

10 Requirements for Your Next Generation Managed Cloud Firewall

The Internet is ubiquitous for businesses today; it is required in order to communicate with customers, identify and nurture prospects, and interact with employees, partners, and other constituents. While Internet connectivity has improved operations, increased efficiencies, and reduced costs, businesses have become more vulnerable than ever to the threats of unauthorized access, malicious attacks, and the latest threat from web-based applications. To protect against existing and future threats, businesses should require and demand a “next generation of protection”, or a Next Generation Managed Cloud Firewall (NGMCF). This whitepaper will outline the 10 key capabilities your NGMCF must deliver in order for you to feel confident with your security solution.

Application visibility and control of your network security is vital. The reason is obvious: applications can easily slip by traditional port-based firewalls. Employees, contractors, and partners will leverage any available application they need to get their job done—often indifferent to or unaware of the risk that poses to the business. Nearly every network security provider has acknowledged that application control is an increasingly critical part of network security. While the “Next Generation Firewall” is well defined by Gartner as leading edge and enterprise-focused, many network security providers are claiming a Next Generation Firewall is a subset of other functions such as Unified Threat Management (UTM) or Intrusion Prevention System (IPS). Most traditional network security vendors are attempting to provide application visibility and control by using a limited number of application signatures supported in their IPS or other external database. But underneath, these capabilities are poorly integrated and their products are still based on legacy



port-blocking technology, not Next Generation Firewall technology. Perhaps most importantly, these vendors are missing the point—it's *not about blocking applications, but safely enabling them*. Unfortunately, the solutions proffered by legacy network security providers ignore much of what businesses do with applications today—they use them to enable their business—and as such, need to make sure that those applications run securely.

For businesses looking to improve their security protection, the most important consideration is: **Will this new service empower my business to securely enable key applications to the benefit of the organization?** Key questions to ask include:

- » Will it increase visibility and understanding of application traffic?
- » Will it expand traffic control options beyond blunt allow/deny?
- » Will it prevent threats?
- » Will it eliminate the need to compromise between performance and security?
- » Will it reduce costs for my organization?
- » Will it allow my IT staff to focus our resources on business critical functions?
- » Will it make the job of risk management easier?
- » Will it make my business more secure today, tomorrow, and in the future?

If the answers to the above questions are “yes,” then a transition to a Next Generation Firewall is easy to justify.

Architecture and Security Model: Traffic is Best Classified in the Firewall

There are substantial differences between NGMCF and UTM-style devices in terms of architecture and security model. These differences have dramatic impacts on real-world functions and features, operations, and performance. In building the Next Generation Firewall, vendors have taken one of two architectural approaches:

- 1) Build application identification into the firewall as the primary classification engine.
- 2) Add application signatures to an Intrusion Prevention System or IPS-like pattern matching engine which is then added to a port-based firewall.

Both can recognize applications, but with varying degrees of success, usability, and relevance. Most importantly, these architectural approaches dictate a specific security model for application policies—either positive (default deny), or negative (default allow).

Firewalls use a positive security model, or “default deny”. Default deny means that administrators write policies to ALLOW traffic (e.g., allow WebEx, GoToMyPC), and then everything else is denied or blocked. Negative policies (e.g., block Limewire) can be used in this model, but the most important fact is that the policy in a positive security model says, “all else deny.” One of the key implications of this approach is that all traffic must be classified in order to allow the appropriate traffic. So visibility of traffic is easy and complete, and policies enable applications. Another key result of this approach is that any unknown traffic is, by default, denied. In other words, the best Next Generation Firewall is a firewall.

Intrusion prevention systems (IPS) typically employ a negative security model, or “default allow”. Default allow means that IPS identifies and blocks specific traffic (traditionally threats), and everything else is passed through. Traditional network security providers are adding application signatures to an IPS-style engine and bolting it onto a traditional port-based firewall. The result is an “application prevention system.” The application control is in a negative security model—in other words, it's not in a firewall. The outcome is that one only sees what is expressly looked for, and unknown traffic is, by default, allowed.

While this paper is focused on the 10 specific things your NGMCF must do, knowledge of the architecture and models as outlined above are prerequisites to understanding the different capabilities of the many solutions on the market and their ability to deliver these critical functions.

