"One of the nice things about the ConSentry platform is that it logs all the traffic that comes through," says Randy Potts, Town North Banks' information security engineer." This gives us more knowledge about our network. I can see who's trying to use IM or peer-to-peer clients, which is a great benefit." Previously, IT had to use multiple tools and check traffic on a server-by-server basis to get the information ConSentry's InSight now provides in a single place.

ConSentry Helps Town North Bank Achieve PCI Compliance

Bankcard processing is a strong growth area for Town North Bank, one of the largest independent banks in North Dallas. As of mid-2007, the company's TNB Card Services division owned and operated the credit card portfolios of more than 125 credit unions. As this business grew, so did the impetus for IT to segment network traffic and set up access controls to comply with the Payment Card Industry (PCI) Data Security Standard (DSS).

Founded in 1972, Town North Bank today has assets of $1 billion and provides banking services ranging from commercial lending to financial planning. Its card services division offers full service bankcard processing and agent issuing to financial institutions throughout the U.S. With this portion of its business expanding, the bank needed to take steps to protect cardholder data in accordance with the PCI security standard. Given that the bank's LAN was completely flat with no virtual LAN (VLANs) or other internal access controls in place, the IT team had its work cut out for itself.

"Externally we have a great network, but internally our network was lacking a lot in terms of security and controlling user access. We had no segmentation on the network," says Randy Potts, information security engineer. "Auditors always gave us a crooked eye about it."

Fundamental to protecting cardholder data is the ability to restrict, by user, who can access what data on the LAN. The bank's IT staff initially planned to implement a series of VLANs to segment the network and access control lists (ACLs) to control user access to resources. However, the inflexibility of VLANs and the high management overhead of setting up and maintaining ACLs gave the IT staff pause. Fortunately, personnel at value-added reseller Vigilar, which specializes in PCI compliance and other security services, recommended the bank deploy ConSentry Networks' LAN security platform. A recent PCI audit proved that was sound advice.

SIDESTEPPING VLAN HEADACHES

The bank's primary requirement was to segment traffic so that credit card data was protected as it was processed, stored, and transmitted. VLANs seemed an obvious solution, so IT hired a Cisco networking consultant to help them work out a VLAN structure.

"Each department was going to be its own VLAN," Potts says. "But we realized that trying to use our Cisco gear to do access control was going to require too

Town North Bank

About Town North Bank

Town North Bank is a leading financial institution in the Dallas/Fort Worth Metro area. Founded in 1972, Town North Bank today has assets of $1 billion and provides banking services ranging from commercial lending to financial planning. Its card services division offers full service bankcard processing and agent issuing to financial institutions throughout the U.S.

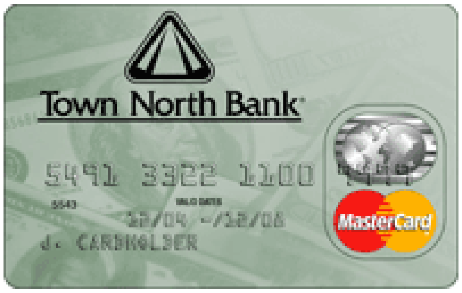
The Challenge

Needed to segment network traffic and set up role-based access controls to comply with the Payment Card Industry (PCI) Data Security Standard (DSS).

The ConSentry Solution

ConSentry's LANShield platform enabled Town North Bank to deliver role-based access controls and segment the LAN without using complex VLANs and ACLS.

much overhead. It was going to take way too much management and way too much time to do ACLs for all of our switches and routers. And, knowing how routing works between VLANs, we were probably going to add a good bit of latency to our network."



After Vigilar suggested ConSentry's LANShield platform, the IT team also investigated Cisco security solutions. "But they didn't even compare with the ConSentry product," says Potts. Available as an appliance or wiring closet switch, ConSentry's LANShield platform delivers a suite of security services encompassing admission control, traffic visibility, identity-based access control, and threat control, including anomaly detection and malware containment.

The LANShield Controller is installed between the wiring closet and network core and requires no changes to an organization's existing IT infrastructure or to desktops. The LANShield Switch provides full per-port security control in a gigabit Ethernet wiring-closet switch. The bank purchased Controllers for its primary operation center in Dallas and its disaster recovery back-up location, along with the InSight Command Center. InSight's graphical user interface makes it easy for IT to see and control all network traffic on a per-user, per-flow basis as well as to define role-based access policies and malware control policies.

"The ConSentry Controller does both pre-connect and post-connect filtering, allowing us to segment users away from servers and lock down access through sets of policies," Potts says. "ConSentry offers the most non-obtrusive and granular approach to segmenting traffic that we've seen. And it requires the least amount of down time to implement.

"If we changed our VLAN configuration floor by floor, we'd need to make numerous changes to our core switch and to the users," Potts adds. "ConSentry lets us do the same thing, but it takes days as opposed to a month to implement. Plus we avoided all the little issues that pop up with VLAN segmentation and ACLs. That's what made ConSentry such an easy choice – it was recommended by a vendor we trust, and it was just so low overhead to implement."

