SOPHOS
Security made simple.

CORE toCLOUD™

FIREWALL BEST PRACTICES TO BLOCK RANSOMWARE

Recent ransomware attacks like Wanna and Petya have spread largely unchecked through corporate networks in recent months, extorting money to restore your data and regain control of your computers. Modern firewalls are purpose-built to defend against these kinds of attacks, but they need to be given an opportunity to do their job. In this whitepaper we'll discuss how these attacks work, how they can be stopped, and best practices for configuring your firewall and network to give you the best protection possible.

A Sophos Whitepaper July 2017

How Recent Ransomware Attacks Spread

Wanna, Petya, and other ransomware attacks have crippled countless organizations. Together, these two attacks have infected hundreds of thousands of computers all around the globe. These particular attacks spread by exploiting a vulnerability in Microsoft's Server Message Block (SMB) network file-sharing protocol. This protocol is ubiquitous on corporate LANs and allows computers to discover each other for the purpose of sharing files and other resources like printers. It can also be used for file sharing outside the firewall if the necessary ports (TCP 139 and/or 445) are opened or forwarded on the firewall.

The particular exploit used by Wanna and Petya is known as EternalBlue. EternalBlue allows remote code execution by sending carefully crafted messages across the network to the vulnerable SMB service on computers running Microsoft Windows.

In general, every networked system, whether it's running Windows, Linux, Mac OS, or some other operating system, relies on a variety of services for network functionality, and occasionally new vulnerabilities are discovered in these services that can have dire consequences if maliciously exploited.

In the case of the EternalBlue exploit, Microsoft quickly issued a patch for this vulnerability once it was publicized, but hackers took advantage of the fact that rolling out patches in organizations is a considerable undertaking and were able to launch these attacks before many systems had been updated.

Even in the most diligent organizations, there's always a gap between vulnerability discovery and patch deployment, which is why it's so important to have leading next-gen technology protecting your network and endpoints from these kinds of attacks.

So how can you protect your organization from letting these attacks into the network in the first place? And if an attack should somehow penetrate your network, how can you prevent it from propagating or moving laterally, infecting other systems in its wake?

Blocking Network Exploits

IPS (Intrusion Prevention System) is a critical security component of any next-gen firewall as it performs deep packet inspection of network traffic to identify vulnerability exploits and block them before they reach a target host. IPS looks for patterns or anomalies in the code that either match a specific exploit or a broader target vulnerability.

As with the EternalBlue exploit discussed earlier, these attacks typically attempt to send malicious inputs to a host application or service to compromise it and gain some level of control to ultimately execute code – such as a ransomware payload in the case of Wanna and Petya.

Blocking File-Based Ransomware Payloads

While Wanna and Petya spread like worms, many ransomware variants leverage social engineering tricks through phishing email attacks, spam, or web downloads to gain entry to your network through more conventional means. These attacks often start as cleverly crafted malware lurking in common files like Microsoft Office documents, PDFs, or executables such as updates for common trusted applications. Hackers have become very effective at making these files seem benign or obfuscating the malware to get past traditional signature-based antivirus detection.

As a result of this new breed of file-based malware, sandboxing technology has become an essential security layer at your network perimeter. Fortunately, cloud-based sandboxing typically doesn't require any additional hardware or software deployment – it simply identifies suspect files at the gateway and sends them to a safe sandboxing infrastructure in the cloud to detonate active content and monitor the behavior over time. It can be extremely effective at blocking unknown threats like new ransomware attacks before they enter the network.

