

Astaro OrangePaper

Reinventing Branch Office Security: Configuration-less UTM protection for small offices

Author: Udo Kerst
Astaro Sr.
Product Manager



Date: 15.07.2010

Content	Page
Executive Summary.....	2
Branch Office Security – what are the real problems?	2
Managing Branch Office Security	3
Implementing Security Policies.....	3
Security measures for very small offices	4
A new approach for Branch Office Security.....	5
Two-Minute Deployment.....	5
Centralized Management	6
Astaro Branch Office Security.....	7
Saving up to 80% of your TCO	8
Summary.....	10

Executive Summary

When it comes to IT security, almost all businesses using IP networks to transmit data will know that they have to protect themselves, and they will have systems in place to keep their data secure. However, this is often focused at the head office. For workers that are not located at the central office - whether this is a branch office environment or a remote worker at home - the question of security is a harder one to answer.

On the one hand even smallest offices that connect to the internet should get the same level of safeguards as large offices but on the other hand professional security devices are expensive, their management is time consuming and IT security knowledge at small offices is scarce.

This Orange Paper is explaining a new approach for providing complete, affordable and easy to manage security to even smallest branch offices.

Branch Office Security – what are the real problems?

The number of companies that have remote workers or branch offices is constantly growing. This expansion comes alongside greater use of the Internet for communication and collaboration. Typical examples of branch office IT deployments are retailers, travel agents, petrol stations or local sales offices. The IT requirements at each location can be fairly basic, and IT management skills at these branches often don't exist. However, the typical branch office environment needs often the same functionality as the head office when it comes to security - firewall, VPN, IPS, web and email security are all just as important to remote workers as those at headquarters.

Hence support and security of such branch office environments can be a significant challenge if not approached correctly.

The primary challenges are deploying the same level of security to all branch offices and implementing security policies in an efficient way.

Managing Branch Office Security

*Central management
is key*

The first area to consider is how to manage many branch networks efficiently. Because each branch office is small, it will typically not have any on-site IT staff available to support users if something goes wrong. The emphasis therefore has to be on how the central IT department can provide this support and security. However, the amount of time that can be spent on this activity could start to have a serious impact on productivity and costs if not carefully planned. For the central IT team, committing human resources to a new office installation or upgrade can be very expensive, especially when dealing with multiple offices at separate locations.

If you are starting a new branch office, being able to configure and manage security systems centrally, without having to put an engineer on the road for several days, provides a far better return on investment and much lower costs. Pre-configuring each system at the head office is one approach, but in most cases adjustments must be made on-site. This leads to a different configuration in each location, which makes it hard to keep track. Dedicated solutions for central management exist, but are expensive and often very complex.

Implementing Security Policies

*Maintaining separate
rules for every office can
become a time
consuming task*

Once you have the IT network protected, the next point is to look at the company's existing policies around how IT assets are used. From access to the Internet for personal use through to application installations and stopping unauthorised software, this set of rules for IT can be extrapolated into the branch office environment. Most of these guidelines should be the same - for example, not allowing peer-to-peer software to be installed without a valid business use case or not allowing surfing during business hours for private purposes.

Creating and maintaining these rules separately on every single security device can become a time consuming task requiring several hours of work as every device has to be updated each time the policy is changed.

Again dedicated systems for central management are available, but most often they are too expensive and too complex to use.

There is no ideal solution for securing small offices available today

Security measures for very small offices

Botnets, automated scripts and other malicious hacker tools are often randomly choosing their target of attack seeking to spread malicious code anywhere in the internet without consideration as to whom it is they are infecting- large corporations, small offices or even home users. Hence protecting small offices against internet based threats requires the same level of safeguards as for large offices.

Deploying security devices with comprehensive enterprise-class security functionality within every single office would be the ideal solution. But there is no easy way to achieve this when considering the costs and IT knowledge required by many of today's solutions:

- **Low-End Unified Threat Management (UTM) Appliances** are offering the required functionality in most cases. But, if you add up the amount of work and hidden costs of many solutions e.g. for roll-out, maintenance, subscriptions and management software they are too expensive for very small offices.
- **Consumer grade routers** are used by many companies due to budget constraints. These devices are cheap, but rolling out and managing these boxes one-at-a-time is a big headache – and most devices only provide very basic security functionality (e.g. firewall or VPN) and often lack important security safeguards like IPS, web and email filtering.
- **Managed VPN or MPLS services** are another alternative to securely connect remote offices to the central office and provide all security functionality through a centralized gateway device located at the head quarter. This approach has the benefit that it doesn't require any IT-experts at the remote office. However VPN or MPLS services are often quite expensive and not available at every location. Furthermore they lock you to a specific service provider.

The bottom line is that all solutions that exist today are either too expensive, too hard to manage or don't provide the required level of security.

