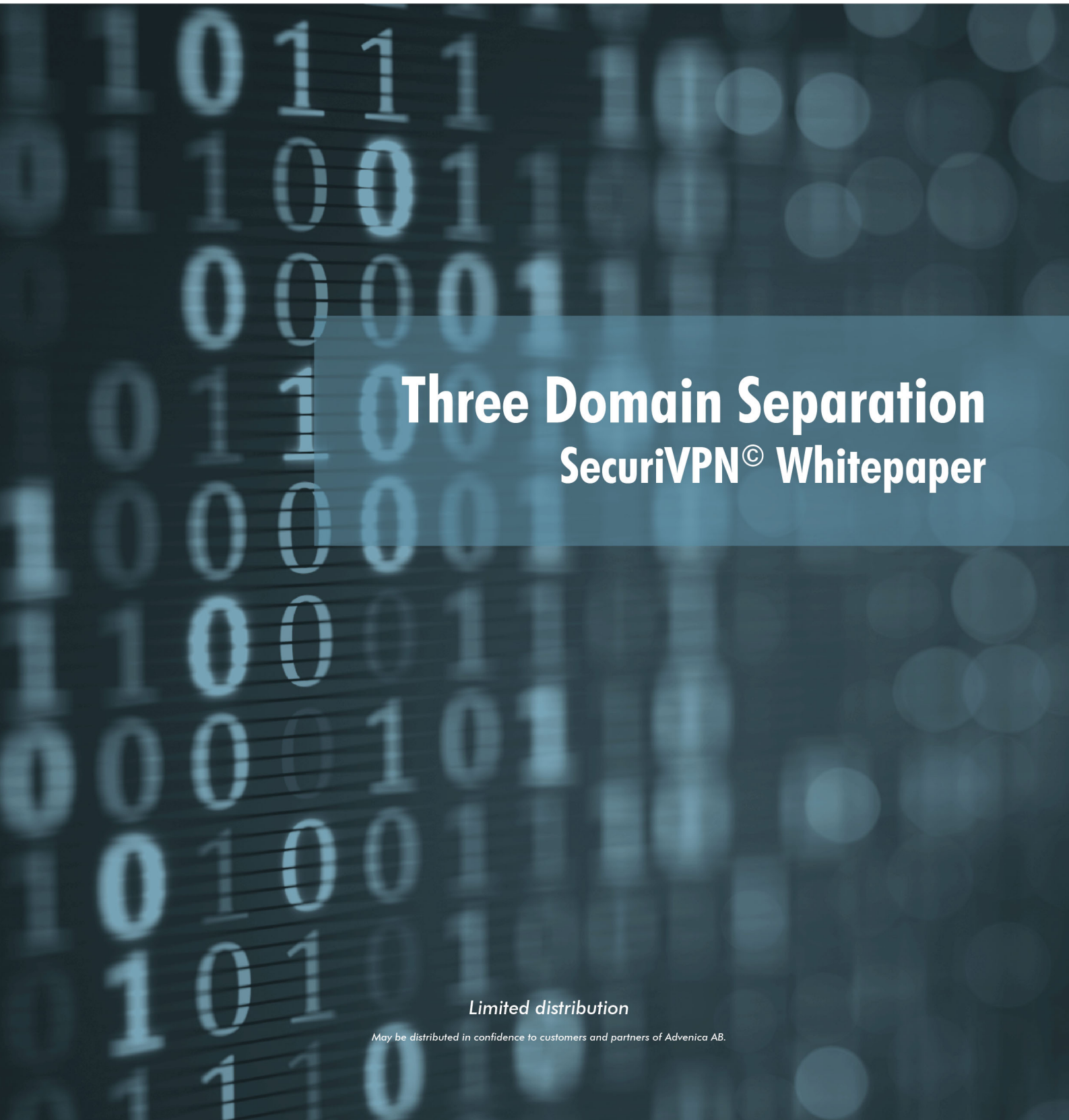

advenica

Three Domain Separation

SecuriVPN© Whitepaper

Limited distribution

May be distributed in confidence to customers and partners of Advenica AB.