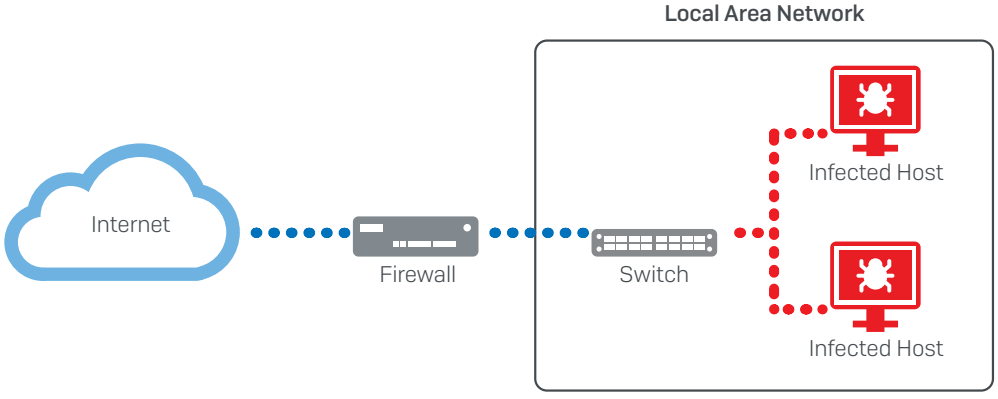
Best Practices for Firewall and Network Configuration

It's important to keep in mind that IPS, sandboxing and all other protection the firewall provides is only effective against traffic that is actually traversing the firewall and where suitable enforcement and protection policies are being applied to the firewall rules governing that traffic. So with that in mind, follow these best practices for preventing the spread of worm-like attacks on your network:

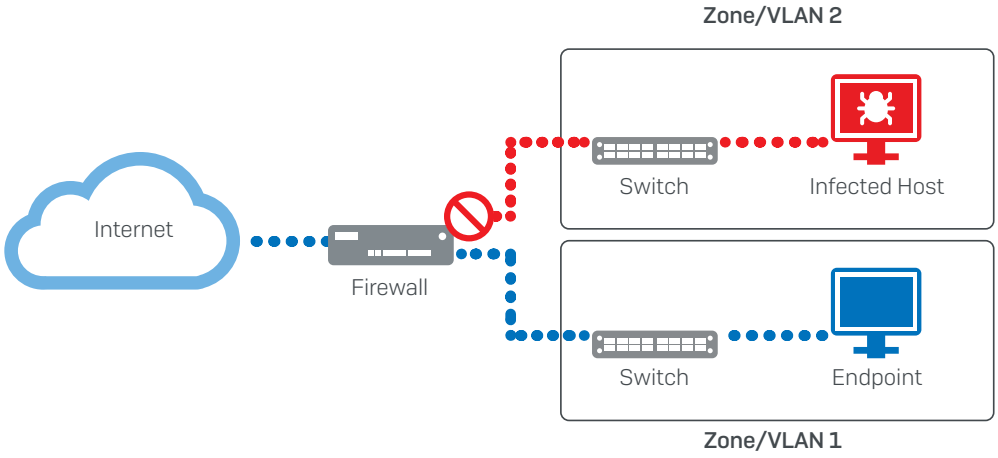
- **Ensure you have the right protection**, including a modern high-performance next-gen firewall IPS engine and sandboxing solution.
- **Reduce the surface area of attack** as much as possible by thoroughly reviewing and revisiting all port-forwarding rules to eliminate any non-essential open ports. Every open port represents a potential opening in your network. Where possible, use VPN to access resources on the internal network from outside rather than port-forwarding.
- **Be sure to properly secure any open ports** by applying suitable IPS protection to the rules governing that traffic.
- **Apply sandboxing to web and email traffic** to ensure all suspicious active files coming in through web downloads and as email attachments are being suitably analyzed for malicious behavior before they get onto your network.
- **Minimize the risk of lateral movement** within the network by segmenting LANs into smaller, isolated zones or VLANs that are secured and connected together by the firewall. Be sure to apply suitable IPS policies to rules governing the traffic traversing these LAN segments to prevent exploits, worms, and bots from spreading between LAN segments.
- **Automatically isolate infected systems.** When an infection hits, it's important that your IT security solution be able to quickly identify compromised systems and automatically isolate them until they can be cleaned up (either automatically or through manual intervention).