The 10 Things Your Next Generation Managed Cloud Firewall Must Do

There are three areas that differentiate NGMCF: security functions, operations, and performance. The security function elements correspond to the efficacy of the security controls, and the ability for businesses to manage risk associated with network traffic. From an operations perspective, the big question is, “Where does application policy live, and how hard or complex is it to manage”? The performance difference is simple: Can the firewall do what it’s supposed to do at the throughput it’s supposed to do it in?

The 10 Things Your Next Generation Managed Cloud Firewall Must Do Are:

- 1) Identify and control applications on any port
- 2) Identify and control circumventors
- 3) Decrypt outbound SSL
- 4) Scan for viruses and malware in allowed collaborative applications
- 5) Deal with unknown traffic by policy
- 6) Identify and control applications sharing the same connection
- 7) Enable the same application visibility and control for remote users
- 8) Deliver the same throughput and performance with application control fully activated
- 9) Be cost effective
- 10) Deliver protection today, tomorrow, and in the future

1 Your Next Generation Managed Cloud Firewall must identify and control applications on any port, not just standard ports (including applications using HTTP or other protocols)

BUSINESS CASE: Application developers no longer adhere to standard port, protocol, or application mapping. Applications such as instant messaging, peer-to-peer file sharing or Voice over IP are capable of operating on non-standard ports or can hop ports. Additionally, users are increasingly savvy enough to force applications to run over non-standard ports (e.g., Microsoft Remote Desktop Protocol, SSH). In order to enforce application specific policies where ports are increasingly irrelevant, your future firewall must assume that any application can run on any port. This is one of the fundamental technology drivers that make the Next Generation Firewall an absolute necessity, while making traditional port-based firewalls obsolete. It also underscores why a negative control model cannot solve the problem. If an application can move to any port, a product based on negative control would have to run all signatures on tens of thousands of ports, which is not scalable or manageable.

REQUIREMENTS: This one is simple—if any application can run on any port—your future firewall must classify traffic, by application, on all ports—all the time. Otherwise, security controls will continue to be threatened by the same techniques that have plagued them for years.

2 Your Next Generation Managed Cloud Firewall must identify and control circumventors: proxies, remote access, and encrypted tunnel applications

BUSINESS CASE: Most organizations have security policies—and controls designed to enforce those policies. Proxies, remote access, and encrypted tunnel applications are specifically used to circumvent security controls like firewalls, URL filtering, IPS, and secure web gateways. Without the ability to control these circumventors, organizations cannot enforce their security policies, and expose themselves to the very risks they thought their controls mitigated. To be clear, not all of these

types of applications are the same, remote access applications have legitimate uses, as do some encrypted tunnel applications. But external anonymous proxies that communicate over SSL on random ports, or applications like Ultrasurf and Tor have only one real purpose, to circumvent your security controls.

REQUIREMENTS: There are different types of circumvention applications each using slightly different techniques. There are both public and private external proxies (see proxy.org for a large database of public proxies) that can use both HTTP and HTTPS. Private proxies are often set up on unclassified IP addresses (e.g., home computers) with applications like PHPProxy or CGIProxy. Remote access applications like GoToMyPC or LogMeIn can have legitimate uses, but due to the associated risk, should be managed. Most other circumventors, (e.g., Ultrasurf, Tor, Hamachi) do not have legitimate business uses. There are, of course, unknown circumventors—see #6 below. Regardless of the policy stance, your future firewall requires specific techniques to deal with all of these applications, regardless of port, protocol, encryption, or other evasive tactic. One more consideration: these applications are regularly updated to make them harder to detect and control. So it is important that your future firewall can identify these circumvention applications, and will also ensure that your firewall's application intelligence is updated and maintained on an ongoing basis.

3 Your Next Generation Managed Cloud Firewall must decrypt outbound SSL

BUSINESS CASE: Today, more than 15% of network traffic is SSL-encrypted and in some industries such as financial services or healthcare, it can be more than 50%. Given the increasing adoption of HTTPS for many high-risk, high-reward applications that end-users employ (e.g., Gmail, Facebook), and users' ability to force SSL on many websites, network security teams have a large and growing blind spot without decrypting, classifying, controlling, and scanning SSL-encrypted traffic. Certainly, your future firewall must be flexible enough that certain types of SSL-encrypted traffic can be left alone (e.g., web traffic from financial services or health care organizations) while other types (e.g., SSL on non-standard ports, HTTPS from unclassified websites in Eastern Europe) can be decrypted via policy.

