The Need for Secure Communications in a Distributed Environment
Summary
Distributed computing environments pose distinct threats to your information systems. Your organization needs to provide information to people when and where it’s required. At the same time, you need to properly identify each user, adjust their access accordingly, protect information in transit and protect your intellectual and physical assets in both remote locations and headquarters. Strong security for distributed environments requires systems that are designed to work together in a unified manner.

The Need For Secure Communications In A Distributed Environment

Information is only useful when it’s being used. Decision-makers need to have access to information at the right moment in time. Customers expect answers to their questions when they ask them. The days of 'I'll get back to you on that' are a thing of the past.

Organizations of all sizes have recognized the need to adjust their IT strategies accordingly. Remote access to your corporate network, once rare, is now commonplace. The Telework Research Institute estimates that in the United States, 20 to 30 million people currently work from home at least one day a week. 15 to 20 million are road warriors/mobile workers; and about 3 million are based at home full time1. IT departments need to react to this changing workforce and new business demands by providing safe, secure access to information wherever it is needed.

This opening of the network to remote access is no longer a technical problem. Bandwidth is inexpensive. DSL and cable modems are ubiquitous. WiFi access is available in most public spaces and 3G and 4G mobile networks are commonplace. Getting information to people is not a problem. Protecting information, unfortunately, is a problem. Users have to be properly identified, their devices protected, information in transit encrypted and the information residing in corporate headquarters protected. Any point in this distributed environment can be a point of attack and every point must be protected.

Organizations also face a regulatory environment as well as industry best practices that require them to protect sensitive information. For example, if your organization handles credit card information, you must comply with the Payment Card Industry Data Security Standard (PCI DSS), a demanding 12-point standard for ensuring cardholder data security. Retail organizations, financial institutions and service providers must ensure their IT infrastructure complies with PCI DSS or face heavy fines. In the United States, organizations that handle medical information are subject to the Health Insurance Portability and Accountability Act (HIPAA).

The Predicament: Making Security Technologies Work Together

The wide spectrum of threats requires a wide spectrum of technologies for end-to-end protection. Unfortunately, no single technology will, by itself, protect your data. For example, Virtual Private Network (VPN) encryption only prevents others from seeing the content of a remote communication. It doesn’t ensure that the content of the transmission is free of malware or the device tunneling into the corporate data network is compliant with corporate standards.

Security professionals use the concept of ‘defense in depth’ to describe the approach of using multiple layers of security to address the need to protect against a wide range of threats. A defense in depth design incorporates different security technologies that address different security issues throughout the IT system. The problem is that most of these defense mechanisms have not been designed to work together. In fact, many vendor solutions are far from complete. Solutions such as VPN are network centric, while other

---

1 Telework Research Network, February 2011
solutions are virus centric, or focus on firewall technologies. This can result in redundant, complex management, difficulties in trouble-shooting and added expense.

Furthermore, the lack of integration means that one hand doesn’t know what the other is doing—there is no aggregation of data to help security professionals ‘connect the dots’ and see patterns in the data. Instead, organizations rely on additional third party tools to help them extract specific, actionable information from the high volume of data. Security technologies must be designed to work as a comprehensive whole in order to be most effective. A recent article in the New York Times, entitled Security Professionals Say Network Breaches Are Rampant, put it this way; “I.T. departments must manage a growing array of specialized security technologies that may or may not work together to help security departments detect and halt attacks.”

Adding to this predicament, different users have different security requirements. You security system must take into account the fact that different levels of trust exist for different users. And, that level of trust will vary by location. Executives may need full access to network resources from remote locations. Other workers might require just web access and email. This impacts your security architecture in a variety of ways. For example, some users will require fully encrypted IPSec tunnels, while others, such as part-time contractors or partners, use SSL encryption. Users requiring full network access may have network access control technologies applied to their device as they are likely to be accessing a range of applications and sensitive data. Web content filtering will also vary from user to user, such as tightly controlling web access for one set of users while giving others more freedom.

Taking A Unified Approach
The nature of the security threat and the requirement for a variety of different security technologies requires a unified approach to security in a distributed environment. The various components need to be designed to work together. And they need to be managed in holistic manner. For any organization seeking to protect critical information, device and user management, threat and usage analysis and the creation and enforcement of policies is critical. Strong security requires the ability to fully understand the state of your IT environment at all times. And, your management technology needs to be simple and easy to use. Whatever complexities you have in a local environment are amplified in a distributed environment due the wide range of users and their geographic spread. A ‘single pane of glass’ approach is necessary to handle this complexity.