Segmenting LANs to Minimize Lateral Movement

Unfortunately, many organizations operate with a flat network topology – with all their endpoints connected into a common switch fabric. This topology compromises protection by enabling easy lateral movement or propagation of network attacks within the Local Area Network since the firewall has no visibility or control over the traffic through the switch.



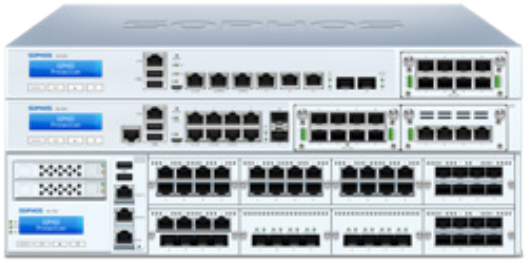
A best practice is to segment the LAN into smaller subnets using zones or VLANs and then connecting these together through the firewall to enable the application of anti-malware and IPS protection between segments that can effectively identify and block threats attempting to move laterally on the network.



Whether you use zones or VLANs depends on your network segmentation strategy and scope, but both offer similar security capabilities by providing the option to apply suitable security and control over traffic movement between segments. Zones are ideal for smaller segmentation strategies or networks with unmanaged switches. VLANs are the preferred method for segmenting internal networks in most cases and offer the ultimate in flexibility and scalability, but require the use (and configuration) of managed Layer 3 switches.

While it's a best practice to segment your network, there's no "best" way to segment a network. You can segment your network by user type (internal, contractors, guests), by department (sales, marketing, engineering), by service, device or role type (VoIP, Wi-Fi, IoT, computers, servers) or any combination that makes sense for your network architecture. But generally, you will want to segment less trusted and more vulnerable parts of your network from the rest, and also segment large networks into smaller segments all with the aim of reducing the risk of threat penetration and propagation.

Sophos XG Firewall



Sophos XG Firewall includes all the technology needed to help protect your organization from the latest attacks like Wanna and Petya. In particular, XG Firewall includes one of the best performing and most effective IPS engines on the market as recently confirmed by NSS Labs. Our IPS patterns are updated frequently to detect the latest vulnerabilities and, in the case of Wanna and Petya, had received pattern updates well before these outbreaks. And since the initial attacks, additional patterns have been added to catch new variants.

XG Firewall also enables excellent protection against the spread of attacks on your network, but as with any security product it must be given an opportunity to do its job. Proper deployment and configuration is key to reducing the surface area of attack and minimizing the risk and potential scope of propagation. XG Firewall offers flexible and easy segmentation tools like zones and VLANs to secure your LAN and reduce the risk of lateral movement.

Synchronized Security; Unparalleled Protection

Ransomware, botnets, and other advanced attacks will often work their way through your entire IT infrastructure. XG Firewall is part of the Sophos Synchronized Security ecosystem where security products actively work together to stop advanced attacks. The result: faster, better protection – and simpler IT security management.

For example, XG Firewall works with Sophos Intercept X, our anti-ransomware and anti-exploit solution proven to stop ransomware at the endpoint. They share real-time threat, health, and status information via our patented Security Heartbeat™, automatically responding to attacks – instantly identifying and isolating infected systems on the network while they are being cleaned up.

And you don't need to rip-and-replace anything to get all the great benefits of XG Firewall, Intercept X, and Synchronized Security. You can deploy XG Firewall in-line with your existing firewall, and Intercept X alongside your existing desktop antivirus client. Together they give you unparalleled protection against ransomware and other advanced attacks. It's next-gen protection against next-gen threats.

Core to Cloud
Address: Unit 5, Radcot Estate, Park Road, Faringdon, Oxfordshire, SN7 7BP, United Kingdom
Tel: +44 (0) 1367 701500
Email: info@coretocloud.co.uk
URL: www.coretocloud.co.uk

Learn more

and try for free at
www.sophos.com/xgfirewall

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

© Copyright 2017. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2017-07-12 WP-NA (NP)

CORE to CLOUD™

SOPHOS