TREND ADVISOR:

Securing Networked Applications with Cryptographic Segmentation

The rules and economics of IT security have changed radically in the past two years.

Hacking attacks and data breaches are no longer mere nuisances or relatively trivial cases of “cyber graffiti” like in the past. The costs of breach cleanup in only one of the retail breaches last year could easily top half a billion dollars. In another case, a judge has cleared the way for banks to sue a retailer for negligence for letting a breach take place. We have witnessed impacts in terms of company valuations, reputations and even senior executive departures. Hack attacks now have a direct impact on the bottom line and company operations.

Why is this happening now?

We are witnessing the convergence of three long-term technology trends.

Easy sharing also means easy sharing with everybody, including potential hackers or insiders.

Trend 1: Digitization of sensitive data

Enterprises in a wide range of sectors have converted all manner of mission-critical data to digitized form, and placed this data on networks.

Previously this information resided on paper in a filing cabinet under lock and key.

But now enterprises have successfully digitized healthcare data, credit card information, financial transactions, proprietary secrets, system control data, student records and much more. Digitizing has brought amazing advantages to the business with increased efficiency, mobility, and a major boost to productivity thanks to the ability to share this data with employees, partners and customers, including across previously trusted enterprise perimeters.

But there's the dark side. Easy sharing also means easy sharing with everybody, including potential hackers or insiders. Having this information digitized means it can also be accessed by remote attackers or unauthorized insiders.

Trend 2: Hacking incentives on the rise

Modestly skilled hackers have gained access to everything, mission-critical data that they can hold hostage, or use for identity theft, or sell on the black market. There's tremendous financial incentive for hackers today. For example, experts estimated that hackers in only one of the recent retail breaches made off with credit card numbers worth more than $1 billion on the black market. There is an active and expanding market for virtually all types of hacked data and this incentive ensures that hackers will continue to test the limits of our security architectures.

Trend 3: Lagging security

The most common security architecture relies on the quaint notion that a firewalled perimeter can keep the bad guys out and that the enterprise has a "trusted" internal network. The idea is that a security architecture is like a piece of candy: "crunchy" on the outside, with strong firewalls, but "chewy" on the inside, with internal networks easily navigable for the sake of application access and performance.

As Target, Home Depot, Sony, Anthem and countless other data breach victims have shown, this belief is a dangerous fantasy.

Again and again, hackers compromised firewalls and then had complete freedom to access sensitive data on other systems in the internal networks.

Plugging this security hole is actually really straightforward: encrypt sensitive data traffic everywhere and use cryptographic segmentation to isolate sensitive applications even on internal networks. This requires adopting a "no trust" security model.

No Trust Security Models

Technology analysts have been advocating a "no trust" security model for years now, advising IT managers to assume the internal network cannot be trusted.

This means IT needs to encrypt the traffic of all sensitive applications even when they are hosted and accessed internally. This approach is predicated on these assumptions:

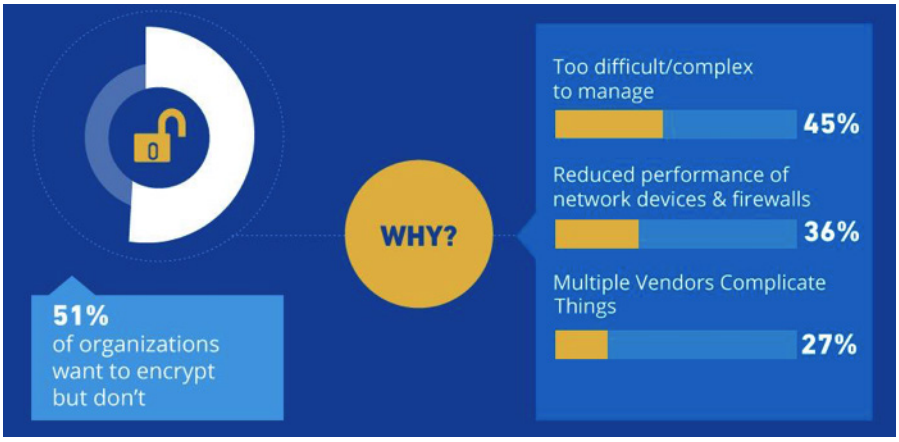
- Assume there is malware already in the LAN that could affect these applications. Assume the network perimeter has already been breached.
- Assume that hackers can remotely access a given system.
- Assume that logical network segmentation controls, such as VLANs and ACLs, are already compromised and easily bypassed, which is trivially easy for a script-kiddie hacker.

Encrypt traffic of all sensitive applications — even when hosted and accessed internally

51 percent of IT managers want to use encryption to protect sensitive application traffic

In late 2014, research service Spiceworks conducted a global survey of IT decision-makers to understand their challenges with protecting networked applications.

The survey found that 51 percent of IT managers want to use encryption to protect sensitive application traffic. But these managers are unable to perform cryptographic segmentation of sensitive traffic because of infrastructure shortcomings, including management issues and performance degradation.



Spiceworks Survey results on protecting sensitive networked applications – December 2014

First, more than 75 percent of IT managers have to use two or more different forms of encryption to secure a networked application from end-to-end across its entire path. More than a third reported having to use three or more forms of encryption.

