CIPHEROPTICS

Network Security Best Practices: 15 Minutes to Complete Data Protection

An illustration of a company transforming to complete data security in 15 minutes

Copyright © CipherOptics 2006. All rights reserved.

Table of Contents

Copyright © CipherOptics 2006. All rights reserved.

Protecting customer data

It's 10 o'clock. Do you know where your data is? If you think for just a moment, you'll realize that it could be anywhere in the world and you have no idea if it is protected or vulnerable. Your personal information is somewhere at your bank, sent over the Internet when you buy a book or CD online, and stored at your health insurance company, not to mention state, local and federal government agencies. Whether it's the potential of embarrassment or financial ruination, shouldn't your private information remain secret? A slew of government regulations imply that it should be. And yet, the security breaches keep coming. ChoicePoint, a name made famous by a huge breach in early 2005, has become a rallying point for organizations to re-examine their approach to data security.

Threat Identified:
Customer data could be exposed to unauthorized parties through a third party network provider.

Best Practice Defined:
Add encryption for data moving between data centers on a 3rd party MPLS service.

A simple Google search reveals there is a growing illicit market for sensitive, personal information. And with information like Social Security numbers, bank account and credit card numbers and corporate intellectual property widely available, it's time for organizations that house and use that data to get serious about protecting it.

As your customers trust their most important information to you, protecting networks with firewalls, intrusion detection and ID management are essential first steps, but protecting the data itself is the true goal. After all, because most network data is dynamic, it can be moving around the network at any given time. How do you approach securing that dynamic data? According to best practices espoused by top security experts, encrypting the data in motion over the network is key to protecting it. Once encrypted, when an unauthorized person is able to access it, customer records would be useless to them and your business would be protected. As organizations integrate encryption into their best practices for protecting data and complying with regulations, they often encounter highly complex, time-intensive and expensive solutions that, while protecting data, degrade network and application performance. Perhaps it's time to take a better approach to encryption as a means of data protection.

Is protecting data really that difficult?

You know you need to secure your data. But you have heard all the stories about how difficult the job of securing your data on your networks can become. Router upgrades with new software and new hardware, encryption accelerator add-ons so the router CPUs do not roll over, complicated ACL rules— the list just goes on.

Given all of these complicated tasks, protecting data can seem too difficult because we often look to the router to provide all the security we need. However, is that the best place to look for data protection? After all, routers route, switches switch and they need to be secure to perform their tasks. However, when routers are burdened with other tasks, such as encryption, implementation issues, management issues and network performance, issues arise. Maybe it's time to look outside the router and see the network as a system.

What if you could overlay security onto the network, in a cost effective architecture? With the strategic placement of encryption appliances throughout the network that security overlay is possible.

Copyright © CipherOptics 2006. All rights reserved.

Use Case: Personal Information Protection for Customers of an International Bank

A bank with multiple data centers elected to use a third party MPLS provider for data center-to data center connectivity. The benefits were financially motivated— they save on telecommunications expenses by switching to MPLS. But they were concerned about what happens to their customers' financial data if the MPLS provider misconfigured a switch. The chain of trust on the customer data would be broken. They had no way of assuring that there was no customer data leakage between the two data centers.

Threat Identified:
The current network infrastructure couldn't adequately isolate and separate confidential and proprietary information between two companies sharing a single campus.

Best Practice Defined:
Add encryption for data moving between communities of interest to protect confidential and proprietary corporate

Their solution was to add authentication and encryption to the bank's existing router/switch infrastructure. The required architecture was quickly self-evident. Two CipherOptics appliances created a secure tunnel over the MPLS infrastructure, preventing any unintended data leakage. No router infrastructure upgrades were required, no complicated project plan needed. Just plug in the CipherOptics appliances, add the encryption policy and watch it work. The link is secure.

