Business Internet Security and Firewall Protection

Cyber criminals are hard at work 24/7 to gain access to and steal information from business networks. Ensure your network is protected with an industry leading Dell/SonicWALL Security Appliance.

Data breaches can cost your business thousands of dollars and damage your service reputation. Employee misuse of internet access can expose your company to legal risk, degrade employee productivity, and consume network resources that could be used for legitimate business purposes. For these reasons and many more, POPP installs and recommends Dell/SonicWALL Security Appliances.

For our VoIP and Internet Phone System clients we lease and install a Dell/SonicWALL Appliance as our VoIP Management Device (VMD).

Clients who need additional control over their network security or want to tap into advanced big-business security and productivity features, may purchase a Dell/SonicWALL Internet Gateway Firewall Appliance complete with the SonicWALL Comprehensive Gateway Security Suite (CGSS) software to be installed and managed by POPP. An Internet Gateway Firewall Appliance will work on its own or in conjunction with a VoIP Management Device.

VoIP Management Device Benefits:	
Prioritization/Quality of Service (QoS)	Voice traffic is prioritized over general internet traffic. Thereby ensuring your customers experience the best possible voice quality.
Remote Access and Administration	POPP can troubleshoot issues and perform common changes, often without dispatching a technician, saving you time and money.
Automatic Failover (AFO)	Automatic Failover protects your productivity. With internet connection offerings from POPP, Comcast, and CenturyLink we can find affordable multi-provider options to add Automatic Failover to ensure your business doesn't miss a beat if a single connection goes down.
Basic Firewall Protection	The VMD acts as a NAT firewall for clients without an existing dedicated firewall/security appliance.
Internet Gateway Firewall Appliance Benefits:	
Content Filtering	Select from a list of website content categories (e.g. Pornography, Gambling, Social Media) to allow/or block access to for your employees.
Geo IP Filtering	Does your company conduct business with Russia, Nigeria, Indonesia? If not, why not block IP addresses from foreign countries from accessing your equipment? Most hacking originates from outside the United States. You can block/allow access by country.
Virtual Private Networking (VPN)	If your business has branch offices, you can often save money (vs. dedicated private connections interconnecting offices) by installing a branch office VPN, which creates an encrypted site-to-site connection over the internet. If you would also like to enable your workforce to work from home or other off-site locations, a mobile user VPN will create a secure connection from a computer to your office network. This gives your mobile workforce access to all of the shared files, printers, and other network resources they'd have if they were physically connected in the office.

Internet Phone System Security

The security and confidentiality of your business communications are of critical importance to you, and the customers you serve. Thousands of business clients trust us to help keep their communications secure, and we take that responsibility seriously.

Our Security Protocol

Here are just a few of the security measures we have in place to protect our network and your information:

- POPP's network is protected by redundant SonicWALL NSA Firewalls and Metaswitch Perimeta Session Border Controllers
- POPP monitors network phone traffic patterns and failed login attempts for suspicious activity and will disable access from hackers
- Phone configurations containing passwords are encrypted
- Web portals use HTTPS security and strong passwords
- Encrypted Voice adds 256-bit encryption as part of RFC 6188
- Call recordings are encrypted with 256-bit AES encryption
- Voicemail-to-email messages are transmitted using SSL encryption when supported by the far-end server

Additional Best Practices

Beyond our standard security measures, we recommend the following best practices to further reduce risk:

- If specific positions in your company work with sensitive information like credit card or social security numbers, their voicemail greetings should advise callers not to include that information in their message
- Require account codes to make outbound international calls, or block them entirely, to lessen the risk of unauthorized calling
- Require employees to change web portal passwords and voicemail pins on a regular basis

Learn more at POPP.com or call us at 763-797-7900.