

Social Housing Program Protects Network Inside and Out



EXECUTIVE SUMMARY

Organization: New Charter Housing Trust

Industry: Public Housing Association

Location: United Kingdom

Employees/Rental Units: 1000 employees; 20,000 rental units

Business Challenge

- Integrate new networks into existing IT infrastructure
- Keep public Internet sites safe and secure for all residents
- Secure corporate network from unauthorized connections

Security Solution

- Cisco ASA 5545-X Next Generation Firewall
- Cisco Cloud Web Security
- Cisco Identity Services Engine

Business Results

- Reliable, secure access for residents in sheltered housing
- Control access to network, applications, and websites
- Role-based access managed from central platform

New Charter Housing Trust uses Cisco Next-Generation Firewall to deliver secure Internet access to staff and residents.

Business Challenge

New Charter Housing Trust Group (New Charter) is a social housing authority, located in the Manchester region of the United Kingdom. The organization has approximately 20,000 housing units serving area citizens. New Charter works to provide accommodations that are affordable to people on low incomes, and limits to rent increases set by law mean that rents are kept at reasonable rates. Residents also include at-risk individuals or families who previously were homeless or in abusive relationships and need a fresh start.

The IT department provides services for the New Charter corporate staff of approximately 1000, as well as IT services onsite at the housing units. Providing both corporate and public networks is a big job in its own right, but the company is also actively increasing its housing stock and must integrate newly acquired sites and services into the network on an ongoing basis.

“We have to integrate these units into New Charter’s existing IT network. On the face of it, you’d think that wouldn’t be too difficult,” says Darren Fishwick, telecommunications and network manager for New Charter. “But sometimes we run into massive incompatibilities with some of the legacy hardware and software.”

In addition, Fishwick and the IT team at New Charter need to help ensure that the networks at existing and new locations are secure and that web-based filtering is in place.

“When we first implemented the resident PCs, we didn’t put any filtering on, because we were of a mind that we didn’t want to filter or restrict what people could access. But unfortunately, people are people, and we had a certain minority that was accessing things they shouldn’t,” Fishwick says.

“The thing that makes Cisco Security products great is that you put them in, and they run, and they run, and they run. You can turn them on and forget about them.”

Darren Fishwick

Telecommunications and Network Manager
New Charter Housing Trust

Finally, New Charter needed to develop role-based access for its corporate network. “We had a supplier come in to do a bit of work for us, and it took us several hours to realize that all he’d done was disconnect the PC at the desk he was working at and connect his own laptop. This, of course, goes totally against our policy and highlighted that we need to ensure that people can’t just come along and connect to our network,” says Fishwick.

Security Solution

New Charter has long used Cisco products to help create a secure, reliable network. “The thing that makes Cisco security products great is that you put them in, and they run, and they run, and they run. You can turn them on and forget about them,” says Fishwick.

At the center of its security infrastructure, the organization uses the latest firewall platform, leveraging the Cisco® ASA 5545-X Next-Generation Firewall with Intrusion Detection and Prevention. The organization also uses the Cisco Cloud Web Security Connector for ASA to extend web security and control without additional hardware expense.

Cisco AnyConnect® is deployed to allow corporate tablet users to connect to the New Charter VPN. Cisco Identity Services Engine (ISE) is also being implemented, proscribing which users and devices can access which parts of the network; it is a key component of the organization’s bring-your-own-device policy.

Fishwick never lets go of the organization’s Cisco equipment. He finds it useful when working to integrate new housing sites into the New Charter network. “There can be a lot of head scratching as we try to figure out why the systems aren’t integrating. Recently we resolved an integration problem by using some older Cisco routers. I had the equipment just hanging around in the cupboards, and I configured them for the sites,” he says. “They worked perfectly the minute we deployed them. That’s Cisco for you.”

The New Charter team also uses Cisco Catalyst® switches, as well as Cisco Wireless LAN Controllers, and Cisco Wireless Access Points.

Business Results

The new 5545-X Next-Generation Firewall platform is helping New Charter to improve its bandwidth capabilities. “The compression code in the ASA is helping us with bandwidth issues. It’s a much better user experience,” says Fishwick. “The compression assists the data throughput, whether a user is coming from within the organization or from outside via a web browser. This means the user isn’t waiting for a screen refresh or for a full page to load.”