Bank --Benefits of CipherOptics appliance approach

- Cost savings – enabled toll-bypass of telecommunications company by using MPLS
- Customer information protection – prevented data leakage in cases of misconfigured switches
- Investment proof – network overlay or "bump in the wire" appliance

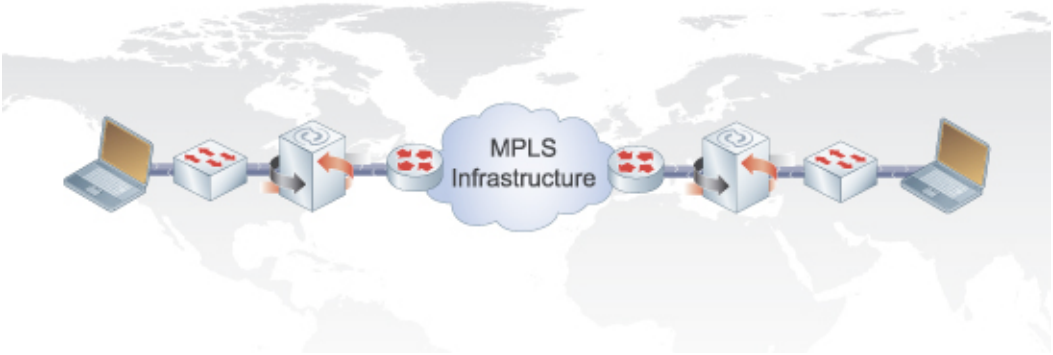

Figure 1: International Bank – Secure MPLS Infrastructure Diagram

Use Case: Fortune 100 Corporation – Securing 12 Links in 4 Hours

Another example is a Fortune 100 corporation using a local gigabit fiber ring to connect their campus buildings. In this case they were not changing the telecommunications provider, they were changing their business operations and sharing common campus network facilities with a new company.

Copyright © CipherOptics 2006. All rights reserved.

The business opportunity involved selling one of their operating units, which meant that employees of the new company would be sharing the campus-networking infrastructure with the selling company. Everyone was highly concerned that the proprietary and confidential data that traversed this shared common networking environment could, and would, be inadvertently shared with unauthorized people in different companies. Therefore, a requirement of the sale was the complete lockdown and isolation of the data network, preventing the unauthorized access of vital confidential and proprietary intellectual property.

The focus of the project was to secure 12 vital communication paths within the common infrastructure. These communication paths were traversing shared-media Ethernet hubs and switches in-route to the routing points within the network. These communication paths linked various R&D labs that were scattered across the campus. The customer had provisioned VLANs within the network to create community of interest networks, however VLANs only separate data flows and may be compromised by any user with a data analyzer could obtain access to everything on the network (or accessing the built in network diagnostic tools of many routers):

- VLANs have been shown to leak when routers get congested
- Configuration errors that send information to the wrong destination.

Because of the short time frame to implement, the sensitivity of situation, and the improvement of data being secured, the customer's IT organization took on the task of doing the complete installation.

Figure 2 depicts an illustration of the technology customer's network before adding the CipherOptics appliances.