A system utilizing a variety of technologies that are designed to work together is critical. And, such a system must provide protection without impeding the normal operations of your organization. Good security shouldn’t slow people down. Security systems must be easy to use as well as powerful enough to inspect traffic without degrading network performance.

Protecting Information In Transit: IPSec and SSL VPNs.
VPN technology allows you to encrypt traffic as it transits the Internet from remote devices to corporate access points, preventing anyone who might intercept it from viewing the content. There are two types of VPNs; IPsec and Secure Sockets Layer (SSL). Each has its advantages and is appropriate for different types of users and deployments.

SSL-based VPNs allow connectivity from almost any Internet-enabled location using a Web browser and its native SSL encryption. There are two different types of SSL VPNs: client and clientless.

• Clientless SSL VPNs require no specialized software and are ideal for deployments where you

---

cannot easily provide a 'client' to the user such as employee-owned PCs, contractors and business partners. Only Web-enabled and some client-server applications (such as intranets, applications with Web interfaces, e-mail, calendaring, and file servers) can be accessed using a clientless connection.

- SSL VPN clients provide more complete access to network resources. A client resides on the remote device and allows access to the same applications and network resources employees use when in the office.

IPsec-based VPNs offer a technically different approach to remote access in how the encrypted tunnel is formed. Like client-based SSL VPNs, IPsec VPN connections are established using pre-installed VPN client software on the user desktop, thus focusing it primarily on company-managed desktops. IPsec VPNs are also used for site-to-site connectivity where remote branch offices are connected over the public Internet.

Both techniques offer strong protection as information transits the Internet. If you require a solution for a variety of different remote users, you should consider both SSL and IPsec technologies. For example, placing an IPsec client on those systems under your control and using clientless SSL-based connections for those systems you don't control. Whichever you choose, keep in mind that encryption alone does not offer complete protection. Just because an outsider cannot decipher encrypted data as it passes over the public Internet does not mean that the information is 'safe'. For example, without other protection, malware as well as legitimate traffic can be transmitted through a 'secure' VPN tunnel.

**Are You Really Who You Say You Are? Two-Factor Authentication**

Authenticating users before they access your network is critical. Unfortunately, simple username/passwords are not enough. Passwords can be guessed or hacked. And, despite constant reminders and training, end-users inevitably will engage in worst practices such as writing down their password and keeping it adjacent to their device or using weak, easily guessed passwords.

Two-factor authentication relies on the concept of 'something you know' and 'something you have' to provide stronger authentication than simple username/passwords. The 'something you know' is the user's own individual name and password. The 'something you have' is typically a small device or 'token' that the user possesses. Upon entering a password, the token provides a one-time password that is synchronized to the access server back at headquarters. This way, any unauthorized individual would have to possess both the user's individual password as well as the token itself in order to gain access. The utilization of two-factor authentication greatly reduces the potential that unauthorized individuals will gain access to network resources.

**Just Like Being In The Office: WAN Optimization**

Users accessing your network from a variety of locations expect to have their 'office' environment exist wherever they happen to be. This can be a problem as public Internet bandwidth speeds are often not adequate for data-intensive applications. In such circumstances, WAN Optimization can play a critical role. WAN Optimization uses various techniques to improve WAN performance. These techniques include protocol optimization, byte caching, web caching, SSL offloading, and secure tunneling to deliver improved performance of applications and networks while making remote workers more efficient:

- Protocol optimization can improve the efficiency of traffic that uses a variety of protocols. Byte caching caches files and other data on head-end units to reduce the amount of data transmitted across the WAN.
• Web caching stores web pages on those head-end units to reduce latency and delays between the WAN and web servers.
• SSL offloading offloads SSL decryption and encryption from web servers onto head-end SSL acceleration hardware.

Protecting The Rest Of The Network: Policy Enforcement

The weakest link in your security is often your most trusted employees. It's not that they have malicious intentions, it's just that they can allow threats to infiltrate your network via their remote access connections. For example, it's common for employees to visit non-work related sites while surfing the web, exposing them to malware. Your distributed network needs to ensure that only devices running approved applications are allowed onto the corporate network. Client software on the remote device can list the applications resident on that device. Then, as the device tries to sign onto the network, it is checked to ensure it is running only approved applications. If not, the user is denied access and told to remove the offending application before being allowed entry. If need be, network administrators can remove the application remotely.