The improved user interface and instant visibility are other features Fishwick cites as important improvements. “We can log in, more easily provide alerts, and the throughput updates are tremendous.”

The Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) capabilities keep the New Charter network secure and available. “It provides protection from the outside world, and it is a big bad world out there,” Fishwick says. “It’s surprising to look at the potential intrusions and see where in the world they’re coming from. We’re not even a very large network, but people try daily to hack in.”

“I’m using the ASA connector to push traffic onto the Cloud Web Security. I also actually push all our help desk requests and information through that. If it’s good enough for me and the team, it’s good enough for anybody. I practice what I preach.”

Darren Fishwick

Telecommunications and Network Manager
New Charter Housing Trust

Fishwick also appreciates the Botnet Traffic Filter capabilities of the Cisco ASA 5545-X. “IPS and IDS gives New Charter protection from the outside world. But the botnet filter looks at connections inside your network going out, looking for anomalies.”

Cisco Cloud Web Security (CWS) is used for guest traffic. In the past, New Charter used to provide a bypass, but Fishwick says it introduced too much risk. CWS protects users across the public and private networks. “I’m using the ASA connector to push traffic onto the Cloud Web Security. I also actually push all our help desk requests and information through that. If it’s good enough for me and the team, it’s good enough for anybody. I practice what I preach,” says Fishwick.

Cisco CWS also allows New Charter to control what applications and websites public users are allowed to access. Fishwick says, “As much as I don’t mind what people do in their own homes, the PCs in our housing units are in public locations, so we must have some controls on them so our network isn’t compromised. With the Cloud Web Security, we just branch the traffic off through the Cisco ASA and they’re blocked from going to places they shouldn’t.”

Using Cisco ISE for both wired and wireless connections lets the organization ensure role-based access to their network. ISE will also let New Charter provide full guest access for residents who live in sheltered housing, accommodations for those who need additional support in their living environment. “We don’t just want to provide a common PC for residents to use, but rather, full access to a public wireless network. Currently, we’re using just the Cisco Wireless Access Points. ISE will allow us to come from a central platform to leverage both tools for more granular access levels,” Fishwick says.

“The integration of the ASA 5545-X with ISE and TrustSec will mean that when users come into network, the Change of Authorization will enable us to more easily make changes in the posture assessment, as needed,” says Fishwick. “Using TrustSec’s Security Group Tagging inline will allow us to streamline changes to the firewall rules and our Access Control Lists (ACLs).” The IT team can update the antivirus, file availability, and more, ensuring that people joining the network have the up-to-the-minute level of access and security.

Fishwick also says, “It was very easy to implement. I can see the benefits of having an end-to-end solution to allow access control built into the Ethernet packet. This will also be extremely useful when controlling remote access users and BYOD.”

Next Steps

New Charter is now considering using the Cisco Cloud Web Security for all its web filtering. “We have to manage the appliance internally. It will be quite nice to manage all web filtering in the cloud, instead of just part of it,” says Fishwick.

The organization is also considering Cisco Security Manager. “Security Manager is proactive, so you don’t have to rely on IT staff going in and checking on the logins to see whether there have been any potential attacks on the network. We need that process to be proactive.”

For More Information

To find out more about the Cisco ASA 5545-X Next-Generation Firewall, go to:

- <http://www.cisco.com/go/asa>
- <http://www.cisco.com/go/anyconnect>
- <http://www.cisco.com/go/ise>
- <http://www.cisco.com/go/cws>

PRODUCT LIST

Security

- Cisco AnyConnect®
- Cisco ASA 5545-X Next-Generation Firewall
- Cisco Cloud Web Security Connector for ASA
- Cisco Identity Services Engine

Routers and Switches

- Cisco Catalyst® 4506E Supervisor Engine-7-E
- Cisco 877W Integrated Services Routers
- Cisco 887V Integrated Services Routers

Data Center

- Cisco Catalyst 4506E Switch
- Cisco Catalyst 3750-X Series Switches

Wireless

- Cisco 3201 Mobile Access Routers
- Cisco Aironet® 3502I-E-K9 Wireless Access Points
- Cisco 2106 Wireless LAN Controllers
- Cisco 5508 Wireless Controllers



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)