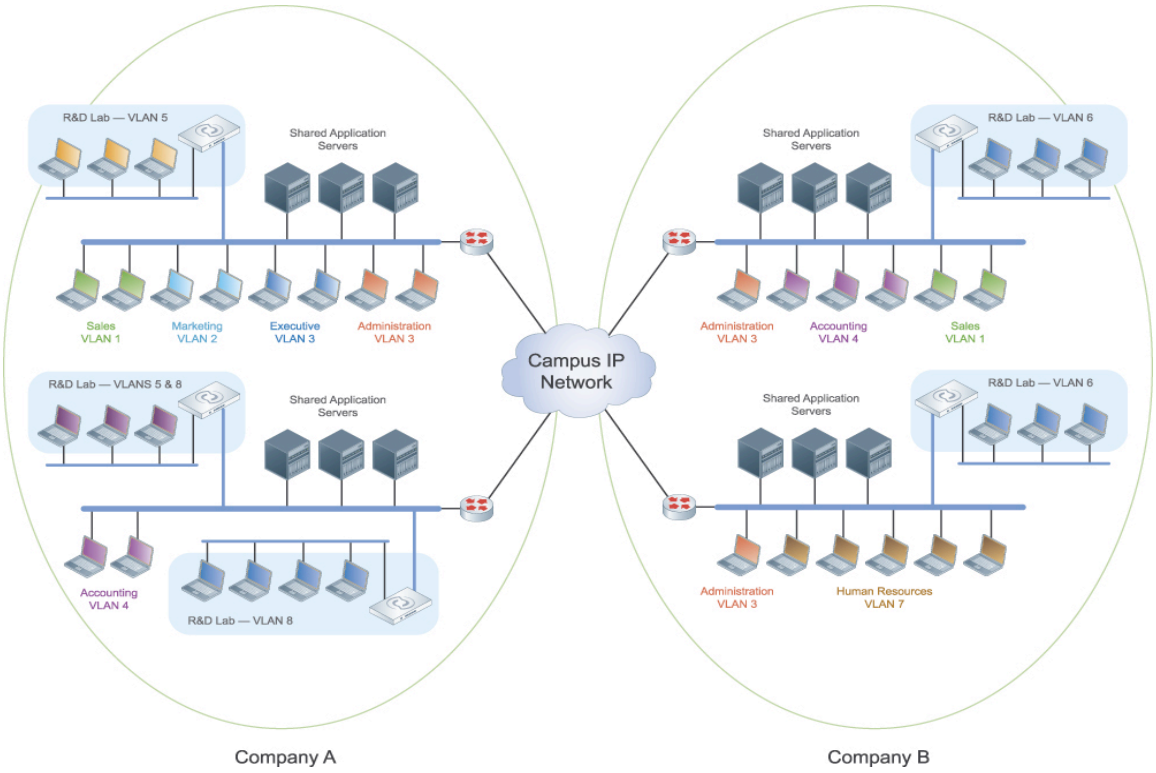

Figure 2: Fortune 100 Corporation – unsecured network diagram

Copyright © CipherOptics 2006. All rights reserved.

