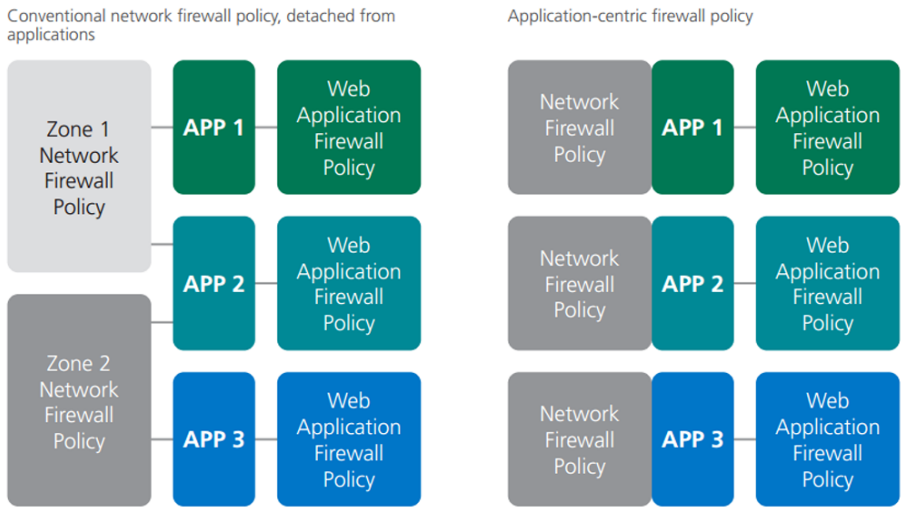

Figure 1: Application-centric firewall policies ease management by linking security policies more directly with each application.

Reducing misconfiguration

In addition to making management easier, the reduction of abstraction has a tangible security benefit, too. Firewall misconfiguration is the leading vector for network breaches. By using an integrated platform with a focus on application delivery, security administrators can much more easily create accurate rules for all applications. This is because the platform configuration template already contains the pre-configured destination IP, destination port and service, and pools and monitors. Testing and troubleshooting are also simpler because instead of dealing with two platforms (the ADC and the firewall), a security administrator only needs to deal with one.

Reducing work per application

To understand a specific example of how the application-centric approach improves manageability, consider the cost of manual work per application. The app-centric approach reduces this workload through the creation of reusable application templates that include pre-defined firewall policies. When applications are created from the template the associated firewall rules are automatically created, saving both the application and network security teams work. The application team doesn't have to change the way they work. The security team doesn't need to continually handle requests to open a tuple on the firewall and define logging as applications come and go.

Helping the auditor

In another example of greater efficiency, using application templates to configure the app-centric firewall policy enables an administrator to assist the auditor by simplifying the information the auditor must review. The auditor can look in a single place (the template) on a single device to see the definition of the firewall rules and the application configuration. From the auditor's perspective, there is a single pane where the configuration for each application (including certificates) can be audited.

Performance

Every firewall administrator for a large organization has been faced with the issue of performance as it relates to firewall rule-set ordering. Most experienced administrators have found that they had to reorder a firewall rule-set to bring performance back to an acceptable level after a change. Certainly some of the performance degradation is a result of the policy bloat common to zones. The remainder is due to the fact that firewalls—even those that perform policy compilation—do not attempt to optimize rule performance with the behavior of the underlying applications in mind.

Application-centric firewall policy management, on the other hand, does not suffer from these drawbacks. All other things being equal, smaller rule-sets perform faster. The abstract nature of zones discourages the proper pruning of stale rules, and as a result, global rule-sets grow unbounded. In the app-centric approach, as applications are retired, their security policies are automatically retired with them. This helps avoid the problem of orphaned firewall rules that are not owned by anyone, yet everyone is afraid to remove, and thus ensures smaller, faster rule-sets over time.

Another performance consideration addressed by the app-centric approach is optimization. In this approach, optimization is improved because the underlying firewall can optimize around a discrete object (the application), not an abstract collection. Performance therefore becomes bounded by the application delivery architecture, not the zone where policy is attached to abstraction.

