Network Solutions Overview

A deeper look at the security services offered by our expert engineers

**Contact Us Today
To Get Started**

317.225.4117
sales@firewalls.com

What's In It For Me?

If your firewall isn't performing exactly as you expect, don't just go buy a bigger and better box! Let our engineers wring out every last available megabyte of processing power. Firewalls.com employs some of the most talented, experienced, and authoritative minds in the network security industry.

With our very own Security Operations Center located in our Indianapolis office, our team of engineers possess the unique ability to inspect, diagnose, & configure firewall appliances in real-time lab environments. This process ensures that your appliance is fine-tuned to the most efficient settings and always in line with modern security best practices. Network security is hard. We simplify the process by eliminating redundancies, inefficient settings, & obsolete practices. Scroll down for an A to Z sampling of the solutions we offer.

Access Control Lists
Capitalize on infrastructure and bring identity to the forefront to gain control of information exposed and traversing the network by utilizing hardened access controls. Permit, deny, and prioritize network functions and reduce user risk by controlling who has access to what, when they can access it, and where that access may originate from. Safeguard your data by implementing granular control of users and groups.
By taking advantage of pre-defined blacklists and whitelists, your network starts with a strong foundation of access controls upon which you can build the granular rules and exemptions unique to your network. Meet regulatory compliance requirements by limiting access to sensitive data, functions, & applications.

Active Directory Integration with Single Sign-On
Greater control over the users operating on your network lightens the load of network administrators. Instead of being tied to a single machine, Single Sign-On lets a user's identity transfer from device to device, simplifying the process of user audits and activity tracking.
If an infection should occur, Single Sign-On can save you time as you work to detect, locate, and quarantine the threat. Root Cause Analysis is a breeze, allowing administrators to see exactly where, when, and why a breach occured. Make a commitment to user accountability with Single Sign-On.

Content Filtering
Tired of seeing Facebook, YouTube, Twitter, and other time-wasting websites in your workplace? Content filtering gives you granular control over the websites that your users can access. By restricting users and groups to only the types of websites necessary or their role, you eliminate the risk of inappropriate and unproductive web usage.
Organizations are often unaware that they may be held liable for any illegal activities that take place on their network. By deploying a smart Content Filtering strategy, organizations demonstrate a best-faith effort to prevent such illicit usage of company resources. Content Filtering services are common requirements for regulatory compliance.

DPI/SSL & CA Certificate Deployment
With over 60% of web traffic hiding behind encryption, implementing Deep Packet Inspection is crucial to analyze encrypted data. Our engineers assist with deployment of appliance certificates that allow for SSL scanning on Edge, Internet Explorer, and Google Chrome. Please note, this service is currently only available for Windows OS users.
Deploying advanced certificates is a notoriously time-consuming process that is often better left in the hands of experts. Let our engineers authenticate and secure your website with DPI/SSL so that your appliance scans even encrypted traffic for the latest advanced security threats.

Email Security
Your inbox represents one of the most common routes of infection on company networks. If you have been the target of phishing, spearphishing, whaling, or any other form of social engineering, then you understand just how clever and manipulative this branch of cyber crime has become. Our engineers review cipher settings and POP3/IMAP/SMTP protocols so that your mailbox won't leak like a sieve.
Your firewall can scan both inbound and outbound traffic, looking for clues of any sensitive information such as credit card data, social security numbers, or personally identifying information that hackers can use as leverage for further attacks. Quarantine and detonate suspicious payloads before they can impact your network!

Enterprise Wireless
Wireless networks present more complicated security challenges than their hardwired counterparts, especially in a large-scale, enterprise setting. Yet WiFi is vital to doing business. So your enterprise must not only connect but also protect the systems, mainframes, computers, smartphones, tablets, IoT devices, and more.
Our certified engineers can assist you in setting up your enterprise wireless network to keep it (and all its associated devices) running smoothly. This includes heat mapping using the best tools to ensure you have the right number of access points placed in the right spots to serve your organization's needs. And of course, we do security too, so you can count on a safe, secure WiFi network in expert hands.