What is needed is a new economic approach to branch office security that ensures that each branch office remains secure by only using the skills that already exist at the head office.

A new approach for Branch Office Security

RED reinvents Branch Office Security

A new way to solve these problems is to use a kind of “virtual Ethernet cable” for connecting your central and branch offices. Instead of running firewall, VPN, IPS, web and email security functions on an expensive branch office device all functions are provided via a centralized powerful security gateway which can sit in your head office or in the cloud (e.g. at a service provider). A small “Remote Ethernet Device” (RED) in the branch office only forwards all traffic via an encrypted tunnel to the central device where it is scanned and filtered, before it is sent to the internet. It acts just like a ultra long “virtual” Ethernet cable from your headquarter to your branch office. By using standard VPN technology it’s also independent from your service provider. It can be used worldwide – wherever an internet connection is available.

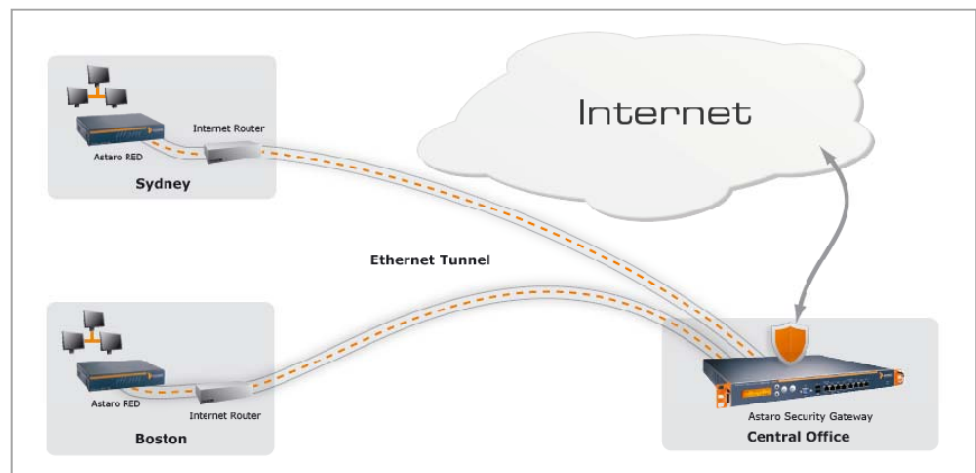


Fig. 1: Complete UTM Security through Virtual Ethernet Cable

Two-Minute Deployment

Plug & Play Security Deployment

The beauty of this approach is that Remote Ethernet Devices don’t require any local configuration; they don’t even have any button or management GUI. Their complete configuration is done on the central gateway.

The device can just be shipped unconfigured to the branch offices. Someone - no technical skills required – tells IT the serial number of the box, plugs it into the internet router, connects it to the computer and plugs it into the wall. When the branch office device comes on-line, it automatically retrieves its set-up information from the central provisioning service, configures itself and establishes an encrypted tunnel to the head office, without requiring IT staff on site.

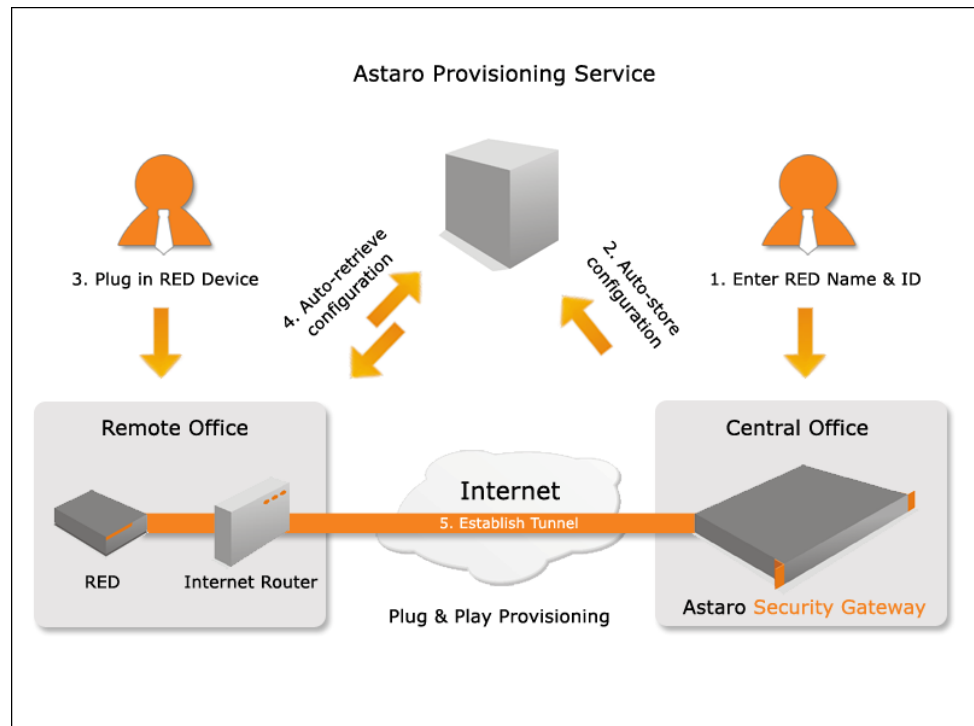


Fig. 2: Rapid Deployment of Remote Ethernet Devices

Using these fully automated deployment process even mass-roll outs of up to 100 appliances per day are feasible.