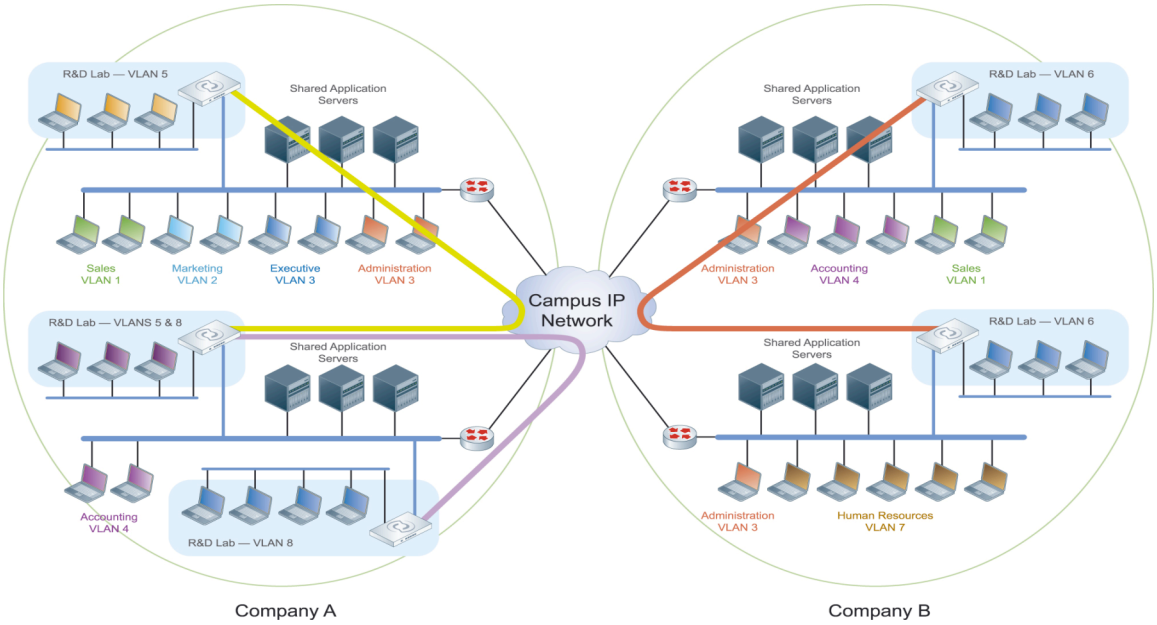

Figure 3: shows connectivity paths on the Fortune 100 corporations network

Once the connectivity paths were known for the various locations, it became a simple matter of installing the CipherOptics' appliances at all connection points into the R&D labs.

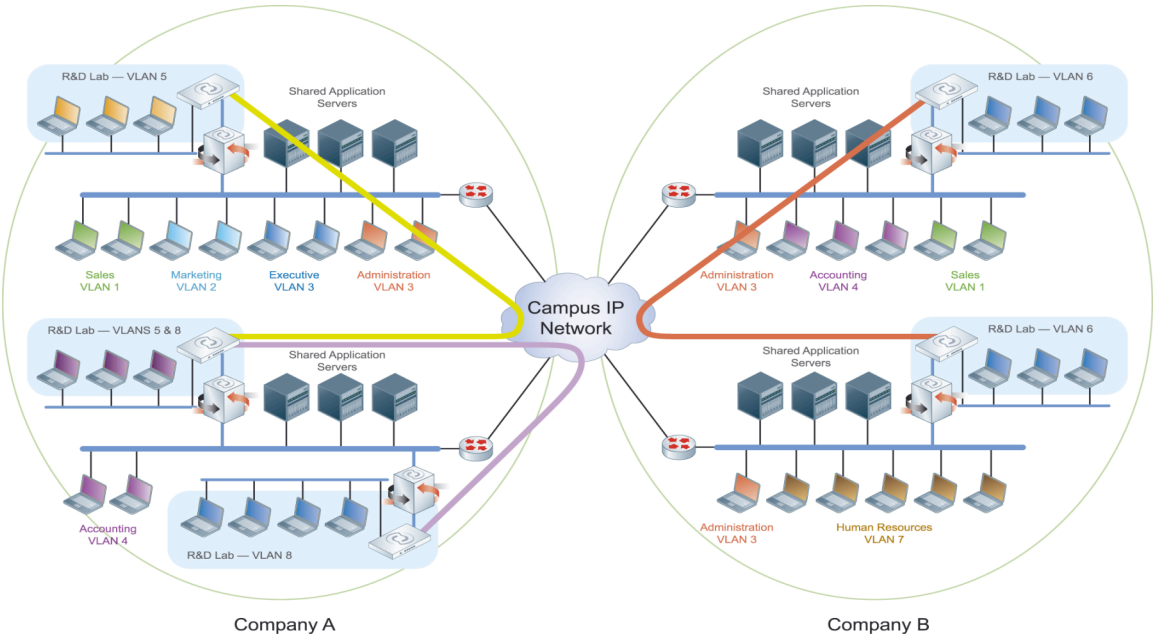

Figure 4: Fortune 100 Corporation –connectivity paths diagram

Copyright © CipherOptics 2006. All rights reserved.

With the CipherOptics appliances installed and security policies activated the connectivity paths between the various R&D labs were then fully functional and protected from all unauthorized access.