Document version: 16153v1.2 SecuriVPN - Three Domain Separation

TABLE OF CONTENTS

1. VPN - a brief overview 5
2. VPN management methods 6
2.1 Local access to the VPN device 6
2.2 Accessing management interface via local network 6
2.3 Accessing management interface via remote management 7
2.4 Out-of-band management 8
3. A paradigm shift in VPN management 10
3.1 Central Administration with Three Domain Separation 11

1. VPN – A BRIEF OVERVIEW

Virtual Private Network (VPN) extends a private network service across a public network such as the Internet. The VPN devices protect information and ensures privacy through use of cryptographic functions combined with tunnelling protocols.

From a system point of view, a VPN device acts as a gateway between two different types of networks, also called domains:

- **Protected network, RED domain** - All information and network traffic within the RED domain is considered protected and therefore in plaintext.
- **Transport network, BLACK domain** - All information, sent between VPN devices, on the BLACK domain is protected with cryptology and tunneling protocols.The transport network is usually a public network such as the Internet.

The RED and BLACK domains cannot share any information which is the very definition of two domain separation.

Figure 1 depicts the information flow in a simple VPN system. Information bound from one RED domain location to another, is routed through the VPN device. The device encrypts the information and ensures that each datagram within an information stream is provided with necessary addressing information to traverse through the BLACK domain to the designated VPN device. The receiving VPN device decrypts each datagram before routing them to its corresponding RED domain, bound for its final destination.

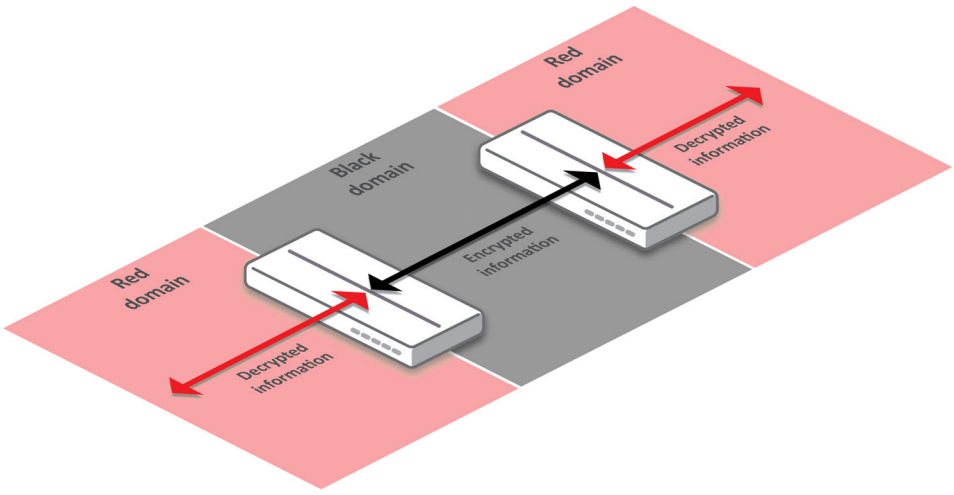

Figure 1 - Basic VPN, information flow.

2. VPN MANAGEMENT METHODS

Traditionally, there have been four more or less accepted methods for managing a VPN system, using two domain separation:

1. Local access to the VPN device
2. Accessing management interface via local network
3. Accessing management interface via remote management
4. Out-of-band management

2.1 LOCAL ACCESS TO THE VPN DEVICE

Direct **local access** from within the RED domain to the VPN device has historically been the most common way to manage the devices. Usually the command-line interface (CLI) was accessed through a serial interface or dedicated console port. This method works well when only a few VPN devices have to be managed, e.g. when a link is protected by two VPN devices on either end of the communications link. Also, the device configuration complexity is rather low, e.g. pre-shared keys are commonly used.