Currently, the IT staff has all user access switches feeding through the Controller to the rest of the network. The bank has also purchased a LANShield Switch, which has been deployed in its disaster recovery site.

"The PCI auditor told us that the ConSentry implementation far exceeded their expectations and provides better compliance than solutions from any major vendor they've seen."

Randy Potts, *Information Security Engineer, Town North Bank*

RESTRICTING ACCESS TO CARDHOLDER DATA

The LANShield platform's network admission control (NAC), identity-based access controls, and visibility capabilities are helping Town North Bank address PCI requirements much more comprehensively than a simple VLAN architecture could. For example, the bank is using ConSentry's NAC feature to strictly limit who can access network resources. "If you're an authenticated user, you have relatively free rein. If you're unauthenticated, you get nowhere – you don't even get Internet access," Potts says.

For network admission control, ConSentry supports passive and active authentication as well as host posture check. With passive authentication, the platform watches users authenticate to back-end identity stores such as RADIUS and Active Directory, verifying that users have authenticated successfully. ConSentry also offers active authentication, in which the LANShield platform actively challenges a user for authentication information via a browser-based captive portal. This capability allows IT to extend admission control to users, such as guests, contractors, and vendors, whose machines aren't under IT's management and whose names are not in the directory store. Through these admission control capabilities, the LANShield platform prevents any new device, including a wireless access point, from passing any traffic without first authenticating, thus blocking rogue devices.

Once users are admitted to the network, ConSentry's identity-based post-admission controls give granular control over what resources users can access. After the LANShield platform learns a user's identity, usernames are bound to an IP and MAC address. As a result, LANShield platforms can track and control individual user's application flows, files opened and closed, and the use of printers, VoIP phones, and other resources. Because these controls are tied to a username and not a machine address, they apply to users regardless of how they connect to the network, whether they're attaching locally via a wired or wireless connection or connecting remotely through a VPN.

LANShield platforms perform Layer 2-7 deep packet inspection and full Layer 7 application decode, enabling them to identify and control network traffic at a granular level. And because ConSentry platforms tie all LAN activity back to a username, it's easy to define and implement identity-based access controls.

IT can strictly limit access to cardholder data and related resources by creating the appropriate policies. For example, IT can define the role "PCI user" and limit access to cardholder data to users with that role, denying users in any other role access to that data. IT could further limit PCI user access to cardholder data to specific times of day, by address, by location, or other parameters.

Similarly, IT could define an access policy that blocks traffic from unknown addresses, and one that provides an alert if any protocol tries to access cardholder data other than those needed for cardholder data environments. ConSentry's support for access controls based on address, application, and user group gives IT has complete flexibility in defining access policies.

> *"ConSentry allowed us to segment our network without having to deploy a complex and difficult VLAN structure."*
>
> **Randy Potts,** *Information Security Engineer, Town North Bank*

PLANNING OUT POLICIES

Town North Bank is a small organization relative to other places Potts has worked – there are some 250 employees and 20 access switches in one building. "I've worked at places where we had 5,000 users and close to 60 sites, and we did access control on Cisco devices using ACLs," notes Potts. "We were controlling by MAC address, so this user could only be on that switch, for example. If I had ConSentry at that site, I could have controlled users through policies. It would have saved an enormous amount of time on that job."

Though the scale is smaller at Town North Bank, ConSentry is easing the burden considerably for the IT staff of four and providing significant benefits for the bank over using VLANs. A key benefit is that ConSentry de-couples access control from the physical infrastructure, so controls apply wherever a user connects to the network.

"If we'd done standard ACLs on our switches, we would have ended up with a situation where a fourth floor card person, who had to be on the first floor explaining something to somebody, wouldn't be able to bring up all the same applications and data as they could on the fourth floor," says Potts. "With ConSentry, wherever users log in, they can see whatever they have access rights to see. It's given us more flexibility in where we put people."

And knowing how much overhead VLANs entail, Potts is happy to have avoided them. "ConSentry allowed us to segment our network without having to deploy a complex and difficult VLAN structure," says Potts. "Instead of having to create a VLAN for card people, a VLAN for bank people, a VLAN for accounting folks, etc., we can throw all the users into one VLAN and all the servers into another VLAN and use the ConSentry platform to control which users can access which servers."

Being able to segment users from servers and restrict access based on someone's job position is a significant benefit, Potts says. "With ConSentry, we can identify those people in our card services business unit who need access to cardholder data and what application systems need access. Going forward we'll create policies based on the need to access sensitive data," he says.

Potts plans to restrict which user accounts access servers with cardholder data, as well as to limit by MAC and IP address what systems talk to each other. "Before, pretty much any user could get to any server," Potts notes. "Now with ConSentry we have the ability to say this group of users can only get to these servers, and this group of users can only get to those servers. And we can segment PCI-specific servers from the rest of the servers."

Using ConSentry's visibility feature, Potts is monitoring user traffic to determine which resources users access on a daily basis. With this information, he plans to create ever more granular access controls based on an implicit deny policy. "I want to lock down traffic internally just as we do externally with our firewall," he says.

"The IT team also investigated Cisco security solutions. But they didn't even compare with the ConSentry product."

