McAfee®

Eight "Must-Have" Firewall Rules

With the torrent of new threats resulting from Web 2.0, it's likely that your existing firewall is leaving you exposed. This checklist should help you understand the advanced features available in next-generation firewalls and guide your evaluation process. We contrast aging, end-of-life, or technically deficient systems from vendors such as Cisco and Check Point with the next generation McAfee® Firewall Enterprise V8 appliance. If you are facing a "forklift" upgrade, this list should help you get the greatest benefit from your investment.

Rule 1—Fine-Grained Control Requires Visibility and Enforcement Tailored to the Interactions of Users and Web 2.0 Applications

Since the majority of today's traffic uses HTTP (port 80) and HTTPS (port 443), you need to be able to look inside these protocols and ports and deeply inspect the traffic itself, including encrypted traffic. Encryption is a common cybercrime tactic today. Client-side attacks targeting vulnerable web browsers and using encrypted connections traverse Cisco's firewall without being decrypted and inspected, leaving networks completely unprotected.

To exert control, you should be able to uncover what's happening, such as Skype activities, within the context of who is using each application. This perspective lets you define rules that cater to business needs by matching the user, the context, and the sophisticated web applications that are necessary and appropriate. For instance, you may want to allow IRC chat while blocking FTP operations for the customer service organization behind the web service portal. You may want to allow Yahoo searches but block Yahoo mail and instant messaging applications. And you may want to block access to risky or inappropriate websites unless you receive a genuine business case for a specific user community—at which point you must be able to implement that policy with a relevant rule.

Advanced next-generation firewalls like the McAfee Firewall Enterprise appliance give you visibility into your application traffic, including inbound and outbound encrypted traffic. While Cisco only decrypts VoIP traffic so it can travel through its firewall, McAfee actually inspects SSH, SFTP, and HTTPS traffic for malicious content. Check Point cannot peer inside encrypted traffic at all.

We go beyond application control so you can enforce policies on inbound and outbound activities at the user level. This approach allows you to create precise, accurate application rules that work for your business based on the user groups that already exist in your Microsoft Active Directory or LDAP directory. This application and user awareness means fine-grained control with less maintenance hassle.

Rule 2—Multivector Threat Protection Shouldn't Cost Extra

Over the years, the lack of granular inspection and defenses within firewalls has resulted in a variety of layered or bolted-on protections. Some architectures force you to choose between protections. With Cisco, you have to decide if you want anti-virus or intrusion prevention on a specific system. Other vendor's firewalls lack integrated security offerings, forcing you to buy additional point solutions.

Naturally, every separate product bears obvious capital and operational costs—from purchase through maintenance and separate subscription renewals. But they also carry some hidden costs. For instance, Check Point activates protections—such as intrusion prevention system (IPS) signatures—globally, rather than per rule, a big demand that takes a big toll on performance. Some Check Point users choose to turn

From IRC to P2P to HTTP

"Recently, we've seen a change in how bots are controlled, moving from IRC channels to websites, using the common HTTP. This change began with the advent of exploit kits, mostly developed by Russian cybercriminals. Mpack, ICEPack, and Fiesta are a few of the leading kits. They can install software on remote machines and control them from a remote website."

"All hackers have to do is send spam with links, which lead victims to a website where the exploit kit is installed. Once there, the exploit kit can determine which exploit to use—depending on a system's country, operating system, browser, and multiple client application versions."

—McAfee Threats Report, Fourth Quarter 2009

off protections rather than take the performance hit, or they allow Check Point to deactivate protections for them when certain thresholds are reached. Peak activity is precisely the time to expect an attack.

Where reinforcing protections are implemented by separate devices on the same traffic, rather than inline in one operation, each independent process slows down throughput and requires extra hardware for processing.

McAfee offers you a major step forward in both functionality and cost, with consolidated security services that bring together multiple protections in every preconfigured McAfee Firewall Enterprise V8 system. Without additional charges or integration effort, you can activate intrusion prevention, anti-malware, anti-spyware, global reputation (to block risky sites and known spammers), and URL filtering. These protections can be controlled by high-level categories of applications or per application, protocol, and rule. Flexible, granular control like this allows you to determine how best to boost protection—perhaps for traffic into and out of specific regions—and refine protection rules as needed. Inline inspection allows us to perform multiple protection operations at wire speed. You won't have to turn off critical protections to maintain acceptable performance.

Rule 3—Control Should Take Moments, Not Minutes

"The key to keeping cost down is to drastically reduce the number of successful attacks, and from the data that means improved firewall rule management. By properly investing in firewall solutions that offer improved security with signature reduction, organizations should be able to drastically cut the average yearly breach loss of over one million dollars."

