



iPolicy Networks' Intrusion Prevention Firewall safeguards Consumers Professional Credit Union from external and internal attacks. The system addresses several NCUA 748.0 and state of Michigan OFIS CISP security requirements and can easily adapt to new security applications.

Case Study

EXECUTIVE SUMMARY

Industry: Financial Services

Environment:

Consumers Professional Credit Union serves groups in Lansing, Battle Creek, and Eaton Rapids, Michigan. The credit union's main office and remote branches are connected by point-to-point communication lines.

Key Business Challenge:

- Identify when external and internal attacks occur on the credit union's network
- Stop and prevent attacks from happening
- Keep applications protected 24/7
- Leverage limited resources
- Access to meaningful security reports

Key Business Solution:

- Installed iPolicy's firewall and Intrusion detection system module to detect attacks
- Implemented iPolicy's intrusion prevention system to block viruses and worms
- Redundant system deployed to keep network running in the event of system failure

Key Business Benefit:

Members' sensitive financial information kept highly secure and accessible 24 hours a day, 365 days a year. Provides compliance towards applicable security regulations. The iPolicy investment can adapt to new types of security threats

Background

For over 50 years, Consumers Professional Credit Union (CPCU) has been the financial institution of choice for employee groups of businesses, schools, and churches in the Lansing, Michigan region. A full service credit union offering both online and in-house banking to over 7200 members, CPCU has additional branches in Battle Creek and Eaton Rapids.

In a recent poll on CPCU's website, an overwhelming majority of responders voted the financial institution as "the best credit union ever." And clearly, CPCU places customer relations and satisfaction at a premium. With consumer privacy becoming a growing public concern, CPCU has taken decisive and pre-emptive steps to protect the sensitive information of its members.

Challenge

Cyber attacks on financial networks are on the rise. And as online banking increases in popularity with consumers, credit unions that offer this convenient service to customers are prime targets for outside hackers.

CPCU's technical department had determined that the credit union's existing security was outdated for today's sophisticated attackers. What's more, the hardware that ran these security applications were single points-of-failure. In other words, if the security system went down, there were no redundancy measures in place to block attacks. This clearly posed a problem for a credit union that offered 24/7 financial services.

And finally, existing reports did not translate security data in an easy to understand format for management, operations, and auditors.

"We have been using iPolicy Networks' Intrusion Prevention Firewalls for some time now and I would highly recommend iPolicy's products to anyone who wants their networks truly protected. Their high performance, feature-rich security applications, and timely updates keep our network secured at all times."

Nick Cappelletti, Consumers Professional Credit Union, IT Supervisor

Existing Issues

CPCU's previous firewall and intrusion detection system (IDS) were outdated single components, and they did not work in sync together. The firewall looked at information packets to see where they came from, and if they were going to approved places. The IDS system looked inside the packet for worms and viruses, but only alerted or noted the suspicious activity. A technical employee would need to take manual action to remove any anomalies. In a 24/7 environment, this was not a practical arrangement and many times it was too late to stop the exploit.

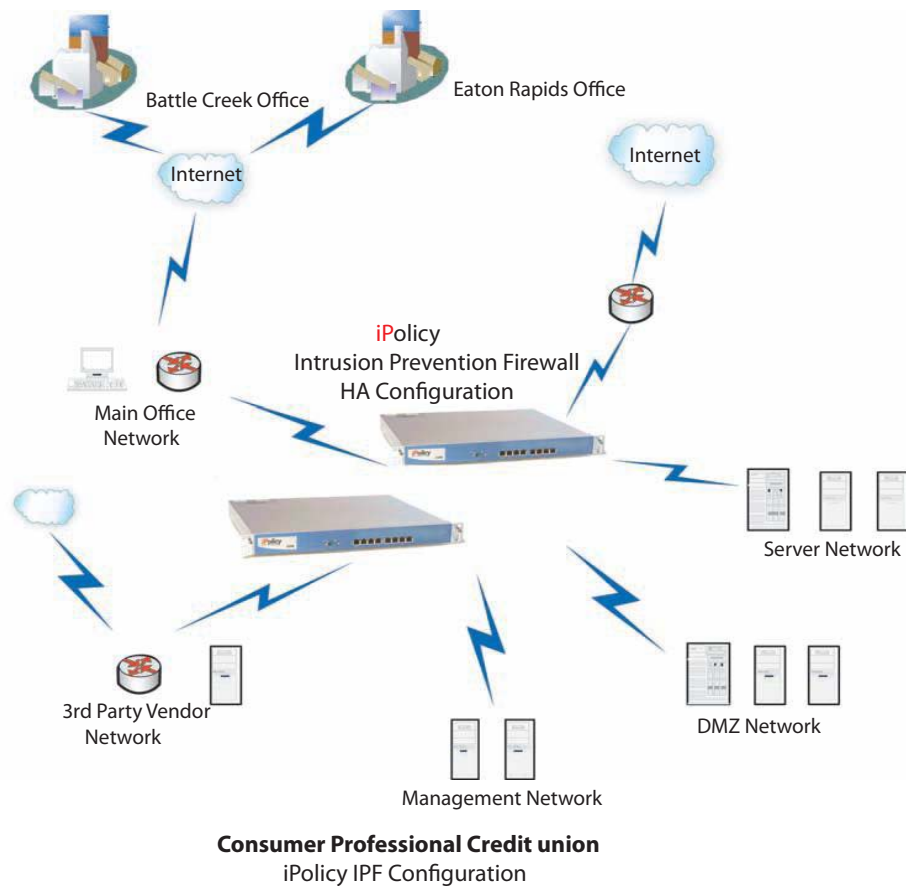
Another serious issue CPCU faced was lengthy downtime in the event of a security system failure. For a credit union that prided itself on high levels of customer satisfaction, this was simply not acceptable. Yet, the current network did not offer a "mirror" version that would stay up if the other went down.

Emerging Issues

While external network attacks are a primary concern, the unfortunate reality is that employees can also pose a threat to the internal network security. This can be unintentional, for example, when an employee or contractor accidentally inserts a worm or virus from a CD, a USB memory stick, or plugs in an unprotected laptop. But there have certainly been cases in the financial world where employees have purposely hacked into databases containing sensitive information. Member confidence is paramount in an increasingly Internet-based financial operation.

CPCU realized that as hackers have become more advanced in their techniques, then so must the security systems that combat them. Therefore, the new security platform put in place must provide perimeter and internal security, and easily adapt to new applications.

Figure 1 - Network diagram showing deployment of iPolicy's Intrusion Prevention Firewall 3300



Solution

CPCU installed two iPolicy Intrusion Prevention Firewall 3300's working in a high availability configuration to protect against outside and inside attacks. The iPolicy system delivers layer 3 to 7 stateful inspection firewall services, intrusion detection, and adds intrusion prevention services that collectively monitors, identifies attacks, and protects the network in real time. The high availability configuration provides 24/7 security uptime. The reporting system delivers meaningful information in graphic form that can be tailored to report on key assets. Additional applications, such as Web Filtering, can be easily added to the iPolicy security platform with the same familiar administrative tools without loss of performance.

Summary

CPCU continues to keep member information privacy its most important priority. Today, key business applications are secured and available 24 hours a day, 365 days a year. Of course, as online applications grow in popularity, so will CPCU's need to stay ahead of would-be hackers. With this in mind, the credit union will be evaluating additional iPolicy Networks security applications.