REQUIREMENTS: The ability to decrypt outbound SSL is a critical element, not just because it's an increasingly significant percentage of enterprise traffic, but also because it enables a few other key features that would end up incomplete or ineffective without the ability to decrypt SSL (e.g., control of circumventors, application function control, scanning allowed applications, and control of applications sharing the same connection. Elements to look for in a provider include recognition and decryption of SSL on any port, policy control over decryption, and the necessary hardware and software functions to perform SSL decryption across tens of thousands of simultaneous SSL connections while maintaining good performance and high throughput.

4 Your Next Generation Managed Cloud Firewall must scan for threats in allowed collaboration applications

BUSINESS CASE: Enterprises continue to adopt collaborative applications hosted outside their physical locations. Whether it's hosted Microsoft SharePoint, Google Docs, Box.net or Microsoft Office 365, or an extranet application hosted by a contractor or business partner, many organizations need to use file sharing applications. These applications are considered to be a high-risk threat vector as many infected documents are stored in collaboration applications, along with documents that may contain sensitive customer information such as credit card information. Furthermore, applications like Microsoft SharePoint rely on supporting technologies that are regular targets for exploits including Microsoft SQL Server or IIS. Blocking the application altogether isn't ideal or even realistic, but collaboration applications can pose a risk to your organization.

REQUIREMENTS: Part of safe application enablement is allowing it and scanning it for threats. These applications communicate over a combination of protocols (e.g., SharePoint—HTTPS and CIFS, see requirement #3), and require a more sophisticated policy other than "block application". The first step is to identify the application regardless of port or encryption, allow it, and then scan it for any threats, exploits, viruses/malware, or spyware...or even confidential, regulated, or sensitive information.

5 Your Next Generation Managed Cloud Firewall must create policies for unknown traffic

BUSINESS CASE: There will always be unknown traffic and it will always represent significant risks to any organization. There are several important elements to consider with unknown traffic—minimizing it, easily characterizing custom applications so they are “known” in network security policy, and having predictable visibility and policy control over traffic that remains unknown.

REQUIREMENTS: First, by default, your future firewall should attempt to classify all traffic. This is one area where the earlier architecture and security discussion becomes very important. Positive (default deny) models classify everything, negative (default allow) models classify only what they’re told to classify. Second, for custom developed applications, there should be a way to develop a custom identifier so that traffic is counted as “known.” Third, the security model plays into these requirements again—a positive model can deny all unknown traffic—so what you don’t know can’t hurt you. A negative model allows all unknown traffic—so what you don’t know will hurt you. For example, many botnets will use port 53 (DNS) for communication back to their control servers. If your future firewall lacks the ability to see and control unknown traffic, bots will be able to access your network unimpeded.

6 Your Next Generation Managed Cloud Firewall must identify and control applications sharing the same connection

BUSINESS CASE: Applications share sessions. To ensure users are continuously using an application “platform,” whether it’s Google, Facebook, Salesforce.com, LinkedIn, or Yahoo, application developers integrate many different applications—which often have very different risk profiles and business value. Let’s look at our earlier example of Gmail which has the ability to spawn a Google Talk session from within the Gmail session. Gmail and Google Talk are fundamentally different applications, and your future firewall should recognize that, and enable the appropriate policy response for each.

REQUIREMENTS: Simple classification of the platform or website does not work. In other words, “fast path” is not an option—“once and done” classification ignores the fact that applications share sessions. Traffic must be continuously evaluated to understand the application, when the user changes to a completely different application using the same session, and enforce the appropriate policy controls. Looking briefly at the technical requirements using the Gmail/Google Talk example: Gmail is by default HTTPS so the first step is to decrypt, but it has to be continuous, as does the application classification, because at any time the user can start a chat which may have a completely different policy associated with it.

