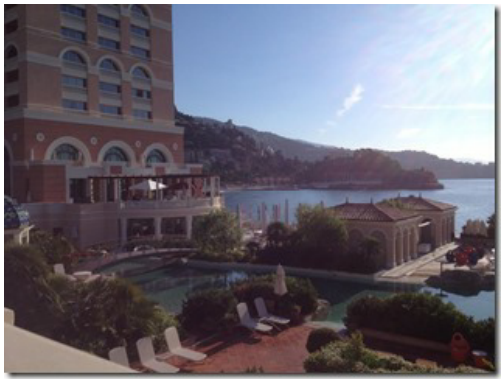
F5 Firewall Like No Other - Ruling the Application

David Holmes, 2013-19-06

“Vive la différence!” I’ve been here in Europe at our Agility Conference in Monte Carlo (the theme: GO BIG) talking with customers and partners about what makes the F5 firewall different.



F5’s European Conference at Monte Carlo Bay, Monaco

Old School Excel

As I made my presentation to a packed room of customers, I noticed that one story really got them nudging each other.

We had an early customer of the **Advanced Firewall Manager** (AFM) module. This customer used to organize their firewall rules in an old-school way – with an Excel spreadsheet. The spreadsheet was 300 pages long! This is how that happens:

Imagine a new firewall operator. A bizdev team builds a new application and asks him to open a hole in the firewall for it. He checks, and sees that there is already a working rule for an existing marketing application, so he doesn’t create a new one.

Six months later, the bizdev application is retired, and he is asked to remove the firewall rule. By now he has forgotten that he didn’t create a rule for this application and he removes the one that is there. This stops traffic to the original marketing application as well. When the marketing team realizes that they have stopped receiving traffic, they come and yet at him.

He quickly learns that it is “**safe**” to create a firewall rule but “unsafe” to remove one. This is the opposite of good security posture but it is a scenario that many, many, many organizations face today. This explains why so many in the audience were nodding and nudging each other.

Ruling the Application

The reason that F5’s firewall is different is because **we build the application firewall rule into the application itself**. It is part of the definition of the application, right there next to the http options, the pool definition and the tcp profile parameters.

```
ltm virtual bizdev1 {
    ip-protocol tcp
    pool bizdev_pool
    profiles { http tcp }
    fw-rules {
        reject1020 {
            action reject
            log yes
            source {  addresses {  10.128.20.0/24 } }
        }
        allow_http {
            action accept
```

```
            action accept
            destination { ports { http } }
            ip-protocol tcp
        }
    }
}
```

When the application is retired, the associated firewall rules are automatically retired with it.

This has three benefits.

1. **No accretion of stale rules**. While the initial management overhead may be the same for defining the network, over time the active set of firewall rules will remain identical to the active set of applications.
2. **Performance.** This automatic pruning process will have performance benefits because, as firewall operators should know, the smaller the rule set, the faster the firewall.
3. **Application Mobility.** As applications moves between datacenters and/or clouds, the firewall rules move with them. This makes application migration easier and less error prone.

Changing the Firewall World

That's just one way that F5 is changing the firewall world. There are other benefits associated with this "application-centric firewall policy management." If you want to see them all in one place, check out the white paper: "Replacing Abstract Zones with Real Application Security Policy."

Connect with David: Connect with F5:

Related blogs & articles:

Whitepaper: Replacing Abstract Zones with Real Application Security Policy
Whitepaper: The New Data Center Firewall Paradigm

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

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com