—IDC, *The State of Today's Firewall Management Challenges,* June 2009

Traditionally, administration of policies and protections has filled the firewall administrator's day. With separate systems and multiple administrators, rules are hard to get right in the first place, and they are a challenge to maintain. For example, Cisco has users configure firewall and network address translation (NAT) rules in separate windows. Every separate step adds work and creates the opportunity for mistakes. Multiple administrators compound the complexity and increase the chance for rules to overlap, resulting in sluggish performance and rules that never become active. As you add control over applications and users, you face extra options, more decisions, and potentially much more work.

Instead, the McAfee "single-rule view" pulls together the information you need to quickly build precise rules. Within port 80 or 443 traffic, for instance, you can embed restrictions on specific functions, add McAfee TrustedSource™ reputation services, apply geo-location, and more, with each rule associated with specific user groups as needed.

All of these options appear within one window. Each rule takes just a few mouse clicks, so it is both fast and easy to take full advantage of the control options available. Then, use our Rules Interaction window to preview rules to uncover conflicts or overlaps. Because our firewall solution supports natural workflows, you can check the order and drill down to see each entire rule in one window. When you want to understand usage or troubleshoot problems, our visualization shows you activity by user, application, and threat—and lets you navigate directly to adjust the right rules.

Rule 4—Real-Time Risk Assessment Must Cover All Threat Vectors and Be Developed In-House

Beyond cost and performance, the other significant drawback of separate security solutions is their inferior protection. Each tool blocks its narrow view of the problem without learning from other systems that uncover new threats and zero-day vulnerabilities. Cybercriminals now invest heavily in clever multistage and cross-vector threats that count on these isolated tools. Conficker, Operation Aurora, and Mariposa have all incorporated multiple ways in. These devious and complex attacks overwhelm reactive, single-vector, signature-based solutions. While signature technologies remain valuable—ask our researchers, they'll tell you that old worms never die, they just morph—signatures can no longer offer the only line of protection.

Why do signatures fall short? Signatures document known threats only after they are validated, and signature distribution and installation can lag announcement of a problem by days (or longer). Many vendors license protections from third parties, delaying receipt. Check Point passes through technologies from Kaspersky, Websense, and Commtouch. If you use Cisco, you get a weekly anti-virus update via Trend Micro. That means you're exposed to new threats for at least a week. It's common knowledge that signature quality varies from vendor to vendor, gated by the number of researchers and the research scope of the specific vendor (or their supplier). All these separate operations are inefficient, which means you pay for that in subscriptions and a protection gap.

McAfee®

Protection Vector	McAfee Labs™
Malware detection	Detects 50 thousand new malware samples per day
Web filtering	35 million sites categorized for filtering
Spam/phishing	Analyzes 20 billion queries per month
Network IPS	300 million IPS attacks analyzed per month; 100 million IP/port reputation queries per month
Web reputation	6 years of data, now covering 80 million sites
IP address reputation	7 years of data
File reputation	20 years of data

Figure 1. Size and experience matter when it comes to global threat intelligence.

Compromised content and zero-day, unknown threats now present great risk to enterprises. In the absence of a confirmed threat, tools must judge risk based on behavior, reputation, source and recipient addresses, and the content itself (including disguised content that has been decrypted and de-obfuscated). The more data points and threat vectors you can draw on, the more accurate and timely your evaluation will be. When the assessment happens instantly, in real time, it offers the best chance of protection in advance of known threats. That broad perspective may be the most important reason to select a company that monitors and analyzes the big picture in its entirety, without farming out critical pieces to small players.

The McAfee Firewall Enterprise appliance protects you proactively with global threat intelligence delivered in real time. More than 100 million sensors and automated techniques correlate threats across 15 different host, network, web, email, and data loss vectors. We also compare new content and activity against an intelligence base of messaging and communication behavior, including reputation, volume, and trends covering email, web traffic, and malware. This broad, interlaced system, which has been built up over more than 20 years, allows us to infer risk and protect you before a specific threat has been through the formal signature process. Where others pick a single protocol or threat vector, with reputation limited to a single element like spam, McAfee incorporates all protocols and threat trends for the most complete picture and the most effective protection.

Rule 5—Your Firewall Should Not Make You More Vulnerable

Exploit cocktails include an assortment of malware targeting each potential weakness in each system. Your security products should be helping you with this problem, not providing a home for vulnerabilities or acting as the catalyst for emergency patching. Any time you have to install a patch, you run the risk of disrupting traffic or upsetting the system stability.

Based on the hardened McAfee SecureOS® platform developed two decades ago for the U.S. National Security Agency, the McAfee Firewall Enterprise appliance has an unparalleled CERT advisory record, with zero vulnerabilities in our SecureOS, zero breaches, and zero emergency patches.

