



BorderWare Creates iRule™ That Provides Enhanced Threat Protection and Dramatically Reduces Incoming Traffic Volume For A Significant Cost Savings

“Using a very basic iRule, we can provide our customers with considerable value in terms of cost savings by reducing the total incoming traffic by more than 50 percent.”

Peter Cox
Vice President of Product Management

Industry:

Network Security

Challenges:

- Block email attacks
- Reduce costs

Solution:

Integrate BorderWare MXtreme Intercept Engine with F5's BIG-IP device using iRules

Benefits:

- Reduce the amount of mail connections entering an organization's network
- Increase QoS
- Improve available bandwidth
- Significant savings on network bandwidth and processing

Overview

BorderWare Technologies, founded in 1994, is an F5 technology partner headquartered in Canada. The company provides perimeter and application-specific firewalls for email and SIP that are designed to mitigate the risks and threats associated with Internet communications.

Recognizing the need for products that ensure high availability as well as robust security, BorderWare and F5 Networks developed a joint solution for enterprise email management. By combining the patented stateful failover of BorderWare's MXtreme Mail Firewall with F5's BIG-IP Application Delivery Networking system, enterprises can achieve unprecedented levels of email availability, reliability, scalability, and security.

Challenge

The volume of unsolicited and/or malicious email traffic hitting an organization's network has risen by over 300 percent in the last year alone. Email attacks, such as spam, Denial of Service and Directory Harvests, can account for over 80 percent of an enterprise's inbound mail traffic .

BorderWare's MXtreme Mail Firewall is an email security appliance that detects and blocks a variety of threats and malicious

content on an IP basis using several techniques through the MXtreme Intercept Engine. Blocking incoming threats locally on the MXtreme system is useful, but it can do little to stem the flood of malicious traffic entering the network if the system is positioned far from the perimeter.

Local blocking is not as effective at detecting and responding to incoming threats; it ties up connections on the email server and doesn't provide protection for other servers and services in the DMZ. As email volumes increased, customers found it more and more difficult to handle the sheer volume of incoming mail connections on the MXtreme system.

Solution

BorderWare recently released the MXtreme Intercept Engine that includes powerful threat detection and response capabilities that works seamlessly with F5 BIG-IP devices for greater control and value.

By integrating MXtreme with a F5 BIG-IP device, organizations can block threats at the true perimeter of their network. BIG-IP is based on F5's unique Traffic Management Operating System (TMOS) which features iRules, an application-fluent technology that enables organizations to quickly and easily





write custom commands to define how F5 products secure, optimize and deliver any bi-direction IP traffic or flow.

BorderWare built a series of SMTP Threat Detection and Response iRules that enable threat information recognized by the MXtreme to be pushed to the F5 BIG-IP device. The threat information consists of separate lists that contain IP addresses that are known to be malicious or suspicious in nature. These IP addresses are put into data groups that are then fed to the F5 Big-IP system using iControl – F5's SOAP/XML based API - where a series of iRules applies rate shaping, intelligent SMTP rejects, and more.

This enables an F5 BIG-IP to provide proactive perimeter defense for incoming email traffic to better enable organization's ability to protect themselves. By providing this IP block list to the F5 device, MXtreme allows the F5 BIG-IP system to block unwanted mail connections at the network edge.

Specifically, BorderWare applied a simple iRule to each data group mirrored from the MXtreme Mail Firewall that checks, at TCP connect time, if the IP belongs to the data group. If so, it either issues a TCP reject statement and then drops the connection or puts it into a pool for rate shaping or other network traffic management functions.

Benefits

The iRule helps to reduce the amount of mail connections entering an organization's network by blocking over 80 percent of all email attacks at the BIG-IP device. Reducing the overall amount of incoming traffic helps to increase

QoS on the company's network, improve available bandwidth and reduce the overall amount of traffic hitting the MXtreme system. Less traffic arriving at the MXtreme system ensures that it has the resources available to deal with the customer's legitimate business-critical email traffic and not waste time processing unwanted mails such as spam and viruses.

This allows for significant savings on network bandwidth and processing for an organization and a significant reduction in the resources required to administer the email infrastructure. If email attacks represent 80 percent of all inbound email and total email traffic accounts for 60 percent of an organization's inbound traffic volume, then an MXtreme system using the SMTP Threat Detection and Response iRules created by BorderWare can enable an F5 Big-IP to block up to 50 percent of all inbound traffic. This means that an organization's network has to process, log and manage half the traffic it had to deal with prior to deploying these BIG-IP iRules.

The iRule was built in less than a day, according to Peter Cox, Vice President of Product Management at BorderWare, though it took several months work on the MXtreme system to enable it to recognize threats and store the information in such a way that the F5 system could use it. Once this was done, the integration with the F5 device through the iRule was relatively easy to do.

"Using a very basic iRule, we can provide our customers with considerable value in terms of cost savings by reducing the total incoming traffic by more than 50 percent," said Cox. "Working with the F5 DevCentral team, we were

able to easily deliver an enhancement to our product that increases security, saves on network bandwidth and improves performance without the associated administrative overhead."

BorderWare's "SMTP Threat Detection and Response" iRule entry was recognized as the first place winner/partner division in the first annual "iRule, Do You?" contest sponsored by F5. Entries in the iRule contest were evaluated on a weighted scale for innovation, creativity, and business applicability by a panel of leading industry press and analysts, as well as the F5 DevCentral team of iRule experts.

"This is a great use of both iRules and F5 along with a third-party" said contest judge Ronald Schmelzer of analyst firm ZapThink. "In fact, this is what Web Services are all about."

See the following page for the iRule code.

**iRule Code:**

```
when CLIENT_ACCEPTED {
  if {[matchclass [IP::remote_addr] equals $::harvesters] } {
    TCP::respond "550 Message Rejected - Too many unknown recipients\r\n"
    drop
  }
  if {[matchclass [IP::remote_addr] equals $::spammers] } {
    TCP::respond "550 Message Rejected - Too much spam\r\n"
    drop
  }
  if {[matchclass [IP::remote_addr] equals $::blacklisted] } {
    TCP::respond "550 Message Rejected - client blacklisted\r\n"
    drop
  }
  if {[matchclass [IP::remote_addr] equals $::infected] } {
    TCP::respond "550 Message Rejected - Infected\r\n"
    drop
  }
  if {[matchclass [IP::remote_addr] equals $::tarpit] } {
    pool slow_rateclass
  }
}
```

F5 Networks, Inc.
Corporate Headquarters
401 Elliott Avenue West
Seattle, WA 98119
(206) 272-5555 Voice
(888) 88BIGIP Toll-Free
(206) 272-5556 Fax
www.f5.com
info@f5.com

F5 Networks
Asia-Pacific
+65-6533-6103 Voice
+65-6533-6103 Fax
info.asia@f5.com

F5 Networks, Ltd
Europe/Middle-East/Africa
+44 (0)1932 582 000 Voice
+44 (0)1932 582 001 Fax
emeainfo@f5.com

F5 Networks
Japan K.K.
+81-3-5447-3350 Voice
+81-3-5447-3351 Fax
emeainfo@f5.com