The Security Maze

Management & Training

Management & Training are paramount to any best practice security solution. Remember that the strength of your security solution is still at risk to the weakest link, the end user. Most security breaches can be prevented with proper training and education for end users. Well-crafted cyber security training and restrictive acceptable use policies are a cornerstone to maintaining network security. Making sure that your solutions are up to date, firmware updates, best practice configurations, etc., are just as equally important to your security policy. More often than not, this best practice is overlooked and underappreciated.

Exploits

Monitoring & Reporting

Monitoring & Reporting are just as important as any of the other items on this plan. Having a dedicated SIEM position in place to monitor and report network activity is an absolutely mandate for network admins. Not just for security, but for network planning and sizing as well.

Next Generation Firewalls

Implement no-compromise network security that combines intrusion prevention, malware protection, SSL decryption and inspection, and application intelligence with real-time traffic visualization and inspection. Scan every byte of every packet for the deepest level of network protection. Scale to extend state-of-the-art security to growing and distributed enterprise networks. You can deploy SonicWall network security appliances as unified threat management (UTM) firewalls that offer comprehensive security combining gateway content filtering, anti-spam, anti-virus, anti-spyware with intrusion prevention plus application intelligence and control.

Botnets

Malware

Stolen Credentials

Privileged Management

Privileged identity management (PIM) is a domain within identity management focused on the special requirements of powerful accounts within the IT infrastructure of an enterprise. It is frequently used as an information security and governance tool to help companies in meeting compliance regulations and to prevent internal data breaches through the use of privileged accounts. The management of privileged identities can be automated to follow pre-determined or customized policies and requirements for an organization or industry.

Endpoint Threat Detection

By combining the two powerful offerings, SonicWall and SentinelOne will not only automate the distribution and enforcement of SentinelOne's Endpoint Protection Platform (EPP), but also ensure automatic remediation of malicious attacks such as ransomware in the event of infection by reversing system and file modifications. Combining the two solutions will allow administrators to not only create policies to determine which individuals must run the endpoint solution on their devices, but also add controls to ensure that devices are running the endpoint client. SentinelOne and SonicWall will also offer threat intelligence sharing – combining the industry's fastest conversion from unknown to known malware via the SonicWall Capture Threat Network with the addition of threat intelligence from SentinelOne endpoint data.

Hackers

Compliancy Violations

SPAM

Data Protection & Encryption

The SonicWall Email Compliance and Encryption subscription service, an optional service available with SonicWall Email Security, helps organizations achieve regulatory and industry compliance when moving PII (Personally Identifiable Information), PHI (Protected Health Information), proprietary data or any other types of sensitive information. HIPAA/HITECH, GLBA, PCI and other regulations require sensitive data be encrypted when transferred over a public network like the Internet. Since most organizations use email and simple file attachments as the preferred method for business communications, it's imperative that these be secured when transmitting sensitive data.

Two Factor Authentication

One of the many enhanced features found in SonicWall™ Secure Mobile Access (SMA) solutions is end-user authentication, either through an internal database or through integration with one of many dynamic authentication methods, including Quest Defender, Active Directory, RADIUS and LDAP. The SMA solutions notify users prior to password expiration, and can change passwords before or after expiration, even when part of a Microsoft® Active Directory domain. SonicWall SMA solutions offer support for Active Directory nested groups, as well as TLS/SSL support for LDAP/AD. In addition, all appliances offer tokenless two-factor authentication as part of the standard feature set.

Waterhole Attacks

Advanced Persistent Threat Detection

SonicWall Capture extends firewall threat protection to detect and prevent zero-day attacks. The firewall inspects traffic and detects and blocks known malware and intrusions. Suspicious files are sent to the SonicWall Capture cloud service for analysis. The multi-engine sandbox platform includes virtualized sandboxing, full system emulation, and hypervisor-level analysis technology. It executes suspicious code and analyzes behavior, thus providing comprehensive visibility to malicious activity, while resisting evasion tactics and maximizing zero-day threat detection.

Phishing

Secure Remote & WIFI Communications

Provide a single, secure mobility gateway for all platforms — including Windows®, Mac OS® and Linux®—from almost any device, whether for browser-based access or an "in-office" experience. Extend access to iOS, Mac OSX, Windows, Google® Android™ and Kindle Fire devices with the SonicWall Mobile Connect™ app.
This includes Wireless communications. Wireless local area networks (WLANs) offer the flexibility to work from more locations and boost productivity for employees, onsite partners, contractors and guests. However, they also introduce many potential security concerns. SonicWall wireless network security solutions can alleviate these concerns, enabling you to extend your business network without jeopardizing its integrity.

Email Security

Solve the unique email security needs of your organization – whether you have one user or 100,000. From appliances and software to virtual appliances and services, our flexible solutions offer powerful protection against spam, phishing, viruses, and even ransomware threats

Ransomware

Navigate the Threats, Secure the Network

SONICWALL™