TREND ADVISOR:

Principles & Policies of Perpetual Paranoia:

The New Rules for Enterprise IT Security

Enterprise users are putting many more demands on IT security than ever before. At the same time, the IT security architecture is being tested by hackers at unprecedented levels.

In the middle of this “perfect storm” of demands and challenges, how is IT security to cope? How do the stakeholders in network, applications and information security departments gain clarity and alignment to ensure gaps are plugged and compliance needs are met?

An emerging best practice is to adopt a universal IT security policy built around “Perpetual Paranoia.” In other words, assume something will go wrong and you will never be disappointed.

Users, Water & Shadow IT

The demands of enterprise IT users have taken an increasingly troubling turn in recent years from a security perspective.

Users are like water. They follow the path of least resistance.

The phenomenon of "consumerization" of IT has been well documented for the past decade. The trend of employees wanting to use their own devices or personal applications for various work tasks is largely understood and the subject of numerous policies in the typical enterprise.

But consumerization has reached a critical tipping point recently.

First, many enterprises have succeeded in digitizing sensitive, mission-critical data that previously would have been on paper and largely kept under lock and key. Now patient data, financial data, consumer data, student data and many other types of sensitive information have been digitized for sharing and to maximize business operational efficiencies.

Second, consumer-oriented Cloud applications and powerful mobile apps have achieved widespread market penetration and user adoption. It's now possible for a user to easily push huge amounts of highly sensitive enterprise data onto a consumer-oriented Cloud storage service. Or users can choose to use a widening array of applications on laptops or mobile devices to communicate sensitive data completely out of the control or awareness of the IT or compliance managers.

A common approach for many IT shops has been to forbid users from utilizing personal devices, consumer-oriented Cloud services or other unauthorized apps.

But this approach blindly ignores a well-known principle: users are like water. They follow the path of least resistance. They will use the tools they know to get the job done.

Thus we have seen the rise of "Shadow IT," a whole host of unauthorized, untested and non-compliant applications used by enterprise employees, poised to give IT shops massive compliance headaches or worse.

IT security practitioners ignore this trend at their peril because they have no way to audit or control the security posture of these Shadow IT applications.

Principles & Policies of Perpetual Paranoia

Couple the rise of Shadow IT with the massive digitization of critical data, and you can have some serious IT security heartburn. Add to this the onslaught of hacking attacks, with new breaches being announced daily. The result is the perfect storm of IT security woes.

The most effective strategy in dealing with these forces is to assume that the security architecture will be breached and plan accordingly.

This is a policy or principle of "Perpetual Paranoia," the assumptions that malware is already present, that users with access cannot be fully trusted, and that the firewall ultimately will be breached.

Once this principle is embraced, it will drive several IT architecture and deployment decisions. Most notably, cryptographic segmentation of traffic becomes a best practice.

Internal & External Segmentation of Data Traffic

A common architectural principle has been to assume that internal networks, the segments inside the firewalled perimeter, are safe and trusted. Billions of stolen data records in the past two years have shown this assumption to be completely false.

The only way to protect the most sensitive application data is to use strong encryption to isolate the application and its traffic fully, including when it traverses internal networks.

Network segmentation of this type is often talked about but rarely implemented in practice because of the management challenges. Further, the devices typically used for this sort of segmentation – routers, switches and firewalls – experience huge performance degradation when they are

Assume that the security architecture will be breached and plan accordingly.

used to encrypt traffic in real time.

Nevertheless, enterprises are successfully deploying internal cryptographic segmentation of traffic by using traffic encryption tools that are decoupled from the network devices and the firewalls.

Orient security policies around users and applications, not network devices, links, segments or other parts of the infrastructure.