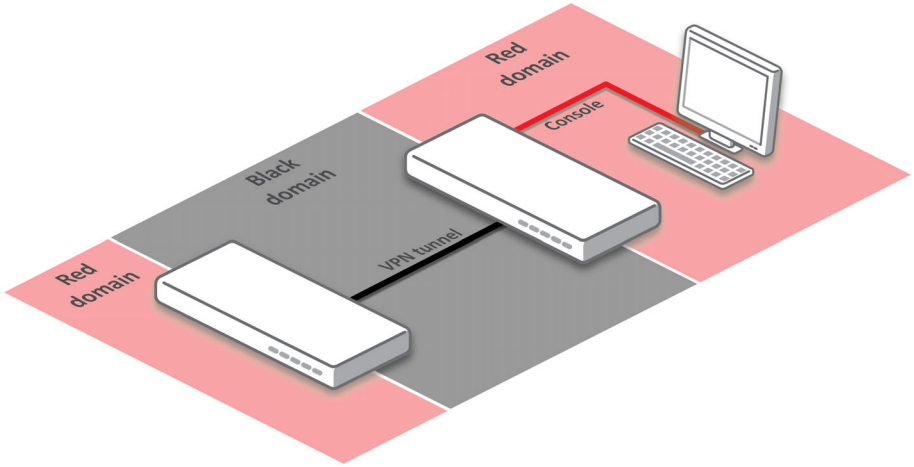

Figure 2 - Local access.

Drawbacks

- Local access management requires physical access to each VPN device.
- Sensitive user information may potentially be accessed by the administrator.

2.2 ACCESSING MANAGEMENT INTERFACE VIA LOCAL NETWORK

A common way of managing a VPN device today is by accessing the management interface through a **local network**, i.e. from the RED domain. Many devices are capable of utilizing different transport protocols for the monitoring and management traffic, such as HTTP and SSH. The insecure Telnet protocol is still supported by some VPN devices, although its use is not recommended.

Drawbacks

- Local network management requires physical access to the RED domain of each VPN device.
- Sensitive user information may potentially be accessed by the administrator.

Alternatively, HTTP and SSH can be configured such that management of VPN devices becomes possible from the BLACK domain, e.g. through the Internet. However, the management traffic does not receive the same level of protection compared to when the traffic is cryptographically protected in a VPN tunnel.

Drawback

- Sensitive user information may potentially be accessed by the administrator.

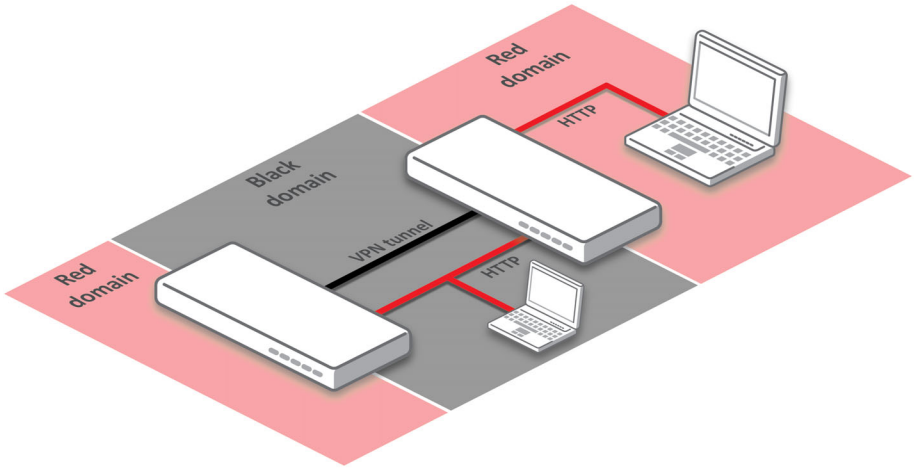

Figure 3 - Network access.

2.3 ACCESSING MANAGEMENT INTERFACE VIA REMOTE MANAGEMENT

A few VPN systems provide **remote management** possibilities. In the traditional two domain VPN solution, the VPN administrator is able to monitor and perform management tasks from a central point. The management interface of the VPN devices are accessed from the dedicated central management point, a RED domain, through a cryptographically protected VPN tunnel via a transport network, a BLACK domain, see *Figure 4*.