Safe Surfing: Web Filtering

The use of the Internet within your organization offers both great improvements in productivity as well as the ability to expose your employees to harmful websites that may not be in compliance with your organization's code of conduct.

Web filtering technology can play an important role in enforcing your organization's security policies. Software residing on the endpoint device can be set to restrict access to websites that do not conform to policy, as well as block malicious sites that may try and infect your mobile devices with malware. As with other security technologies, web filtering tools require regular updates as the list of unacceptable sites is constantly evolving.

All Manner Of Threats: Antimalware

Malware or 'malicious software' is a broad term encompassing all manner of applications, files, and scripts designed to cause harm to a system. These consist of viruses, worms, bots, Trojan horses, spyware, adware, rootkits and scareware among others. Whether they are debilitating, engaged in data theft, or simply annoying, they need to be prevented and eradicated.

The challenge is that the nature of malware is constantly evolving. As a result any antimalware solution requires constant updating. In a distributed environment, an antimalware solution should reside on both the gateway device as well as the endpoint. This way, should the endpoint somehow get infected, the gateway device would prevent the infection from spreading to the rest of the network. Antimalware on the endpoint should also be coupled with policy enforcement at the gateway. This will ensure that the endpoint device has the most recent antimalware update prior to being allowed access to the network.

No Trespassing, No Unwanted Visitors: Personal Firewalls

Since every point on the network is a possible point of attack, every point should also act as a point of protection. Personal firewalls perform an important function within distributed environments. They control network traffic to and from a device, either allowing or disallowing connections. They can also help to make a device invisible to intruders by not responding to unsolicited network traffic as well as enforce data leakage policies.
As in antimalware technology, firewall technology should be deployed on both the endpoint device as well as the gateway device. As with many other technologies described in this document, it is essential to regularly update firewall policies as new threats arise and your organizational policies change.

The Fortinet Solution
Fortinet® offers a complete, unified, end-to-end enterprise security solution. The solution consists of FortiGate® devices at the network perimeter and a choice of FortiClient agents on the endpoint. Centralized management and analysis devices, FortiManager and FortiAnalyzer, allow you to easily manage the complete system. Virtual Machine versions of FortiGate, FortiManager and FortiAnalyzer devices also exist. The FortiGuard® Subscription Service provides comprehensive updates for both FortiGate devices as well as FortiClient endpoint clients. Real-time updates are available for antimalware, antispam, web filtering, intrusion prevention and application control security functions.

FortiGate
FortiGate appliances offer a unified approach to protecting against network, content, and application-level threats. Models are available to satisfy any deployment requirement from the FortiGate-30 series for small offices to the FortiGate-5000 series for very large enterprises, service providers and carriers. Dynamic updates from the FortiGuard Labs global threat research team ensure your systems are protected against the latest threats. FortiGate platforms incorporate sophisticated networking features, such as high availability (active/active, active/passive) for maximum network uptime, and virtual domain (VDOM) capabilities to separate various networks requiring different security policies.

FortiManager
The FortiManager family of appliances supply the tools needed to effectively manage any size Fortinet security infrastructure, from a few devices to thousands of appliances and end-point security agents. The appliances provide centralized policy-based provisioning, configuration, and update management for FortiGate, FortiWiFi, and FortiMail appliances, as well as FortiClient end point security agents. They also offer end-to-end network monitoring for added control.

FortiAnalyzer
FortiAnalyzer offers logging, analyzing, and reporting functionality from Fortinet devices and other syslog-compatible devices. Using a comprehensive suite of easily-customized reports, you can filter and review records, including traffic, event, virus, attack, Web content, and email data, mining the data to determine your security stance and assure regulatory compliance. FortiAnalyzer also provides advanced security management functions such as quarantined file archiving, event correlation, vulnerability assessments, traffic analysis, and archiving of email, Web access, instant messaging and file transfer content.

FortiClient
You have two choices for endpoint protection from Fortinet; FortiClient and FortiClient Premium. Both offer a choice of SSL or IPSec VPNs and both include WAN optimization, two factor authentication, application detection and enforcement, and policy compliance enforcement. The FortiClient Premium agent also includes antimalware, antispam, a personal firewall and Web filtering. Updates to FortiClient Premium are provided by the FortiGuard subscription service.
Fortinet Distributed Security Solution Architecture

For more information on Fortinet, visit [http://www.fortinet.com](http://www.fortinet.com)
For information on the FortiClient endpoint protection visit [www.fortinet.com/endpoint](http://www.fortinet.com/endpoint)