UBM Tech

E-PAPER

FEBRUARY 2014

Next-Gen Security

SSL decryption and inspection keeps attackers away from your data and out of your network.

DELL | Network Security

1401069

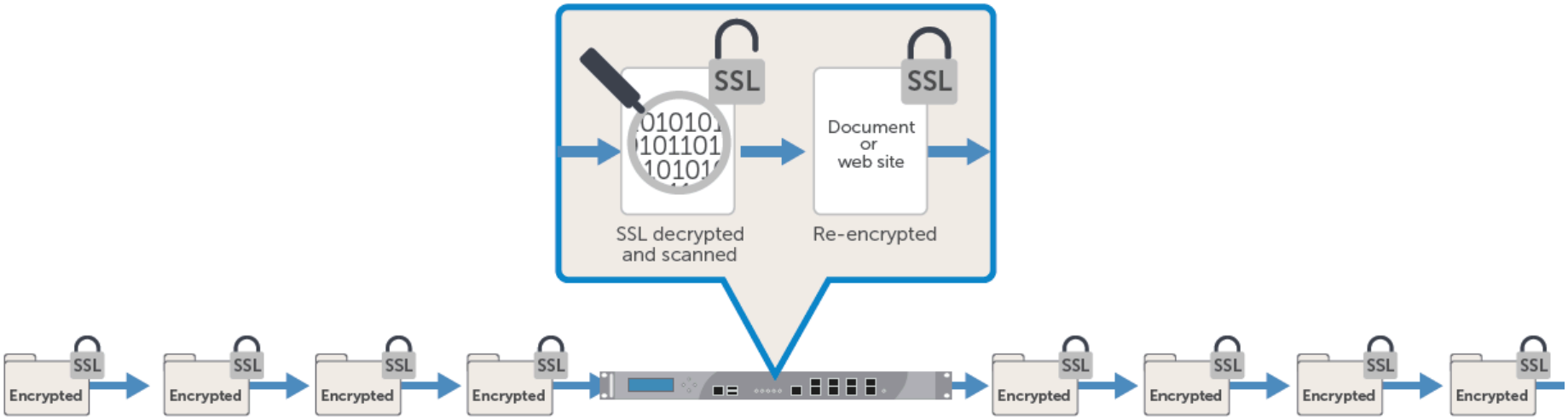
Today between 25 and 35 percent of enterprise traffic is secured using the secure sockets layer (SSL) protocol, according to NSS Labs. In some vertical industries SSL traffic comprises as much as 70 percent of network traffic. This is expected, since SSL is commonly used for everything from e-commerce to online banking. More recently, however, cybercriminals have started using SSL to hide their attacks. That turn of events has CIOs and other security professionals looking to SSL decryption and inspection technologies to improve enterprise security and reduce risk.

SSL is sandwiched between the underlying transport protocol (TCP) and an application or website, protecting data while it's in motion by creating an encrypted channel over the public Internet or a private network. At the same time, SSL provides a way for users to make sure the data's final destination is what it purports to be and not that of a hacker spoofing a well-known or trusted destination. This encrypted channel is a communication avenue that keeps data from being captured or compromised. SSL can be found within most Web browsers and servers, and it's there that the SSL process originates.

25% to 35%
The amount of network traffic using SSL — NSS Labs

The data sender initiates the SSL process with a "handshake." The client sends a hello message containing three elements — the key exchange method, cipher and hash — that essentially help the sender and recipient agree on an encryption method. The recipient's server responds with its own message, agreeing to use a specific key exchange algorithm. To authenticate itself, the recipient's server presents a certificate that contains its identity information, the validity period and additional public key details. The certificate is signed by a well-known trusted issuer, such as VeriSign, that the client can independently verify against third-party digital certificates it has preinstalled to make sure that the incoming traffic is trustworthy. The public key that the recipient's server provides is used by the client to encrypt secret information that's sent to the server as part of a handshake message; the recipient's server keeps a corresponding private key to itself. Only the recipient's server can decrypt the message the client sends, using its corresponding private key, to obtain the secret information. This secret information is then used by both client and server to independently derive the keys used to subsequently encrypt

Next-Gen Security in Action



Next-generation firewalls intercept the keys exchanged during the SSL process, and then open and decrypt SSL traffic to look for threats. Network traffic is inspected for nefarious activity, before being re-encrypted and sent to the recipient.

and decrypt traffic between them. Once the handshake is complete, data can be encrypted and sent.