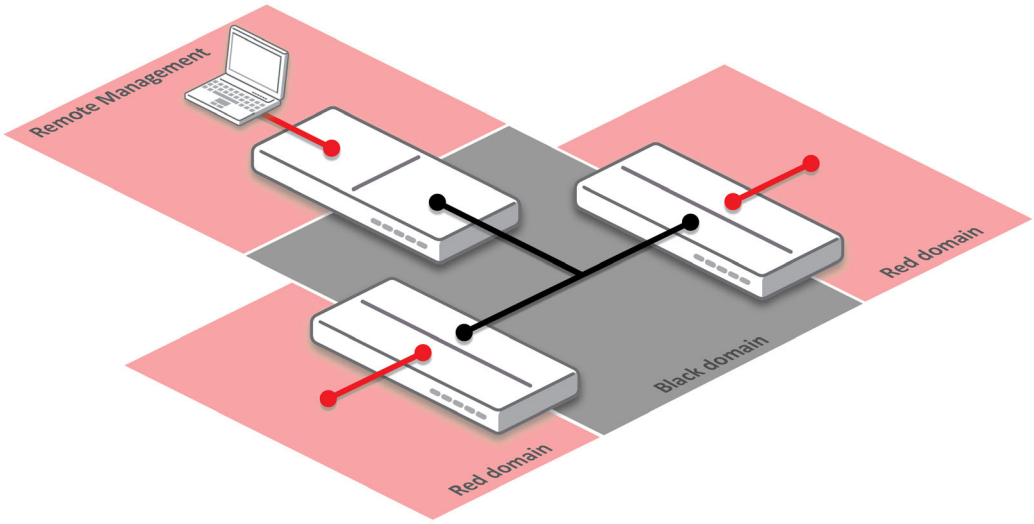

Figure 4 - Remote management with two domain separation.

The advantages of remote management is of course the possibility to simplify and rationalise the monitoring and management of large VPN deployments. The downside is the threat of administrative personnel's ability to access sensitive information on the RED domain from a remote management site potentially causing, intentional or unintentional, unauthorised disclosure of sensitive information, effectively creating "ghost users".

Drawback

- Sensitive user information may potentially be accessed by the administrator.

2.4 OUT-OF-BAND MANAGEMENT

Out-of-band management utilises a dedicated communication interface for VPN device management. The interface is connected to a transport network, often in parallel with the BLACK domain. Basically, this implies that there is a service network dedicated for VPN monitoring and management.

Out-of-band VPN management has had limited success mostly due to the cost involved with operating two networks. Furthermore, it does not address the threat of a potentially malicious VPN administrator accessing and disclosing sensitive information on the RED domain.

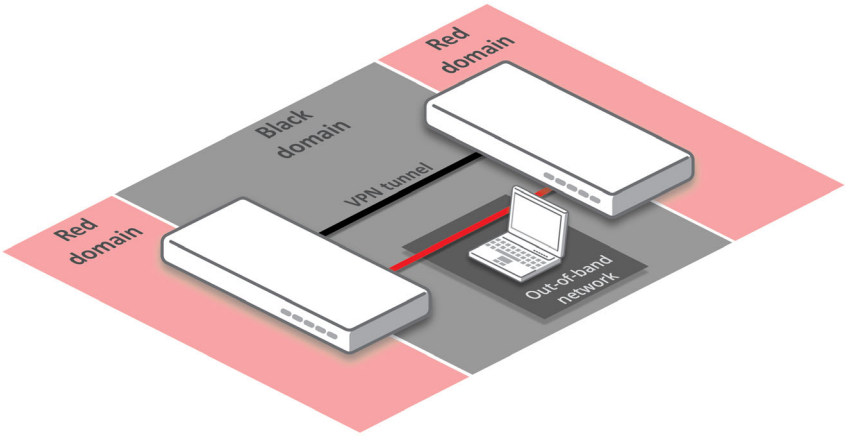

Figure 5 - Out-of-band management.

Drawbacks

- Cost of operating a service network.
- Sensitive user information may potentially be accessed by the administrator.

