

SECURE REMOTE ACCESS THAT PROVIDES DATA ASSURANCE AND BUSINESS CONTINUITY

USB-Based Technology Enables Secure Mobile Working from Unmanaged Locations

Challenge

For business continuity, or the occasional home worker, employees may be required to access an internal network or other business resources from unmanaged machines, which are therefore not trustworthy or properly secured.

Solution

Trusted Client provides a safe, configurable operating system and workspace for remote endpoint PCs via a fully encrypted USB thumb drive. Juniper Networks SA Series SSL VPN Appliances are used to create a secure and verified link between the remote endpoint and the user's corporate network resources.

Benefits

This joint solution allows thin-client applications, e-mail and Internet access, and standalone applications to all be protected when remote users need to access network resources from third-party machines, which may not provide the required levels of security.

If your organization ever needs people to work from home, from client or partner sites, or from other locations, BeCrypt Trusted Client™ and Juniper Networks® SA Series SSL VPN Appliances could provide you with an extremely cost-effective solution. In the event of a major flu pandemic, public transport failure, or loss of one or more of your offices, this solution will help ensure that your staff will be able to continue working securely from any location while maintaining the highest levels of information assurance.

BeCrypt Trusted Client devices are inexpensive to deploy, and should one be lost or stolen, there is no risk to the data contained within it.

The Challenge

There are many security risks that need to be addressed by an organization to ensure that its networks and private information remains safe. An employee that remotely connects into an office network poses a serious risk, as a tunnel into the office network office is created, bypassing the firewall and other external security measures. Mobile users are typically issued laptops, providing an environment that can be managed by an organization, allowing many of the associated risks to be mitigated, particularly when a secure access SSL VPN solution is deployed. However, for business continuity, or the occasional home worker, employees may be required to access an internal network or other business resources from unmanaged machines, which are therefore not trustworthy or properly secured.

An alternative to the use of managed laptops exists, that can provide an equivalent degree of security. An encrypted bootable operating system that can be run from a USB device or CD-ROM across an SSL VPN connection, may be used in place of laptops where cost and scalability are issues, providing complete isolation from threats normally associated with the use of un-managed machines.

The Juniper Networks SA Series and BeCrypt Trusted Client Solution

The BeCrypt Trusted Client USB-based operating system has been optimized to use the Juniper Networks market-leading SA Series SSL VPN Appliances. The solution is particularly suited to government and federal IT infrastructure, as it can re-create specific levels of security accreditation on third-party devices instantly, with an encrypted workspace. This alleviates the situation where an employee that may work with several different levels of classified data and therefore needs several different logins, or needs to work from different computers. It is also relevant for any corporate remote-access strategy that encompasses business continuity and can be used to completely replace corporate laptops.

Trusted Client provides a safe, configurable operating system and workspace for remote endpoint PCs via a fully encrypted USB thumb drive. Juniper Networks SA Series SSL VPN Appliances are used to create a secure and verified link between the remote endpoint and the user's corporate network resources. Thin-client applications, e-mail and Internet access, and standalone applications can all be protected when remote users need to access network resources from third-party machines, which may not provide the required levels of security.

Features and Benefits

A Revolutionary Solution

Trusted Client is a bootable trusted environment that can be run on any unmanaged, untrusted PC platform. When inserted into an untrusted computer, it launches a self-contained working environment that is entirely separate from its temporary host's operating system. This Trusted Client environment, consisting of a lightweight operating system, a Web browser, and Juniper Networks SA Series, plus optional components (such as thin-client applications or an e-mail client), is written on a USB thumb drive. The USB device is protected by FIPS-approved Advanced Encryption Standard (AES) encryption and by strong user authentication and may safely be carried by any authorized users.