This process is the reason that SSL can enable e-commerce and online banking. Crucial and sensitive data such as credit card information, user names and passwords are encrypted and transported in a way that makes it difficult for anyone but the intended recipient to access that data. While websites and FTP and telnet servers were the original users of SSL, today a wide variety of applications use the protocol, including Java-based applications, application management services and cloud-based services. Facebook and Twitter are two of the most popular SSL-enabled applications. Browser add-ons that can force the use of SSL via HTTPS are also available.

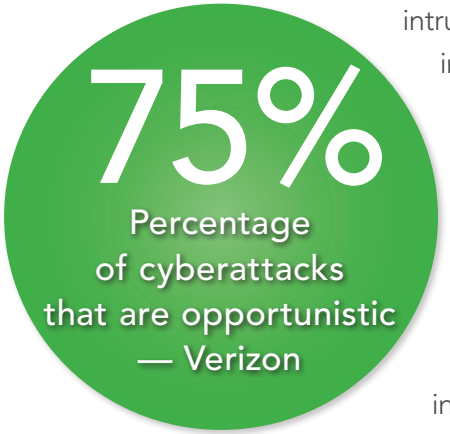
Hidden Threats

The ubiquitous use of SSL to improve security in one respect may be detrimental to overall enterprise security. SSL can "create 'blind spots' that can actually reduce security

on corporate networks because network security products and other defenses may not be able to monitor SSL traffic effectively or efficiently," according to NSS Labs.

Criminals are capitalizing on these blind spots, creating malware that leverages SSL and opens doors directly into the corporate network. By using SSL to hide attacks, criminals can bypass firewalls or other network security solutions, such as malware prevention and intrusion prevention systems. In addition, botnets and Trojans are increasingly using SSL to hide command-and-control traffic that lets hackers connect to and control compromised systems from virtually anywhere. One of the most frightening aspects of cyberattacks is that 75 percent of them are opportunistic, according to Verizon's "2013 Data Breach Investigations Report," and most are financially motivated. This means that organizations of all sizes, not just large enterprises, are at risk of becoming compromised.

Until recently SSL-encrypted attacks were rare; today, however, many experts agree that criminals are starting to use SSL more frequently to hide malware as it is being downloaded or to communicate with command-and-control servers. These situations create a huge threat to the enterprise, since SSL-encrypted attacks are likely to have a very high success rate. If the compromised host is using encrypted communications via its own SSL certificate to send and receive information from the client, many traditional firewall security solutions will let that traffic travel unexamined.



Next-Gen Security

The number of SSL-encrypted attacks is likely to increase, since many organizations are not inspecting SSL traffic for malicious code. Security professionals struggle with a Catch-22: How can they leave the integrity and privacy of SSL communication intact while ensuring security of the network and the data that's being exchanged?

There are tools, such as next-generation firewalls (NGFWs), that can help security pros identify and eliminate SSL-encrypted attacks. According to the Gartner IT Glossary (see *www.gartner.com/it-glossary/next-generation-firewalls-ngfws*), "Next-generation firewalls are deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall. An NGFW should not be confused with a stand-alone network intrusion prevention system (IPS), which includes a commodity or nonenterprise firewall, or a firewall and IPS in the same appliance that are not closely integrated."

NGFWs intercept keys during the exchange and use them to open and decrypt SSL sessions in real time. Network traffic is then inspected for exploits, malware and other nefarious activity before being re-encrypted and sent along to the user. If the NGFW finds a problem, the threat is isolated and never enters the

network. Essentially, NGFWs act as a man-in-the-middle, intercepting client requests and replacing the server's certificate with its own.

NGFW appliances can help boost overall network security due to their multi-faceted benefits. Companies and other organizations should seek to offset the SSL risk by deploying technology that is able to detect command-and-control traffic or malware callbacks via SSL.