Granular Visibility

Application teams and security teams often must work together to debug an issue between the firewall and the ADC behind it. Frequently the application team will tell the firewall team that the application isn't receiving traffic from a certain user, and then the two teams wrangle over packet-captures in non-real time, wasting time on a lengthy and tedious back-and-forth procedure.

Application-centric firewall policies, on the other hand, offer the security team the ability to send the logging data for the specific application, in real-time and for that application only, to the application's management team. This allows the application team to immediately assist in the diagnosis of rule exceptions, run tests, and observe the outcome.

Zone-based firewall policies have no ability to instrument logging parameters at a per-application granularity. Consequently, the more granular visibility provided by app-centric firewall policy management—not just to the security teams but also the application teams—leads to faster issue resolutions for users and less work for both teams.

Logging applications

For a real-world example of the power of more granular visibility, consider an enterprise security team that has worked with two different stakeholders to create a security policy for two applications used by the enterprise, such as Microsoft Exchange and Microsoft SharePoint. These stakeholders may have their own preferred methods and software tools for collecting and reporting information, which differ from the method the security team uses to collect traffic logs from the entire firewall. Both the Exchange and the SharePoint teams want visibility to the traffic on their application, but the Exchange team already uses Splunk to report on their application environment, for instance, while the Sharepoint team has heavily invested in ArcSight. With the app-centric approach, logging data for each can be provided by the ADC without manual intervention by the security team or manipulation of logging data to make it suitable for either Splunk or ArcSight.

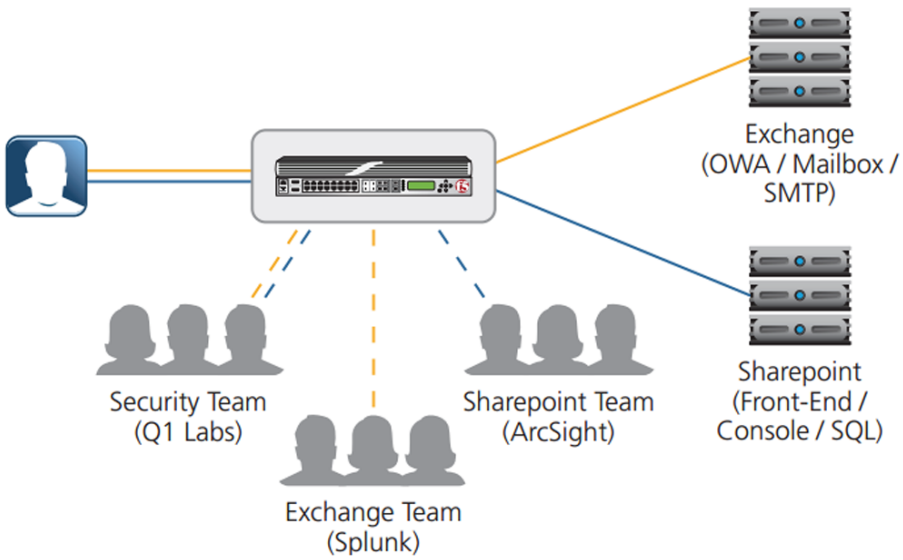

Figure 2: More granular logging helps teams work independently and together in real time.

Service provider efficiency

Another significant example of the benefits of the application-centric approach can be seen in communications service provider industry, where service providers manage hundreds or thousands of applications for their downstream customers. By attaching firewall rules directly to each application, the service provider avoids any need to migrate each customer's security zone abstraction into its own, potentially saving considerable time and complexity.

Conclusion

At the end of the day, increased visibility and manageability saves an IT organization time and operational expense, as well as the opportunity cost associated with each. Until now, the organizations that have benefited from an application-centric approach to firewall policy management have done so out of happenstance, as a valuable byproduct of adopting an application delivery focus. A more deliberate consideration of app-centric firewall policy management, however, can bring the same benefits to more enterprises.

More and more organizations are splitting how they manage in-bound versus outbound traffic, giving each direction of traffic the scrutiny it deserves and optimizing the security approaches to each. As this trend continues, more companies are also beginning to recognize the benefits of a capable ADC, not just for application delivery per se, but also to enable application-centric security policy, both at the ADC and at the security perimeter itself.

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com