3. A PARADIGM SHIFT IN VPN MANAGEMENT

The cost of managing VPN deployments quickly becomes very expensive without central management possibilities. As already highlighted in previous chapters, the benefit of central management is the possibility to rationalize the deployment, monitoring and management of VPN installations. Central management will greatly reduce the total cost of ownership as well as return on investment. However, traditional central management has severe drawbacks when it comes to information privacy and information leakage. The root of the problem lies in the two domain separation utilised by traditional central management where administrative personnel have the ability to access sensitive information on the protected network (RED domain) from the management site.

The solution is to introduce a new domain dedicated for management, the ADMIN domain. The three domains and their purposes are defined as:

1. **RED domain** – for protected user information
2. **BLACK domain** – for transportation of user information between RED domains
3. **ADMIN domain** – for monitoring and management information

A logical consequence of introducing a third domain is that a VPN device now has to be able to keep three domains separated, instead of two.

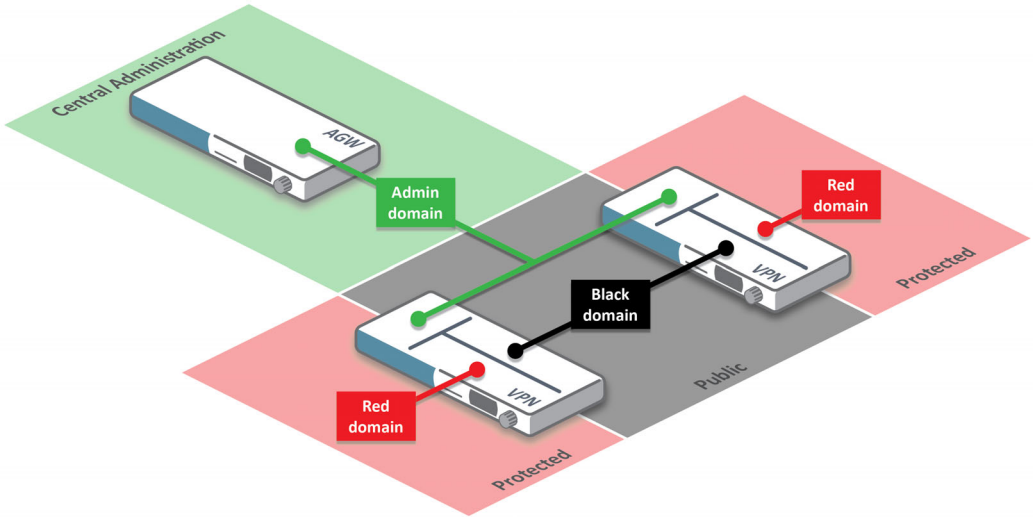

Figure 6 - Three Domain Separation.

Advenicas unique **Three Domain Separation** technology (see *Figure 6*) is the very mechanism that enables domain separation. The technology ensures that only members within the same domain can share information with each other, i.e. the RED domain is now no longer reachable for members in the ADMIN domain. Additionally, the Three Domain Separation technology introduces an Administration Gateway device and a cryptographically protected tunnel dedicated for management traffic, called the administration tunnel. The purpose of the Administration Gateway device it to act as a gateway at a central management site, setting up administration tunnels to all VPN devices managed from the management site. Management traffic coming from the Administration Gateway via an administration tunnel to the VPN device is diverted to a dedicated area of the device (see *Figure 7*). In this

area only monitoring and management information is available. Thus, sensitive information in the RED domain cannot be intercepted, changed or mirrored.