Randy Potts, *Information Security Engineer, Town North Bank*

COMPREHENSIVE AUDIT TRAIL

In addition to being able to segment traffic and protect cardholder data, the PCI DSS requires that financial organizations demonstrate to auditors that such controls are in place and be able to provide a granular traffic history. ConSentry helps IT meet this requirement through InSight's detailed usage logs. InSight retains recent data within its database and supports archiving to outside database schemes for longer-term retention.

InSight enables IT to capture and view network traffic data as well as set policies. It aggregates all captured data and presents IT with actionable information, showing key security incidents in at-a-glance summaries and drill-down, detailed views. InSight also enables rapid forensic troubleshooting, auditing, and reporting. For example, InSight reports can detail every username that has accessed cardholder resources. It can retain a complete log of all interactions with any system; for each event, it can indicate user identity, application, type of event, date and time, success or failure, origination of event, and identity or name of affected data, system component, or resource.

"One of the nice things about the ConSentry platform is that it logs all the traffic that comes through," says Potts. "This gives us more knowledge about our network. I can see who's trying to use IM or peer-to-peer clients, which is a great benefit." Previously, IT had to use multiple tools and check traffic on a server-by-server basis to get the information ConSentry's InSight now provides in a single place, according to Potts.

In addition to having audit data readily at hand, having segmented the network using ConSentry access controls simplifies the audit process by reducing the scope of the devices included in the audit. "We're moving our cardholder data environment to its own network segment and strictly controlling access to them. So rather than having a hundred servers in scope, we only have ten," Potts says.

Beyond helping Town North Bank address PCI requirements, ConSentry is making troubleshooting easier for IT. "The LANShield Controller is like a marrying an IDS [Intrusion Detection System] and a firewall," says Potts. "Policy-wise, it's a lot like our firewall, since we configure roles and apply policies. But it's much better than any IDS I've every used for watching traffic. None offers the same nice, easy-to-use search function. With InSight, if I see that Jan on the third floor is having trouble, I can go to authenticated users, find Jan, and see what traffic of hers is going through and what's not. Then I can pass that off to the help desk. It's a great troubleshooting tool."

PCI COMPLIANCE AND MORE

Achieving PCI compliance is critical to Town North Bank's continued success in the bankcard processing business. "You can't be in the credit card business if you're not meeting PCI requirements," notes Potts.

A recent audit assured the bank that the ConSentry LANShield Controller's traffic segmentation and access control mechanisms provide good compensating controls for some pieces of the PCI DSS specification. Likewise, ConSentry's auditing and reporting capabilities are solid. "The auditor told us that the ConSentry implementation far exceeded their expectations and provides better compliance than solutions from any major vendor they've seen," Potts says.

"ConSentry is supporting a primary business activity. And it's saved us quite a bit of money," he adds. Thanks to ConSentry, "three IT people can focus on other things rather than access control. We don't have the complexity of managing a VLAN structure, which would have taken two full-time employees plus help desk folks a month to create. As the credit card business grows, we'd have had to rethink our VLAN structure. It would be an exponential change involving lost time and lost revenue.

> *"ConSentry is supporting a primary business activity. And it's saved us quite a bit of money."*
>
> **Randy Potts,** *Information Security Engineer, Town North Bank*

"In contrast, ConSentry took one week to set up. Having a centralized way to create and apply access controls is great. And with ConSentry, if I make a mistake on a policy, it's easy to fix, unlike a mistake with a VLAN and ACLs. One person can manage the Controller," Potts notes.

ConSentry also eliminated the need for the bank to buy a separate monitoring and reporting solution. "ConSentry saved us having to buy a $50K or $100K device just for logging database and file server access," says Potts.

By providing a cost-effective, easy to deploy, and simple to manage LAN security solution, ConSentry is enabling Town North Bank to comply with PCI DSS requirements and continue to grow its credit card processing business. IT has more visibility into network traffic than ever before and the ease of operating the LANShield Controller means IT has time to dedicate to other projects.

ABOUT CONSENTRY NETWORKS

ConSentry Networks delivers secure switching, enabling enterprises to control every user and secure every port on the LAN through its LANShield product family—the LANShield™ Switch, LANShield Controller, and InSight™ Command Center. More than 150 enterprises today rely on ConSentry's award-winning secure-switching platforms to protect their corporate assets, ensure continuity of operations, and dramatically reduce the risk of security breaches. ConSentry is backed by blue-chip venture capital firms Accel Partners, DAG Ventures, INVESCO Private Capital, and Sequoia Capital; and is headquartered in Milpitas, California.

Corporate Headquarters
ConSentry Networks
1690 McCandless Drive
Milpitas CA 95035
Phone 408.956.2100
Fax 408.956.2199
Toll-Free 866.841.9100
Email info@consentry.com
www.consentry.com

Worldwide Locations
London, United Kingdom
Phone +44 (0) 00870 351 9494

Frankfurt, Germany
Phone +49 69677 33 4

Tokyo, Japan
Phone +813 5532 7630

For a complete listing of all our
office locations go to:
www.consentry.com/company.html

CONSENTRY™ NETWORKS