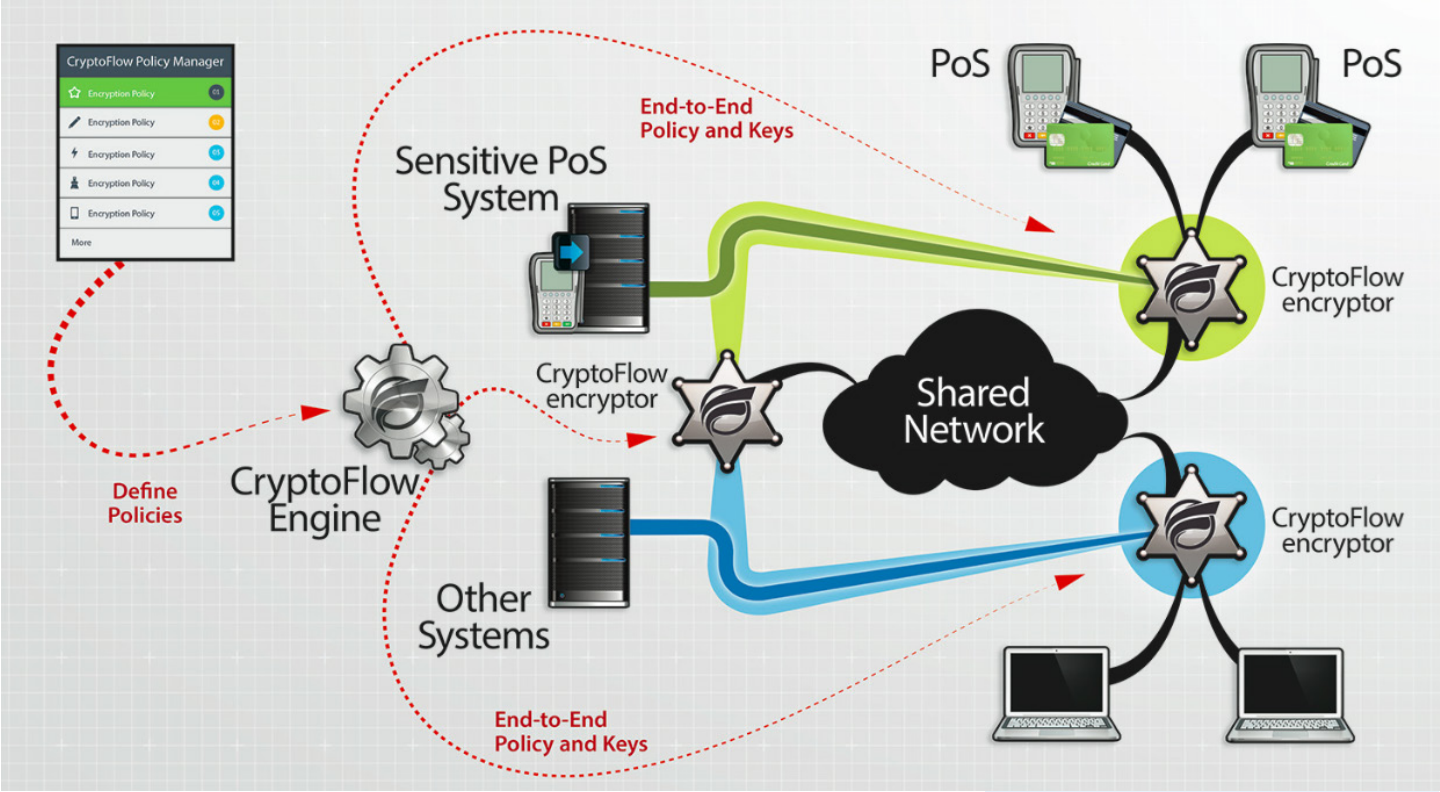
This fragmentation of data traffic encryption leads to configuration errors, difficulty with ensuring end-to-end protection and, frankly, too many wasted hours manually configuring arcane encryption policies on multiple systems.

Second, a little more than a third of the surveyed IT managers said they cannot use cryptographic segmentation because of reduced performance of firewalls and network devices when they are used to encrypt traffic.

Performance of typical firewalls and network devices will drop by 75 percent or more when encryption is turned on, mostly because of the processing toll on the system.

The good news is that cryptographic segmentation, the use of encryption on internal networks, is entirely possible and available today, thanks to products that separate the encryption of data traffic from the network functions themselves. Thousands of banks, governments, schools, hospitals and others are using cryptographic segmentation today for sensitive traffic over all types of networks. These companies generally fly under the security news radar because they are not being hacked.

The diagram below illustrates the utilization of internal cryptographic segmentation in a retail environment.



In this case, the application traffic for the Point of Sale systems has been isolated with cryptographic segmentation. This means the traffic and applications are fully segregated from the other applications that may share the enterprise environment. As a result, this retailer is fully protected from the main attack vector utilized in the high profile retail breaches that have dominated the security news over the past two years.

In the end, enterprises modernizing their security architectures will need to embrace the "no trust" model and put in place strong encryption controls to protect sensitive applications even on their internal networks. While nothing is a guarantee of security, cryptographic segmentation can go a long way toward keeping an enterprise out of the hacking headlines.

More information about the cryptographic segmentation of sensitive networked applications is available from Certes Networks. Visit CertesNetworks.com to learn more.

About Certes Networks

Certes Networks protects data in motion. The company's award-winning CryptoFlow™ Solutions safeguard data traffic in physical, virtual and Cloud environments, enabling secure connectivity over any infrastructure without compromising network device or application performance. Companies around the world rely on network encryption products from Certes Networks to protect data, accelerate application deployment, simplify network projects, reduce compliance costs, and improve the return on investment in IT infrastructure.

For more information visit CertesNetworks.com

Global Headquarters
300 Corporate Center Dr., Suite 140
Pittsburgh, PA 15108
Tel: +1(888) 833-1142
Fax: +1(412)262-2574
www.certesnetworks.com

North America Sales
sales@certesnetworks.com

Government Sales
fedsales@certesnetworks.com

Asia-Pacific Sales
apac@certesnetworks.com

Central & Latin America Sales
cala@certesnetworks.com

Europe, Middle East and Africa Sales
emea@certesnetworks.com

V1-03-31-2015