Centralized Management

Simple Policy Management

By using Remote Ethernet Devices managing your remote site's network setup and security policies becomes very simple. You can easily define your global DHCP and DNS Server configuration on the central Security Gateway and roll it out to all connected sites.

Similarly, creating and managing separate security policies for each individual site is no longer required. You just need to create and maintain one global security policy for protecting all remote sites in your central security gateway.

Keeping control and global visibility of your remote networks has also never been easier. As branch offices can now be managed as if they were connected through an ultra long Ethernet cable they seamlessly integrate into the built-in reporting and logging solutions of the central security gateway. There's no need for separate management and reporting tools.

Astaro Branch Office Security

*The new para-
digm*

Astaro is the first and only vendor offering Remote Ethernet Devices today. Astaro RED 10 appliances, combined with Astaro's award winning Astaro Security Gateway products at the head office, provide complete centrally managed UTM security (see paragraph below) at an affordable price without requiring any technical skills at the branch.

The setup of a new RED 10 appliance at a remote office can be done in minutes. There are no recurring maintenance tasks or subscription costs for the branch, nor do you need any additional management or reporting tools at the central office. All is included within your centralized Astaro Security Gateway, which acts as a central controller for all connected RED devices.

Unified Threat Management – comprehensive security for SMBs

Unified Threat Management (UTM) offerings have exploded in the past years. The concept of integrating multiple security features like firewall, VPN gateway, Intrusion Prevention, E-Mail and Web-Security on a single, All-in-one platform with one graphical user interface is gaining more support than ever before. It's especially attractive to small and medium sized companies who don't have the budget and IT expertise for deploying multiple security products for different purposes.

Inherently, managing multiple products presents a multitude of downsides when compared to an effective UTM solution. Administrators must master multiple management environments, all with different terminologies and feel. They must maintain many firmware and pattern updates, and correctly configure the solutions to interoperate with each other in the proper order so as to ensure the correct functionality is achieved by the entire security deployment. Further, multiple network security solutions present a large increase in troubleshooting complexity since there are many points where misconfiguration and error can occur, raising the amount of places that need to be examined to find the problem. Financially, the deployment of multiple point products becomes even less attractive when the individual subscription services for support, maintenance, and updates are tallied, which are all paid independently for each product. The attractiveness of choosing a UTM appliance is strengthened by having to master just one management GUI, pay subscription fees to one company, and troubleshoot any issues at a single point. Further, the applications on a UTM device interoperate and complement each other so as to best take advantage of the architectural approach of running on the same platform.

Due to the increasing demand many vendors are trying to participate within the UTM market with a deluge of products that in many cases offer similar ranges of features, performance, and capabilities.

However, especially when it comes to integrated management, ease of use and depth of security features there are huge differences between the various offerings. For instance many vendors are offering important but resource intensive features only on larger appliances but not on smaller devices which are primarily used within remote offices.

Therefore making quick, uneducated decisions can lead to unexpected surprises when the products are deployed or when additional features are required later on.

For more information please see Astaro Orange Paper "The UTM Explosion – Sifting through the rubble"

http://www.astaro.com/sites/default/files/Resources/whitepapers/AstaroOrangePaper_UTM_Explosion_en.pdf

Saving up to 80% of your TCO

*Make your
math*

The cost of maintaining a branch office network - particularly one with tens or even hundreds of sites - is an important factor that has to be considered over time. Apart from the initial investment there are many additional components that need to be considered when comparing the total cost for several years.

For instance when comparing the Astaro Branch Office Solution with a solution using standard UTM products in every office the following costs are important:

Central Office Security Appliance

Here you have to consider the costs for the initial Security Hardware & Software (or Appliance) plus recurring costs for Hardware Maintenance and Subscriptions for all security functions in use (e.g. antivirus, antispam, web filter, ISP etc...).

Remote Office Appliances

Initial Hardware costs for small UTM appliances can seem relatively low; however when adding recurring costs for hardware maintenance and subscriptions for every office this often sums up to a high cost component.

When using Astaro RED you don't have to consider any recurring costs for renewing security subscriptions at the remote office. Hardware maintenance is also included with the initial hardware investment. There's only an optional warranty extension available that can be purchased on a 2-yearly basis.