7 Your Next Generation Managed Cloud Firewall must enable the same application visibility and control for remote users as on-premise users

BUSINESS CASE: Users are increasingly outside the four walls of the enterprise. Once the domain of road warriors, now a significant portion of the business’ user population, including employees, contractors, and partners work, remotely. Whether working from a coffee shop, home, or a customer site, users expect to connect to their applications via Wi-Fi, wireless broadband, or any means available. Regardless of where the user is, or even where the application they’re using resides, the same standard of control should apply. If your future firewall enables application visibility and control over traffic inside the four walls of the enterprise, but not outside, it misses the mark on some of the most risky and higher-volume traffic.

REQUIREMENTS: Conceptually, this is simple, your future firewall must have consistent visibility and control over traffic regardless of whether the user is inside or outside your network. This is not to say that businesses will have the exact same policy for both as some organizations might want employees to use Skype when on the road, but not inside headquarters. Others might have a policy that says if outside the office, users may not download salesforce.com attachments unless they have hard disk encryption turned on. This should be achievable on your future firewall without 1) introducing significant latency for the user, 2) undue operational hassle for the administrator, or 3) significant cost for the organization. Additionally, this solution, when layered with a Virtual

Private Network (VPN) connection between remote users, contractors, or a partner's computer and the corporate network will deliver increased security and productivity by allowing the remote users to securely access network applications, data, and resources while away from the physical office. The VPN works on the Network Layer of the OSI Model, securing all data that travels between the remote user and corporate network. A SSL VPN for remote users who require secure access to the network through a web browser without having to first install a client application will add an additional layer of security to further protect your business.

8 Your Next Generation Managed Cloud Firewall must deliver the same throughput and performance with application control fully activated

BUSINESS CASE: Many businesses struggle with the forced compromise between performance and security. All too often, turning up security features in the network security realm means turning down throughput and performance. If your Next Generation Firewall is built the right way, this compromise is unnecessary.

REQUIREMENTS: The importance of architecture is obvious here in a different way. Cobbling together a port-based firewall and other security functions from different technology origins usually means there are redundant networking layers, scanning engines and policies which translate to poor performance and complex administration. From a software perspective, the firewall must be designed to do this from the beginning. Furthermore, given the requirement for computationally intensive tasks (e.g., application identification) performed on high traffic volumes, and with the low tolerance for latency associated with critical infrastructure, your future firewall's hardware should have dedicated, specific processing for networking, security (including SSL termination), and content scanning.

9 Your Next Generation Managed Cloud Firewall must be cost effective

BUSINESS CASE: Business costs related to deployment and managing information security are overhead expenses and have many cost components, including:

- The capital cost to purchase security hardware and software
- The cost to install and configure the software from your staff or contractors
- The annual cost for equipment maintenance and software updates and upgrades
- The annual cost to manage and monitor the systems and the business infrastructure
- The cost for ongoing training of your staff or contractors
- The cost to research new solutions to meet your business' future needs as new threats present themselves

Capital costs, maintenance costs, people costs—most businesses understand that their money would be better spent launching a new product or service. Network security is overhead and it's never-ending. In fact, many of the costs hit a company's bottom line before the security solution is even up and running. A NGMCF solution helps business to manage their capital more effectively and efficiently.

REQUIREMENTS: A NGMCF should *reduce your capital and operation costs while improving your businesses level of protection* by replacing the following with a simple monthly fee.

- Upfront capital expenditures of the hardware and software
- Annual hardware maintenance contracts
- Annual software update contracts
- Staff costs to install and configure your solution
- Staff costs to reconfigure your solution as your business changes
- Staff costs to research future protection solutions
- Ongoing staff training and certification costs
- Staff costs to monitor

Additionally, an NGMCF allows you to benefit from the sharing of overhead costs for the Network Operations Center (NOC), future research on new potential threats and solutions to prevent them, and shared experience and knowledge from threats that affect all businesses. As your business grows or contracts, or as your security needs increase, your NGMCF should be able to change with your business. With the right NGMCF, you should and will be able to reduce your capital and operation costs while improving your level of protection.

10 Your Next Generation Managed Cloud Firewall must deliver protection everyday —today, tomorrow, and in the future

BUSINESS CASE: Most businesses are not static in their operations. They must continually evolve and reinvent themselves to meet new market demands and competitive pressures of the world they operate in. This ever-changing landscape creates new demands on the business, its people, and its infrastructure for new applications and new business processes. More often than not, the business wants to invest in growth areas like sales, marketing and new product development, not in overhead areas like G&A or even information security. Most organizations address information security on a reactive project by project basis, when it should be treated as a 24/7 task to stay ahead of the ongoing changes in the business and the changes in outside threats to the business. All too often, security becomes a reactive task against a problem or breach versus a proactive activity to ensure your business grows and evolves securely. The right NGMCF should proactively protect your business no matter how your business evolves and no matter what the threat is, protecting your business around the clock.