However, as the amount of SSL traffic increases, the NGFW's ability to handle that traffic decreases significantly. NGFW SSL decryption leads to significant performance degradation, since most firewalls, including many NGFWs, don't have the power to do widespread analysis of SSL traffic.

In fact, once the level of SSL traffic surpasses 50 percent of a network's traffic, the performance of the majority of NGFWs on the market tanks, according to NSS Labs. Latency issues are no small problem, especially when you take into account that end-user experience can suffer if packet transport is slowed due to SSL decryption and inspection.

These concerns lead some companies to skip SSL decryption and inspection completely, leaving their networks and users vulnerable.

Real-world SSL decyption and inspection testing by several organizations has found some solid NGFW performers.

The Right Firewall

"Less than 20 percent of Internet connections today are secured using NGFWs. By year-end 2017, this will rise to 50 percent of the installed base," according to Gartner's "Magic Quadrant Intrusion Prevention Systems" report.[1] Given that, it's clear that many organizations are now starting to evaluate and assess NGFW offerings.

Choosing a firewall that protects against SSL-obscured malware, however,

THE DELL ADVANTAGE

The Dell SuperMassive Series Next-Generation Firewall delivers up to 40 Gbps of firewall throughput, 30 Gbps of intrusion prevention with application control and 12 Gbps of malware prevention. In addition to providing intrusion prevention, malware prevention and application control, Dell NGFWs also decrypt and inspect SSL communications at a very high rate.

Dell's NGFWs transparently decrypt, inspect and re-encrypt SSL traffic to allow security services to be applied to all network traffic. In fact, the Dell SuperMassive E10800 NGFW had the highest rated transactions-per-second (TSP) performance for onboard SSL decryption in a recent test, according to **NSS Labs**.

NetworkWorld also gave SuperMassive E10800 high marks. It was able to decrypt and inspect SSL traffic at rates of up to 4.8 Gbps. In addition, it successfully fielded 9.9 million connections at once and handled as many as 5,800 simulated users without errors. The device was easy to use. And most important, the SSL decryption and inspection lets it perform intrusion prevention, malware prevention, application control, bandwidth management and content/URL filtering on SSL traffic.

Click here to learn more about Dell's Connected Security solutions

can be a difficult task. Even vendors that claim to offer SSL decryption and inspection may not have the processing power to handle the level of SSL traffic moving across a network today.

However, real-world testing by several organizations has found some solid performers in the NGFW market. Dell's offerings stand out when it comes to SSL decryption and inspection. Dell's patented inspection technology exceeds basic NGFW considerations while also offering advanced security features and superior scalability.

While nearly all of Dell's network security appliances include SSL decryption technology, the SuperMassive Series Next-Generation Firewalls are specifically designed for organizations with heavy traffic needs. They have a multicore high-performance architecture with specialized security processors optimized for real-time SSL decryption and inspection regardless of the port used. (For more detail about Dell's SuperMassive Series, see story on p. 5.)

Given that SSL threats are likely to increase, it's more important than ever for businesses to consider purchasing next-generation firewalls, such as Dell's SuperMassive Series with its outstanding protection and high-performance results. Organizations must carefully assess the level of risk they're willing to take when it comes to SSL attacks and choose security offerings that can mitigate the most risks. After all, you can stop only the attacks that you can see, and a good NGFW lets you block SSL-encrypted attacks as they happen.

To learn more about the Dell SuperMassive NGFW series, visit www.dell.com/us/business/p/sonicwall-supermassive-series/pd. •

1. Gartner: "Magic Quadrant for Intrusion Prevention Systems;" Adam Hils, Greg Young, Jeremy D'Hoinne; Dec. 16, 2013.

SSL threats are likely to increase, so it's more important than ever to consider purchasing next-generation firewalls.

Dell Network Security products are part of Dell's Connected Security solutions for ensuring that customers won't have to sacrifice performance for security. Dell Connected Security gives organizations the power to solve their biggest security and compliance challenges today, while helping them better prepare for tomorrow. From the device to the data center to the cloud, Dell helps mitigate risks to enable the business. For more information, visit www.software.dell.com/solutions/security/.

Get more information about the Dell SuperMassive Series here