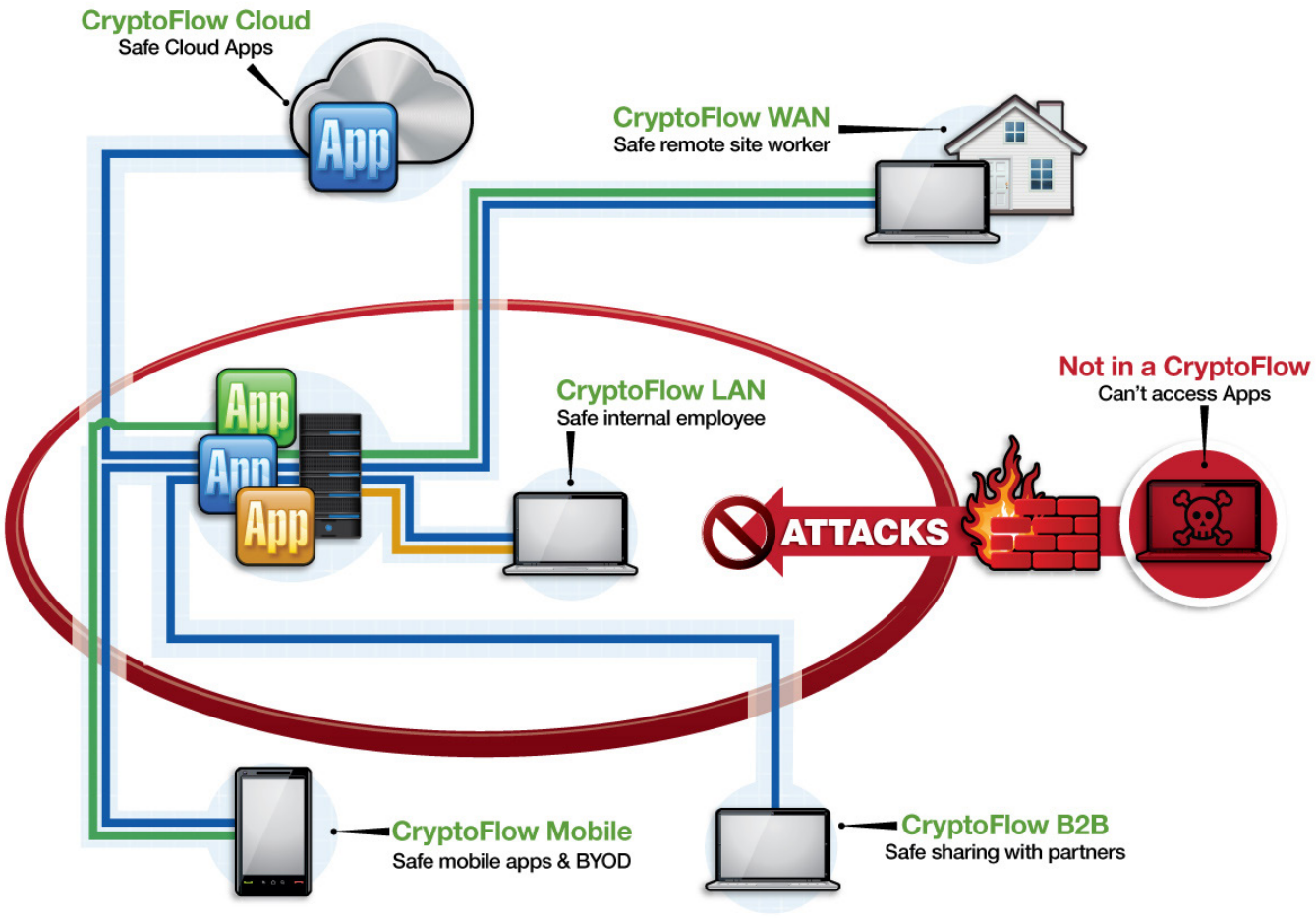
Segmentation and protection of traffic moving outside the enterprise perimeter has traditionally relied on VPNs. Typical VPNs focus on granting access for a trusted device to a trusted enterprise network. Once you do away with the erroneous notion that any networks can be fully trusted, this fundamental architectural principle must evolve as well.

The advanced approach is to identify the specific applications to be protected, align access with the users who should access them, and then actively secure that access from end to end, from the application in the data center or the Cloud to the end user, no matter which devices they are using.

This in turn means that the security policies need to be oriented around users and applications, not network devices, links, segments or other parts of the infrastructure.

Ultimately, this approach serves to address both the need for internal as well as external application segmentation. In fact, the most advanced enterprises can use the exact same centralize point of policy definition and management for cryptographic segmentation of traffic for both internal and external users. From a bird's eye view, if all networks are considered to be effectively untrusted, it should not matter which network the user is on. The same policies and the same cryptographic segmentation should be employed regardless. Further, as users move from network to network, such as from outside to inside the firewalled perimeter, what matters it that the security policy can follow that user and apply the protections consistently.

The diagram below illustrates such a deployment.



In this scenario, the enterprise has deployed cryptographic segmentation for applications extended to internal and external enterprise users, to authorized business parties, to a Cloud deployment, and so on. The attacker in the scenario is not part of any of the user-application security policies and so is not authorized to access any of the sensitive applications. As a result, even if the attacker succeeds in getting past the firewall, the sensitive applications are protected.

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