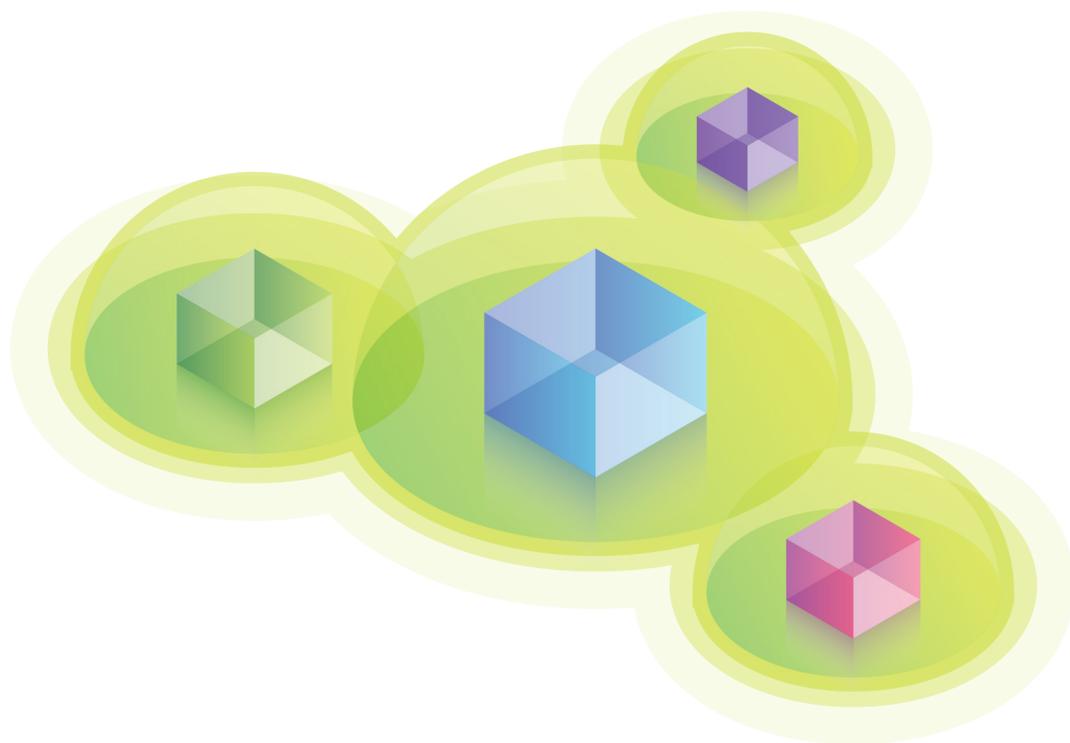


SOPHOS

Security made simple.



Simplifying Branch Office Security

By **Udo Kerst**, Director Product Management Network Security

It is more important than ever to secure your business. Malware, botnets and other malicious programs threaten your network, both at your central offices and your branch offices. Yet enforcing consistent network security throughout your enterprise can be challenging - especially for those branch offices with few users and no IT expertise on-site.

This paper introduces an innovative, cost-effective solution for managing branch office security.

Branch office security—what are the real problems?

Today's increased mobility and 24/7, always-on capabilities may offer your business a competitive edge. But the transmission of sensitive data across business networks and the Internet must be secure. Hackers and malware can easily target any vulnerability in your business.

But to avoid weaknesses in your defenses, your branch offices need exactly the same firewall protection, secure VPN connections, intrusion prevention systems, web and email security as your headquarters.

Three crucial points when managing branch office security

1. Deploying security devices

A small office with just a few workers often doesn't warrant dedicated IT expertise onsite. But many companies simply can't afford to send their IT teams on the road to set up new offices in different locations. Some pre-configure each device at the central office but often need to make final adjustments onsite. A dedicated central management solution that's easy to set up and configure offers the most efficient approach. But it can be as costly—as sending IT out on the road.

2. Providing support

When your branch office or remote worker has a technical problem, business and productivity can come to a halt. Describing issues over the phone is far too complex and frustrating for both your IT staff and your offsite employees.

Shipping the device back and forth is a non-starter. No one can afford the downtime. Your workers need virtual onsite support that helps them get back to business.

3. Implementing security policies

You need to determine how to set up rules and policies for your workers on the network at the individual branch offices. These rules may be the same set of rules you use at the central office. Or they may be different. Some branch workers and remote employees may have unlimited access to company assets and others may be highly restricted. You may want to implement policies that restrict access to Internet software or social media.

How can you manage this cost-effectively and efficiently? Sometimes corporate policies can be extrapolated into the branch office environment. If not, managing separate rules on different security devices is time-consuming and inefficient.

Traditional security measures for very small offices

Investigating the right solution for branch office security is a challenge especially when remote workers have little IT expertise. Many smaller offices start with consumer broadband routers which may be inexpensive and simpler for your remote workers, but they provide little reporting, visibility and only the most basic security. Others deploy entry-level business firewalls to inspect traffic and enforce policies, which offer greater security, visibility and control.

Here are a few of the traditional solutions you may have reviewed:

Low-end unified threat management (UTM) appliances may offer you the required security protection for your industry. However, they are time-consuming to set up. And you may find that the “hidden” costs—ongoing maintenance, subscription fees and management—are too high. Especially if you need to secure large numbers of small offices.

Consumer grade routers may seem like an inexpensive alternative to UTM appliances as they are easier to set up. While they offer you basic security functionality (e.g., firewall or VPN), they often lack important commercial security safeguards like intrusion prevention, web and email filtering. And they have to be managed individually, which can be tiresome if you deploy a number of them.