Encryption and Authentication

All data on the Trusted Client device, including the operating system, is protected by a combination of encryption and strong authentication. Only if the user enters the correct username and password will Trusted Client launch the trusted environment. If an unauthorized user tries to boot from the device, Trusted Client will require a username and password; if the device is inserted into a live machine, because the device is encrypted Windows will view the device as unformatted and prompt for the option to format the drive. In both cases, the content on the device is fully protected: It cannot be read without authorization, and it will be deleted if the device is reformatted.

Configurable Security

The Trusted Client security features are configured to follow an organization's security policy. The configured setup file can then initialize as many USB devices as required.

Each Trusted Client device can have a unique encryption key, username, and password. In addition, restrictions can be set on the use of high-risk features to prevent accidental or deliberate misuse by an authorized user. These features include:

- Allowed IP addresses. Trusted Client can be configured to connect only to allowed machines (IP addresses) and only through specified ports.
- Peripheral device access. Trusted Client can be configured to remove all possible data export paths from the device.

- System persistence. The Trusted Client environment is configured to prevent any unauthorized modifications to system files.
- Password policy. The password format can be restricted to enforce strong authentication; alternatively, the user can be forced to use the embedded strong-password generator.

Secure Access

Trusted Client has been designed to work with the Juniper Networks endpoint inspection product, Host Checker, to help ensure that the virtual system conforms to the administrator's specification and that the user can be uniquely identified. Trusted Client is further controlled through the automatic provision of stateful firewall rules that limit the connection to approved networks only, securing the network layer as well as the session.

When Trusted Client is used with the Juniper Networks SA Series appliance, security layers are introduced at the user's endpoint. Trusted Client provides an isolation layer between the real machine and the virtual machine used for secure network access.

Device Recovery

If the user forgets the device password, Challenge-Response provides a mechanism by which access can be regained with the aid of your help desk. Challenge-Response uses recovery data generated during installation. At no point in the Challenge-Response procedure is the user's original password or encryption key exposed.

Solution Components

BeCrypt Trusted Client protects a trusted environment from unauthorized devices that may connect to the SA Series. Trusted Client can be configured to control the IP addresses to which the user in the work session can connect. Therefore, it sits within the endpoint security layer and works in conjunction with Juniper Networks HostChecker, CacheCleaner, and Advanced Endpoint Detection.

Typically, BeCrypt Trusted Client is deployed in environments where strong data assurance and, often, protection for officially classified, restricted, sensitive or sensitive but unclassified (SBU) data is required. Although BeCrypt Trusted Client works with all Juniper Networks SA Series SSL VPN Appliances, it is usually used with SA4500 and SA6500 models as these are FIPS 140-2 Level 3 compliant, can carry 1000 or 3500 concurrent sessions respectively, and have SSL acceleration, attributes that are all likely to be required for a large-scale or complex deployment.