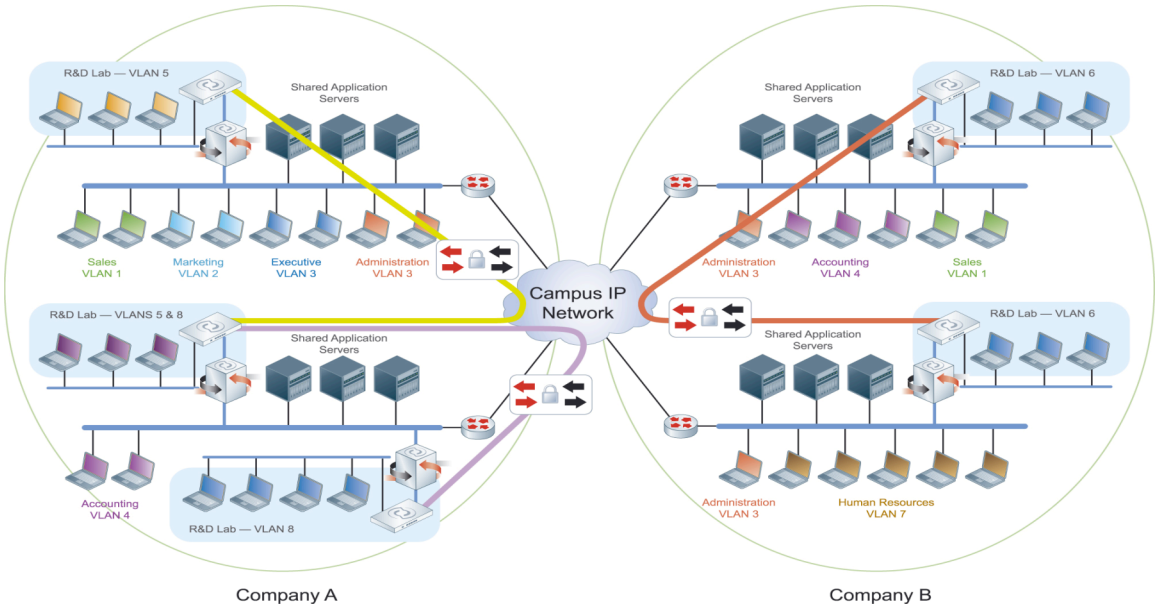

Figure 5: Fortune 100 Corporation – secure network diagram

The results from the actual installation and activation were astounding. The customer's IT organization had a single person do the implementation of 24 CipherOptics IPSec Security Gateways. The total time to complete the entire installation, including the un-packaging, rack mounting of the devices, cabling and provisioning was 4 hours from start to finish.

Fortune 100 Corporation—Benefits of the CipherOptics Appliance Approach

- Fast installation – 24 appliances self-installed in under 4 hours
- Zero network downtime – installation occurred during business hours without causing downtime
- Completely transparent – No impact on network or application performance
- Investment protection – Minimal cost for infrastructure upgrade
- Encryption enforced – New network segmentation guarantee

Securing your data can be easy

Data security appears complicated because networks themselves are extremely complicated. Access rules, end-user authentication, network authentication, encryption algorithms, and hashing algorithms are not easy to implement and maintain. But, that doesn't mean securing your data needs to be hard. Security solutions, from CipherOptics, remove the complexity and allow you to quickly and simply secure your infrastructure.

There is nothing wrong with upgrading your routers and switches — you do that as a matter of course depending on topology changes and user demands. But upgrading routers and switches just to add data protection often doesn't pass the financial test. Its time to change the way we look at security and think outside the router. CipherOptics security solutions install transparently to any network, regardless of size, type or

Copyright © CipherOptics 2006. All rights reserved.

topology. We provide network-wide security, so you can share your information without impacting your network.

CipherOptics CipherEngine enables Secure Information Sharing on a network-wide scale. Let's face it, networks were created to share information with people or devices. The information on your network is the lifeblood of your business. If cyber thieves steel, or even sell, your business critical information, it could cost hundreds of millions of dollars, not to mention the loss of customers, brand equity, or company image. You can't stop sharing your information across the network; however, you can secure it with CipherOptics network-wide security solutions.

About CipherOptics

CipherOptics is the leader in network-wide encryption. Offering an innovative policy and key management solution, coupled with high speed, low latency encryption technology, CipherOptics helps their customers mitigate the risk of data leakage, loss and theft over any network. For additional information, visit www.CipherOptics.com

Copyright © CipherOptics 2006. All rights reserved.