Firewall Health Check

The threat landscape is always changing. With ransomware-as-a-service and malware cocktails resulting in an endless stream of never-before-seen threats, a strong security posture is a dynamic one. The days of "set it and forget it" security have passed and staying at the forefront of cybersecurity means staying on your toes with frequent updates, policy changes, and growth of standard operating procedures.

Our engineers ensure your network is up to date with the most advanced security best practices by reviewing your firewall policies, configurations, cipher settings, user groups, and more. We have been configuring firewalls for over two decades, so if there is any room for improvement in your security, we will uncover it and share real, actionable recommendations to increase performance and strengthen your network.

Gateway to Gateway VPN Tunnel

Branch locations need to be securely networked, just as if their users were down the hall. Did you know, you can accomplish transparent, secured communication between locations without the expense and IT overhead of MPLS.

Our engineers can configure up to two IPSec or SSL VPN Site-to-Site Tunnels with several options designed to meet your organization's needs. And it doesn't stop there. We'll also conduct remote testing and troubleshooting to ensure your tunnel is running smoothly.

High Availability

What plan does your organization have in place in the event of a firewall hardware malfunction? If you're not utilizing a High Availability-enabled setup, you will likely eat the cost of extended network downtime. Employing an identical hardware appliance with synchronized configurations behind your network means that if the primary appliance fails, you have backup!

High Availability grants 24x7 access to data and ensures productivity doesn't grind to a halt in the case of malfunction or disaster. Our engineers synchronize settings across primary and HA units then configure your backup appliance in-line with your firewall, building failsafes into your network.

Hosted Email Security

Hosted email offers businesses the chance to use their own domain as an email address without the potential hassle and cost of running their own email servers. Sounds good, right? The problem is, not all hosted email services are created equal. POP3 is different than SMTP, and different services offer different levels of security. Since emails are often threat vector number one for data breaches, you won't want to take chances. Let our engineers ensure your email setup is second-to-none in network security.

Infrastructure as a Service (IaaS)

When equipment and personnel costs make network management difficult for businesses to handle, the solution often lies in the cloud. Infrastructure as a Service (IaaS) allows businesses to leave the servers, storage, networking, and virtualization to be handled offsite.

IaaS not only saves on hardware and maintenance costs, it's scalable for any size need your organization has, and it still allows you full control over your applications, operating systems, and other infrastructure. And you only pay for the resources you need.

Mobile Device Management (MDM)

Let's face it, we live in a mobile world, complete with mobile workplaces and mobile employees. That means mobile devices like smartphones and tablets likely make up a good portion of your network endpoints.

And many times, these devices belong to the employee, rather than the business. Managing these devices within your network can be a unique challenge, but our engineers are ready to take it on for you, implementing mobile device management tools to monitor and secure the devices using your network.

Network Mapping

To ensure your network is operating to its fullest capabilities, you need a complete understanding of all the devices that make it up. In today's complex modern networks, that is no small task. Discover all your devices, and how they are linked through network mapping.

While there are tools that help automate and integrate the device discovery and mapping processes, you'll want an expert to help you set up your network maps, keep them updating automatically, and provide you with an understanding of the process and its outputs.

Office 365 Migration Services
Moving your organization to Office 365 can change the way you manage your software and reinvent your infrastructure. This cloud-based approach can let you scale-back on server usage and change the way your IT department operates. You'll also be privy to all the regular updates Microsoft provides and have access to the many collaborative options offered by Office 365.
But whether you've been using traditional Office software or another solution, the switch doesn't happen at the snap of a finger. Trust our engineers to help you every step of the way, guiding you through the process of preparing for the migration, the move itself, and how to fully implement Office 365 in your organization.

Remote Access VPN
With an increasingly mobile workforce, you need to ensure your employees can securely logon to your network wherever they are. That means secure remote access via VPN, and our engineers are here to help. They'll configure up to two profiles/access groups with either SSL or IPSec settings. The configuration also includes access controls to help you further safeguard your data.