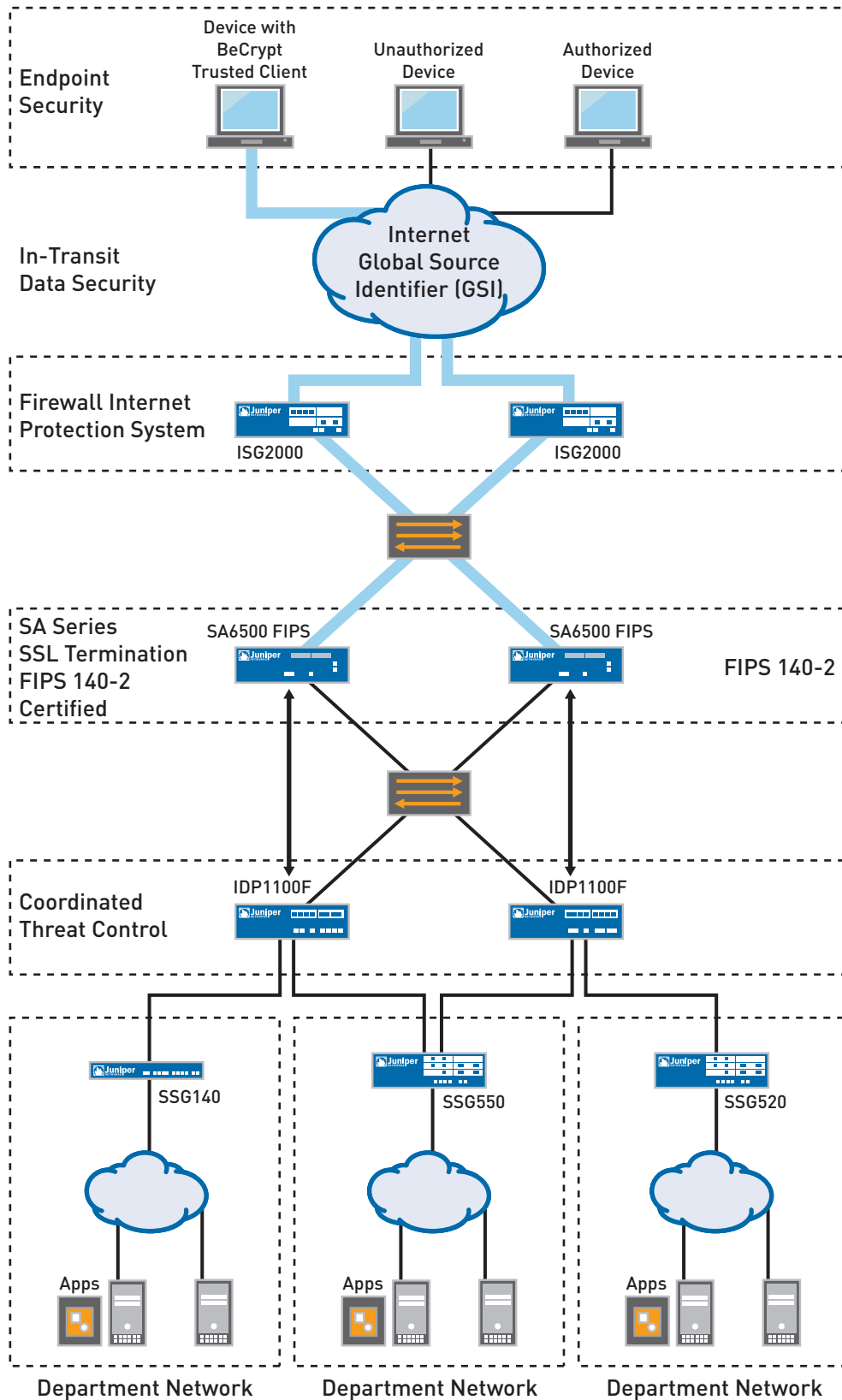


Figure 1: BeCrypt Trusted Client and Juniper Networks SA Series SSL VPN Deployment

Summary: BeCrypt Trusted Client Teamed with Juniper Networks SA Series SSL VPN Appliances Enable Cost-Effective Business Continuity and Information Assurance

The mobility of employees within a business is often seen as a fundamental part of the business infrastructure. Mobility allows employees to work from home, to work from client sites, or to work from anywhere else that is practical. However, this mobility can pose a major threat to security, compromising information assurance and business continuity. BeCrypt Trusted Client together with Juniper Networks SA Series SSL VPN Appliances provide an innovative, cost-effective solution to these challenges.

Next Steps

For more information about how your organization can benefit from BeCrypt Trusted Client and Juniper Networks SA Series, please contact your Juniper Networks representative.

About BeCrypt

BeCrypt Limited was formed in 2001 to meet the growing demand for high-level computer encryption products in the international government and corporate marketplace. BeCrypt products protect customers in key UK government areas including: central and local government, the defense sector, law enforcement and transportation. The company now also provides a range of flexible security products tailored to meet the requirements of the commercial sector. BeCrypt has customers in financial services, pharmaceutical, insurance and banking sectors.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airsides Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
Fax: 35.31.8903.601

Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