REQUIREMENTS: A NGMCF should offer a proactive approach to delivering total security always. Not only should your NGMCF manage the technology protecting your business, it should continually upgrade and update the systems to detect the latest security threats as well as continually monitor all systems, all the time. Just like your home alarm system, you are protected by an extended team of certified professionals at the NOC who are there when you are not. Even if you have a dedicated IT or security team who performs these functions, they cannot provide the breadth of coverage, and typically

are only reacting to a task at hand as opposed to proactively looking for future threats. Additionally, your business is likely not researching new security threats and how to continually remain secure. As your business evolves and grows, your NGMCF provider can evolve and grow or contract with you from a service delivery perspective while enhancing and expanding your security protection to continually meet and match your specific needs at any given stage of your business.

Conclusion: Your Next Generation Managed Cloud Firewall Should Safely Enable Applications and Your Business

Users, contractors, and business partners continue to adopt new applications and technologies and the ever-expanding threats that go along with them. Applications enable employees to get their jobs done, or maintain productivity in the face of competing personal and professional priorities. Because of this, safe enablement is increasingly the standard policy stance. But to safely enable these applications and technologies for the business, network security teams need to apply the appropriate policies governing use, and the controls capable of enforcing them. The 10 Requirements described here are critical capabilities for putting the necessary controls in place, especially in the face of a more varied and rich application and threat landscape. Without the network security infrastructure to cope with that variety and depth, security teams cannot safely enable the necessary business applications and manage risk for their enterprises. To bring your business the security and application protection it needs, you don't have to wait any longer—a NGMCF can deliver the protection, performance, and cost effectiveness your business requires and demands.

ABOUT INTEGRA'S CLOUD FIREWALL SERVICE:

Integra's Cloud Firewall Service, the first in a comprehensive family of new Cloud Security Services from Integra, protects your business by guarding the perimeter of your network providing secure inbound and outbound Internet access through a secure managed gateway. This managed service also provides for a consistent enforcement of security policies for all of your facilities, even staff working remotely without on-premise equipment or dedicated IT staff. Integra's Cloud Firewall Service provides increased security and protection while reducing administrative overhead and costs, eliminating capital outlays, and provides round the clock 24/7 monitoring, while delivering improved employee productivity, improving network performance, and protecting sensitive corporate data and systems. With Integra's Cloud Firewall Service, you are ready to meet the challenges of today's threats and tomorrows with increased capabilities, reduced costs, and better protection. Integra's Cloud Firewall Service is available in three configurations to meet your specific protection requirements. For more information, visit www.integratelecom.com.

Integra's Cloud Firewall Service is powered by technology from Palo Alto Networks™. Palo Alto Networks next-generation firewalls enable unprecedented visibility and granular policy control of applications and content—by user, not just IP address—at up to 20Gbps with no performance degradation. Based on patent-pending App-ID™ technology, Palo Alto Networks firewalls accurately identify and control applications—regardless of port, protocol, evasive tactic or SSL encryption—and scan content to stop threats and prevent data leakage. Businesses can for the first time embrace Web 2.0 and maintain complete visibility and control, while significantly reducing total cost of ownership through device consolidation. For more information, visit www.paloaltonetworks.com.



About Integra Telecom

Integra Telecom Inc. connects business by providing business-grade networking, communications and cloud solutions to thousands of business and carrier customers in 11 Western states, including Arizona, California, Colorado, Idaho, Minnesota, Montana, Nevada, North Dakota, Oregon, Utah and Washington. The company owns and operates a nationally acclaimed best-in-class fiber-optic network consisting of a 5,000-mile high-speed long-haul fiber network and a 3,000-mile metropolitan access network including more than 1,700 fiber-fed buildings.

Contact Us

Integra Telecom
1201 NE Lloyd Blvd., Suite 500
Portland, OR 97232
1-866-INTEGRA
www.integratelecom.com