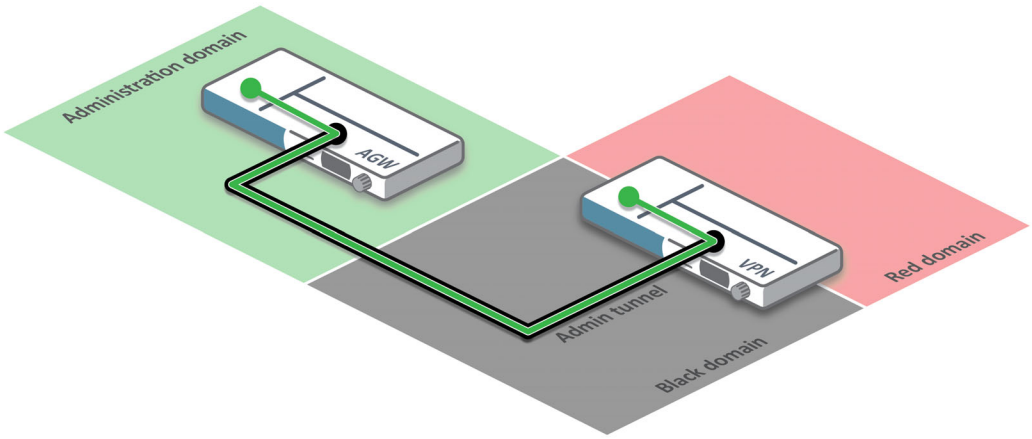

Figure 7 - Administration tunnel.

3.1 CENTRAL ADMINISTRATION WITH THREE DOMAIN SEPARATION

The Central Administration functionality of both Advenicas SecuriVPN and SecuriConnect systems integrates the Third Domain Separation technology. The Central Administration is used to configure, control and monitor the VPN devices from a central site. The following components are part of the Central Administration:

- **Configuration Application -** Creates and manages the entire configuration of the VPN system.
- **Administration Gateway device** - Protects the administration system and management traffic to the VPN devices.
- **Remote Administration Server** - Keeps the VPN devices up-to-date with the latest configuration files and firmware and manages remote control of VPN devices and tunnels.
- **Log Server** - Collects and stores log events sent from the VPN devices.
- **Remote Supervision Application** - Monitors VPN devices.
- **NTP Server** - Provides time information to VPN devices.
- **Key Server device** - Generates and distributes session keys.
- **KSS Database Server** - Provides information about which VPN devices that may communicate.

Each administration tunnel in an Administration Gateway device uses unique session keys to cryptographically protect the management traffic. Session keys are generated and distributed automatically by a Key Server device. They are also continuously and frequently renewed. Moreover, the session keys themselves are protected by a master key, effectively using a hierarchy of keys to achieve layered security.

Key Server devices also generate unique session keys for encryption of end-user traffic sent over a tunnel between two VPN devices. Consequently, different keys are used for protecting management traffic and sensitive end-user traffic to further segregate management traffic from other type of information.

By activating the Central Administration option in a SecuriVPN or SecuriConnect system, Three Domain Separation is automatically enabled in the VPN devices. Deployment of VPN devices with Central Administration requires no IT expertise at the customer site. Once connected to the IP network, the VPN device will automatically contact the Central Administration site and establish the necessary secure connections to other VPN devices. Through the Central Administration site it is of course possible to distribute new VPN device configurations, new firmware etc.

The Three Domain Separation technology represents a true paradigm shift in VPN management. Large VPN deployments can be monitored and managed from a central location, e.g. a Secure Operation Central (SOC), without contaminating the management site with sensitive information stored inside the RED domain. Administrative personnel can only access information that is required for VPN device management.

Benefits of Central Administration with Three Domain Separation technology

- ✓ Superior VPN management technology through Three Domain Separation
- ✓ Utilises key hierarchy to achieve layered security
- ✓ Administration tunnels to further segregate management traffic and sensitive end-user traffic
- ✓ Rationalises VPN monitoring and management
- ✓ Allows organisations to leverage their existing network technology and protect investments already made
- ✓ Available as a turnkey solution that includes all necessary components for successful VPN administration without compromising the privacy of sensitive end-user data
- ✓ Easy to learn, easy to use. High end security in a user friendly solution
- ✓ Greatly reduces Total Cost of Ownership
- ✓ Three Domain Separation technology makes it possible to outsource administrative tasks without compromising the security aspects of the system - a true MSS enabler

advenica

Roskildevägen 1
SE-211 47 Malmö, SWEDEN

Phone +46 40 60 80 401

E-mail helpdesk@advenica.com
URL www.advenica.com