Remote Monitoring & Management (RMM)
Many organizations struggle with the problem of too much to do, and too few people (or too little time) to do it. Even those with IT staff know that bigger picture projects often get stymied by the day-to-day grind of troubleshooting network issues.
With remote monitoring & management, you can turn the task of keeping tabs on your network over to our experts. They'll be alerted to any issues with your network including the devices on it, and be able to respond quickly to address them. You can be assured your network is in good hands, and it's one less thing to do for you or your staff.

SD-WAN
Need a Wide Area Network (WAN) without the rigid structure and expense of MPLS? SD-WAN is the way to go. With SD-WAN, you can increase the performance of your network by ensuring traffic is routed on the path with the most efficiency. If one point fails, unlike MPLS, it seamlessly moves on to the next. Our engineers can get you started identifying applications, configuring IPSec VPNs, setting Dynamic App Failover. And once it's setup, your admins will be able to make adjustments on the fly.

Security Information and Event Management (SIEM)
Security starts with situational awareness. You don't want to be caught unaware of what's happening on your network. SIEM helps fill the information void, providing real-time collection and analysis of log and event data to help you monitor threats and the responses to them - also reporting on security incidents and providing alerts to unusual activity.
Integrating SIEM will get you this level of monitoring throughout your network, including computers, firewalls, applications and more. This not only helps with your organization's security, but for tracking that you're meeting compliance mandates as well. Our engineers can help you get SIEM setup and keep close tabs on your network so you know nothing will slip by.

TMG Migration
Many organizations adopted Microsoft Forefront Threat Management Gateway (TMG) as a comprehensive security solution. But TMG is EOS (end-of-support) now, meaning if it's still a keystone of your network, your organization is vulnerable to the latest threats - and has been for awhile.
The good news is, you have other virtual options available to get your network protected again, and even better than before. Products available now do everything TMG did, while also adding more, stronger protection and being easier to use. Trust our certified experts to get your network migrated from TMG to your new virtual security solution.

Two-Factor Authentication (2FA)
With the ever-evolving online threat environment, one of the prime targets for hackers is a user's log-in information. To help with memorization, many still use simple passwords that are easy to crack. And online scams can skim passwords from phony sign-on pages.
Guard against a single password failure compromising your security by implementing two-factor authentication (2FA). This means not only a password, but another credential must be entered before a login can occur. Our experts can help you add the extra layer of security to your network with 2FA.

VOIP
Optimizing performance of your VOIP means more than just clearer calls. It means you won't suffer the frustrations of dropped calls, one-way calling, missed conversions, & static-filled conferences. VOIP is easier to scale up than traditional phone systems and costs far less to operate internationally.
As one of your organization's most critical resources, reliable calling that follows employees across devices should be a top concern for business owners and administrators. Our engineers allocate sufficient bandwidth to your VOIP systems and prioritize call clients so phone conversations won't be sacrificed for websurfing.

Web Application Firewall
A number of threats can compromise your network when your users browse the web. Many online threats like SQL injections and cross-site scripting (XSS) to name a couple, exploit security flaws in web applications to steal your data and infiltrate your network.
Unlike traditional firewalls, web application firewalls (WAF) target web applications, serving as a filter between them and the internet. They not only monitor HTTP traffic but also protect applications (and thereby your network) from malicious scripts and compromised websites. Our engineers can help you deploy a WAF as part of your network security toolbox and shield your organization from many online dangers.

Wireless Networking
Mobile workers are efficient workers. Businesses thrive on collaboration, teamwork, and flexibility. A WiFi network grants your organization the ability to work when they want, where they want - without being tied to a desk. And fast, secure public WiFi ensures your guests can connect to the Internet without intruding on your internal network where sensitive data is stored.
No matter whether you anticipate 50 users or 5,000 users, our certified experts can help you map and setup your network in a reliable, secure manner.

Contact Us Today
To Get Started

317.225.4117
sales@firewalls.com

Firewalls.com