Central Management and Reporting Tools

In order to centrally manage your remote office UTM appliances you typically need additional management tools at the head quarter. Furthermore for getting up-to-date information about the security landscape of your remote offices (detected attacks/viruses, spam, who has surfed on which website etc...) you also need a central reporting tool. The costs of these tools are quiet significant and can easily exceed the costs of the central security solution itself.

With the Astaro Branch Office Solution there is no requirement for investing in those tools as the central Astaro Security Gateway provides complete centralized management, reporting and troubleshooting functions for the central office as well as for all connected remote offices without any additional costs.

Roll-Out & Administration Costs

Don't underestimate recurring maintenance costs

These costs can vary significantly depending on the organizational structure and the availability of IT experts. However the initial setup of a standard UTM solution can easily last 2 days for the central office and 3 hours per remote office. When adding the time needed for regular software updates for every office (e.g. 2 times 2 hours per quarter) plus the time and costs for bringing an IT expert to the remote office, these costs can sum up to the biggest cost factor at all.

With the Astaro Branch Office Solution the initial setup takes no longer than an hour for the central site and no longer than 15 minutes per remote site. As the complete management of all RED devices is done on the central gateway there are no costs for remote site maintenance nor do you need to bring any IT expert to the remote site.

Considering the total costs of hardware, management tools, subscriptions and ongoing maintenance you can save up to 80% by using the Remote Ethernet Device approach compared with deploying standard UTM gateways at the central office and every remote location.

The following table provides an example calculation for both solutions for 30 remote offices and a 5-year period.

TCO Comparison (30 remote offices - 5 Years)		Strd. UTM product	Astaro
Central Office Appliance (1x)			ASG 220
Appliance		\$ 2.995	\$ 1.275
Hardware Maintenance 24*7 (5 years)		\$ 3.745	\$ 1.180
Security Subscriptions (5 years)		\$ 5.015	\$ 10.155
Remote office Appliances (30x)			Astaro RED
Appliances		\$ 8.850	\$ 8.850
Hardware Maintenance 24*7 (5 years)		\$ 11.100	\$ 4.500
Security Subscriptions (5 years)		\$ 8.400	\$ 0
Central Management Tools			included
Appliance		\$ 6.746	\$ 0
Software (5 years)		\$ 11.245	\$ 0
Central Reporting Tools			Included
Appliance		\$ 4.496	\$ 0
Software (5 years)		\$ 7.495	\$ 0
Administration costs			
initial central site setup	\$ 545 (2 days)		\$ 34 (1 hour)
initial remote site setup	\$ 3.068 (3h/site)		\$ 256 (15min/site)
ongoing remote site maintenance	\$ 16.364		\$ 0
Travel costs	\$ 17.591		\$ 0
Total		\$ 107.655	\$ 26.250
Savings			76%

Fig.3 Calculating TCO for Branch Office Security

Summary

Businesses with many small branch offices like travel agencies, retail stores, or petrol stations are consistently facing the challenge to connect them back to the headquarter and to keep their Internet access secure.

All of today's solutions have a specific drawback. They are either too expensive, too hard to manage or don't provide a sufficient level of security.

Remote Ethernet Devices are a completely new approach combining all the benefits of existing solutions by avoiding their drawbacks at the same time. By acting as a virtual Ethernet Cable from your remote office to the central site they provide complete, centrally managed UTM security without requiring any technical skills at the branch. All configuration and filtering is done via a centralized Security Gateway located at your central office.

This approach provides an easy and affordable way for deploying branch office security even to smallest offices.

--

For more information please visit our website at <http://www.astaro.com/products/astaro-red>

Contact Astaro

Europe, Middle East, Africa

Astaro GmbH & Co. KG
An der RaumFabrik 33a
76227 Karlsruhe
Germany

T: +49 721 255 16 0
emea@astaro.com

The Americas

Astaro Corporation
260 Fordham Rd
Wilmington, MA 01887
USA

T: +1 781 345 5000
americas@astaro.com

Asia

Astaro Asia
8 Eu Tong Sen Street
#12-99, The Central
Singapore 059818

T: +65 6227 2700
apac@astaro.com

Pacific Japan

Astaro K.K.
Shinjuku Nomura Building 32F
1-26-3 Nishi-Shinjuku
Shinjuku-ku, Tokyo
Japan 163-0532

T: +81 3 4360 8350
apac@astaro.com

This document may not be copied or distributed by any means, electronically or mechanically, in whole or in part, for any reason, without the express written permission of Astaro AG.

Copyright © 2010 by Astaro GmbH & Co. KG. All rights reserved. Astaro Security Gateway, Astaro Command Center and WebAdmin are trademarks of Astaro AG. All further trademarks are the property of their respective owners. No guarantee is given for the correctness of the information contained in this document.