

## Cisco network security services localization for Russian market

### Problem statement

Russian domestic legislation puts special regulations on the development and implementation of the information security solutions. One of these requirements is certification of the information security solutions. The necessary condition of the security certification is an implementation of Russian national cryptographic algorithms.

Currently leading western vendors started process of the security localization for the Russian market. Specifically, Microsoft has two implementations of cryptographic service provider library from two Russian vendors. IBM considers project of local cryptography implementation in NetVista and ThinkPad ESS/CSS solution. Check Point negotiates cryptography localization for the VPN-1 platform with Russian vendor.

To win competition in Russia Cisco Systems needs local security solution for the VPN implementations.

“CSP VPN” project delivers proposition of Cisco-complimentary VPN solution for Russian market.

### Value proposition

Implementation of the local cryptographic algorithms as an embedded software libraries inside original Cisco products is technically possible, still it seems rather difficult for several reasons:

Cisco’s software contains a lot of intellectual property; that’s why it is hardly possible to open Cisco’s sources to the local Russian partner, who would implement local cryptography

Cisco owns diversified VPN product line (PIX, IOS, VPN 3000 concentrators) that’s why implementation of Russian local cryptography is a labor costly task

The task of the local cryptography implementation is not limited by cryptography libraries only; this is also the issue of compatibility with local PKIs, hardware tokens, etc. This compatibility hardly can be achieved outside Russia

Cisco regularly updates product software. According to the local regulations, each update needs re-certification. This process is also difficult to manage from foreign country

Even if Cisco will implement Russian cryptographic libraries (say, on the basis of the open sources, available in Internet), this implementation will never be certified because Russian legislation does not trust any vendor who develops cryptographic technologies without Russian government license.

Taking into consideration all these constraints, Russian company “S-Terra group” developed the concept of the Cisco network security implementation as follows.

The concept is based on “two-echelon security” approach.

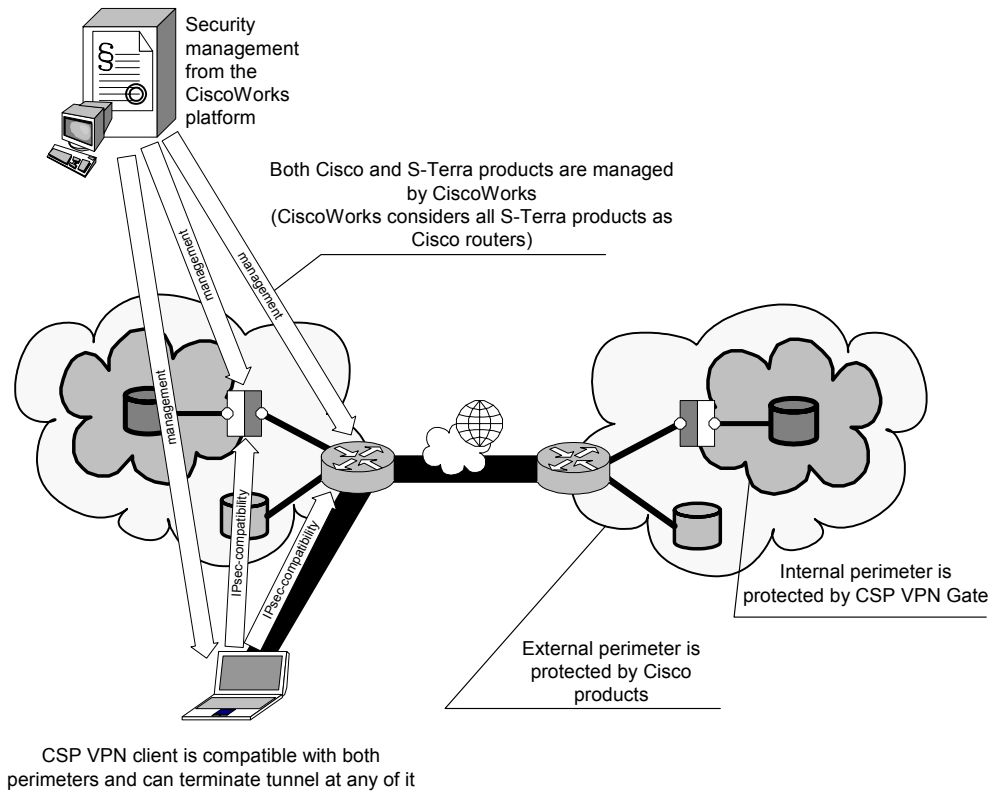
First echelon, external perimeter, is to be protected by original Cisco products. That is legitimate approach, because highly confidential information is never placed on the edge of the external perimeter. The security services that we propose to implement on the external perimeter are: access control of the PIX firewalls and IOS routers and, by the customer decision, IPsec tunnel with AH protocol (it seems that AH without ESP would not be considered as big fault in this case).

Second echelon, internal perimeter, we propose to protect by S-Terra’s devices, CSP VPN Gates, which are 100% compatible with Cisco’s protocol stack and security management/monitoring infrastructure.

Note, we discarded stateful inspection firewall from the CSP VPN Gate to free space for the PIX firewall inside the internal perimeter.

S-Terra's solution consists of 3 products: CSP VPN Gate, CSP VPN Server and CSP VPN Client.

All solution must work inside the original Cisco infrastructure as it shown on the picture below.



## Marketing strategy

CSP VPN solution is to be positioned as Cisco complimentary and should not be sold separately from Cisco solution.

S-Terra group does not plan to implement solution directly, but only by indirect sales schema using Cisco partner channels in Russia. The only exception is pilot implementation of the CSP VPN solution in big Russian bank (Vneshtorgbank).

Pricing model will be aligned to Cisco's product line and partner policy.

## Cisco benefits

Proposition of the CSP VPN solution will allow Cisco to announce at Russian market that Cisco has local solution in Russia. This will open for Cisco possibilities to sell solution for the customers who require certified security and who can be lost without this feature.

Sales of CSP VPN solution would cause growth of Cisco infrastructure sales (management, monitoring, etc.).

Local cryptography proposition will cause better competitive positioning according to another big network security vendor – Check Point. Even if Check Point will localize it's solution in Russia, the competitive differentiator of Cisco and CSP VPN solution will be "two echelon" architecture, while Check Point has single homogeneous solution. The matter of this differentiator is that many security experts do not appreciate any number of echelons of homogeneous perimeter because all of them would be broken by single security exploit.

CSP VPN solution provides possibility to take a great deal of the market from the Russian domestic network security vendors whose solutions are much less robust and flexible than Cisco's network security products. It will open the additional opportunity to sell Cisco.

S-Terra would like to achieve as much as possible close integration with Cisco's solution and to invent extra revenue generation methods for Cisco. Some of these approaches are considered in the separate document ("CSP VPN roadmap").

### **Project status**

The first release of the CSP VPN products will be generally available since late November 2003.

The first reference implementation will be started in the December 2003.

### **About the "S-Terra group"**

S-Terra group operated on the Russian market since March 2003.

CSP VPN is independent development started in March 2003. The project is based on the S-Terra's 8 year experience of the research and development of the network security products. S-Terra group inherits the product development team from the Trustworks Systems b.v. Trustworks Systems b.v. was an Amsterdam based start-up, which delivered network security products and management by the network security solutions. Specifically, the network security of the Cisco PIX and IOS devices was managed from the Trustworks' platform. This provided us with a unique knowledge of the Cisco solution. As per the network security experience – some our specialists started VPN implementation in the Elvis Plus company, who implemented Sun's SKIP protocol in 1995.