Managed VPN or MPLS services offer the most comprehensive solution that is centrally managed. However VPN or MPLS services are not available for all locations, and may lock you into long-term service contracts or might not comply with your corporate policies.

The bottom line is these traditional solutions don't meet your needs. Managing multiple point solutions increases the complexity of your network. It even increases when adding numerous point solutions at branch offices. But a new approach is now available. It is the ideal solution—even for a home office with one user, and it offers the benefits of fully automated central management.

A new approach for branch office security: Central management made easy

An innovative approach opts for a truly unified threat management solution integrating security measures at the branch offices into the corporate structure. This solution sets up a virtual Ethernet cable to connect your central and branch offices. Instead of running firewall, VPN, intrusion prevention, web and email security functions on an expensive branch office device, they are centrally provisioned by a powerful security gateway. It can be located at your central office or in the cloud (e.g. at a service provider).

A small remote Ethernet device (RED) forwards encrypted traffic from the remote office to a central device that scans and filters the data before it is sent to the Internet. It connects your central office to your branch office with secure VPN technology.

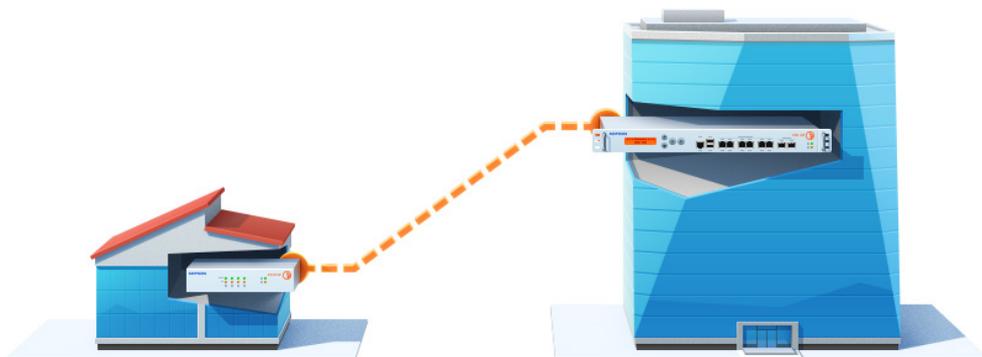


Fig. 1: Complete UTM security through virtual Ethernet cable

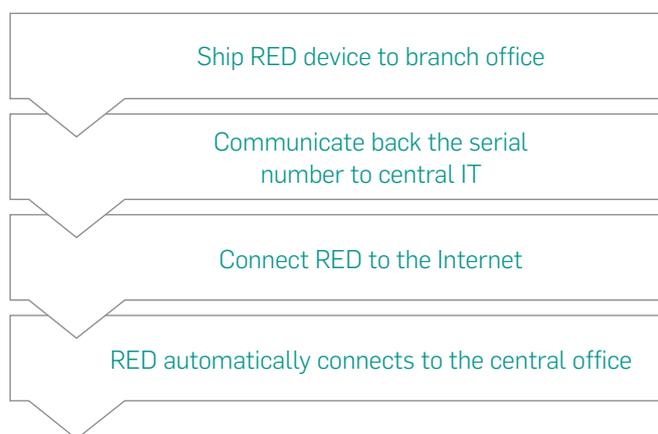
Two-minute deployment

Here's how it works:

RED devices are shipped to the branch offices. The remote worker reads the serial number on the shipping box to central office IT. They activate the device within the central Sophos UTM. The local employee plugs the device into the Internet router, connects the router to the computer and plugs it into the wall. The RED device automatically retrieves its setup information, configures itself and establishes an encrypted tunnel to the central office.

You can deploy up to 100 appliances per day with this automated, flexible solution.

Four easy steps to ensure branch office security:



Central support

RED delivers greater network control and visibility. Your IT staff now have an integrated solution at hand that supports clear centralized reporting tools offering full visibility into each branch office. RED eliminates onsite travel, and enables your IT team at the central office to virtually support your branch office staff with just a few clicks of the mouse.

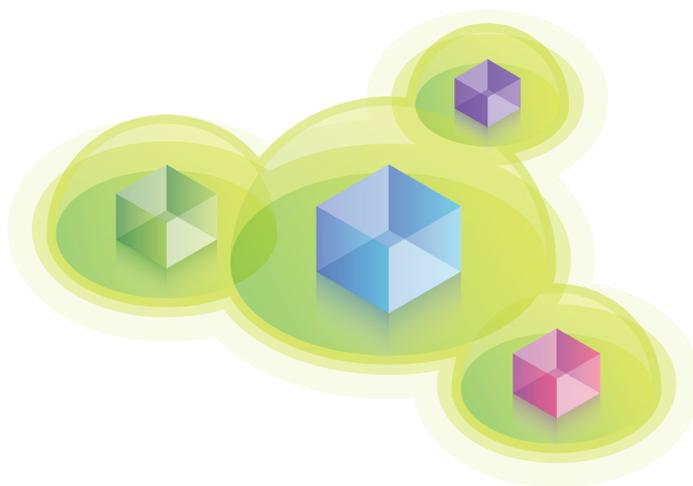
Simple policy management

With RED, you can create and maintain one global policy that protects and tracks all remote sites in your central security gateway. You can set different user rights for individual branches or employees—just as you can do at the headquarters. Therefore the branch office gets the same level of security as the central office.

Summary

Sophos RED is a better way to manage branch office security.

Learn how you can benefit from RED, the new standard for innovative, cost-effective branch office security management.



Sophos RED

Get a free trial at Sophos.com

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com