Rule 6—Transition Your Rule Base Instead of Starting Over

Firewall rules development and maintenance represent the most expensive aspect of owning a firewall. As you think about migrating, you should be able to count on automated migration tools and specific services that will import your old rules into your new environment.

For several years, McAfee has been helping Forbes Global 2000 and government organizations migrate their rules to our simple, centralized rules environment. Typically, our rules migration tool moves 90 percent of all configuration data, including object data, services and existing rule sets. You can also streamline your configuration by choosing not to carry forward objects or services that are not currently being used by the rule set.

Our dedicated network security professional services team offers convenient programs to ease you through the migration process. They have access to this tool to confidently transition policy rules off of Cisco PIX, Cisco ASA, and Check Point firewalls. Tools for Juniper and Fortinet solutions are forthcoming.

McAfee®

Rule 7—You Deserve Integration and Flexibility—All the Way Through to Support

You have better uses for your time than playing integrator or coming up with workarounds for poorly designed and limited products. Today, every enterprise is distributed, and every network is unique. These should be table stakes in the game of security. Smart vendors acknowledge these realities and make it easy for you to implement good protection quickly, and they support you where and when you need it—24/7/365.

McAfee firewall solutions come in a broad range of affordable, hardened configurations that scale from branch offices to 12 Gbps throughput—enough for demanding enterprises. You can select a purpose-built appliance; a multifirewall physical appliance available with four, eight, 16, or 32 firewalls within a small 2U chassis; or a virtual firewall appliance for VMware ESX. We also offer McAfee Firewall Enterprise for Riverbed, which can be installed on several models of Riverbed Steelhead appliances that are running the Riverbed Services Platform, plus ruggedized appliances that can stand up to harsh environments. These are tools you can work with.

All this flexibility comes at an affordable price. Unlike Cisco, with McAfee you won't have to spend additional budget on a patchwork of multiple appliances and security module cards. Unlike Check Point, with McAfee you won't have the complexity and cost of paying for and configuring multiple blade options bolted onto hardware from multiple players.

Since centralized management is at the heart of efficiency (and compliance reporting), you can mix and match enterprise-class appliances with SMB systems within the same management environment. McAfee Firewall Reporter, which is included, will centrally monitor multiple systems and aggregate and make sense of log data coming from multiple devices. We provide more than 500 report templates at no extra charge—there's sure to be one that matches your business and regulation.

If you need help or have a question, our support team of firewall engineers is available 24/7, ensuring fast response times—think minutes, not hours. We don't turn off the phones at night or service only one continent—our customers, research, and support span the globe.

Rule 8—Integration Delivers Optimized Security

We've discussed the savings and simplicity of having multiple protections in one firewall. Since the firewall is just one component of your security and IT controls, you should also look for simplicity beyond the firewall. What about other network security products, remediation tools, security information management, and related workflows? What about endpoint protection, data loss prevention, and risk management? The better your systems communicate, the easier your job becomes. And making security solutions communicate is our specialty.

McAfee is the leading dedicated security vendor. Our firewall is deployed at more than 15,000 customers, and it connects to a range of other network security functions, including web and email gateways, network access control, network user behavior analysis, network threat response, and intrusion prevention systems. We are a long-term, recognized leader in endpoint security, mobile data protection, cloud security, and more. This broad product portfolio connects through the open, centralized McAfee ePolicy Orchestrator® (McAfee ePO™) management platform to bring you operational leverage with each protection you deploy. And more than 90 McAfee Security Innovation Alliance partners connect to the McAfee ePO management platform, extending the savings and simplicity to other security and IT operations.

Web 2.0 Is a New Game. Play By the New Rules.

As you think about migrating to more advanced protection, these rules should provide a playbook to ensure that your new firewall measures up to today's advanced persistent threats and complex Web 2.0 applications:

1. Fine-grained control requires visibility and enforcement tailored to the interactions of users and Web 2.0 applications.
2. Multivector threat protection shouldn't cost extra.

McAfee®

3. Control should take moments, not minutes.
4. Real-time risk assessment must cover all threat vectors and be developed in-house.
5. Your firewall should not make you more vulnerable.
6. Transition your rule base, instead of starting over.
7. You deserve integration and flexibility—all the way through to support.
8. Integration delivers optimized security.

With the McAfee Firewall Enterprise appliance, you can replace port and protocol control with effective and precise protection. Your organization will benefit from greater access to Web 2.0 applications, secured by identity- and application-aware control, global threat intelligence, and multiple security services, working together as a tightly knit team to defend your organization.

We'll make the process easy, with our trial program on a virtual firewall, migration tools, and targeted professional services. Eliminate blind spots and protect your business against today's advanced persistent threats, with fewer fire drills and less effort. Learn more at www.mcafee.com and power up with V8 at www.mcafee.com/virtualtestdrive.

McAfee

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com