

The A to Z of Securing SSL VPNs

When protected only by typical password authentication your VPN isn't private at all. This document describes how to implement a typical CRYPTOCard two-factor authentication solution with an SSL VPN using the Juniper Networks Secure Access SSL VPN as an example.



How it Works

Virtual Private Networks allow companies to take advantage of the cost benefits and ubiquity of the internet by providing employees and business partners access to confidential corporate data, resources, and protected applications. VPNs protect the integrity of the data transmission, but do not strongly verify the identity of the end user. CRYPTO-Shield provides organizations with a strong authentication solution which ensures them that their resources are protected.

The SSL VPN is used to create encrypted tunnels between remote and mobile users, providing access to corporate networks. The SSL VPN (by default) secures browser-based access to applications, such as email portals, and other applications based upon authentication information such as a username and password. CRYPTO-Shield replaces static passwords, which can be lost, stolen, shared, or easily guessed, with strong Two-Factor authentication.

Getting Started

The process of implementing CRYPTO-Shield

strong authentication solution with an SSL VPN begins with the installation of the server. Installing CRYPTO-Server is a simple process completed in less than half an hour by following the guidelines outlined in the Getting Started Guide. During the installation an existing LDAP or Active Directory can be linked to the CRYPTO-Server.

CRYPTOCard works with the RADIUS protocol to provide two-factor authentication. To use, the end-user launches a web browser and navigates to the VPN logon page. Then using their logon name and a one-time password from their CRYPTOCard software or hardware token the end user establishes a connection to the internal network. For the end user's convenience authentication tokens are available in a variety of forms with multiple configuration options that allow you to set up tokens for each individual user in each unique environment.

Token options include:

- Key Chain Token (KT-1)— provides unparalleled convenience in a portable independent computing environment. This token type is Ideal for users of all skill levels.

Benefits of CRYPTO-Card for SSL VPNs authentication

- CRYPTO-Shield strong authentication solution is simple to configure with the SSL VPN server— provides peace of mind about the security of online assets
- Uses standard RADIUS protocol
- CRYPTO-Shield is able to support multiple devices
- Easily integrates with LDAP and Active Directory
- Provides the security needed to protect online resources

- Calculator-style Hardware Token (RB-1)— highly configurable, a multi-function device that is the most versatile hardware token. Ideal for users who desire freedom to logon from any computer running any operating system.
- Smart Card Token (SC-1)— software implementation of the RB-1 hardware installed on a 64k Java smart card. Ideal for organizations that want the advantages of a hardware token with the convenience and integration of a software token.
- USB Token(SC-3)— software implementation of the RB-1 hardware token installed on a USB packaged smart card. Ideal for organizations that want the advantages and flexibility of hardware tokens with the convenience and integration of software tokens. The SC-3 can also store digital certificates for PKI applications.
- Software token for PC, WinCE or Blackberry (ST-1)—software implementation of the RB-1 hardware token for installation on computers and PDAs. It is ideal for organizations that want the strength of two-factor authentication without the overhead and cost of hardware distribution.

To manage all token types three easy steps are necessary:

1. Assign a token to a user
2. Initialize a token
3. Test the token before deployment

After the username and one-time password are verified the SSL VPN passes the authentication information to the CRYPTO-Server via RADIUS.

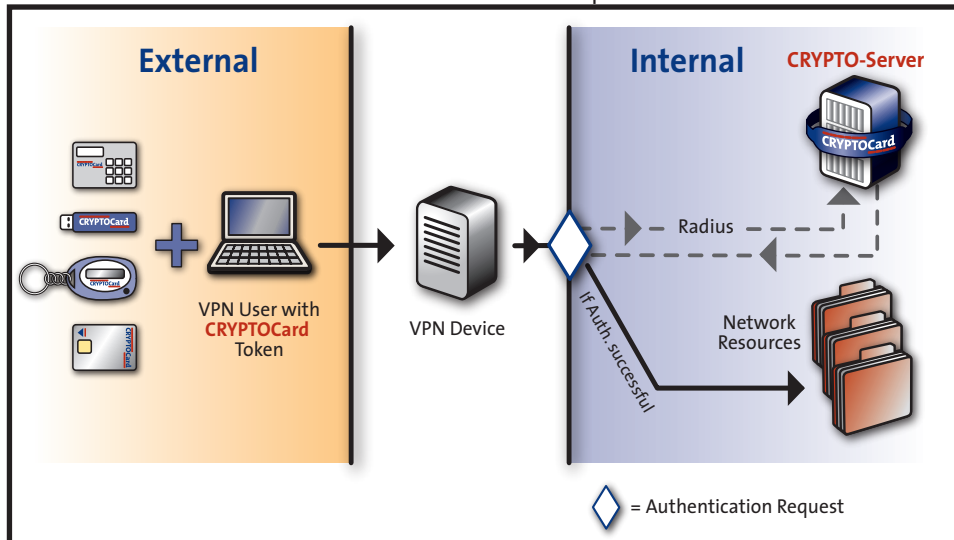
CRYPTO-Server verifies the username and password, and an “Access-Accept” message is sent to the SSL VPN, allowing the user to access the protected network and resources.

Seamless VPN Integration

CRYPTOCARD’s CRYPTO-Shield integrates with any IPSEC or SSL VPN that supports radius, including solutions from:

- Cisco
- FS
- Nortel
- AEP
- CheckPoint
- SonicWave
- Whale
- Juniper
- WatchGuard

The following document will outline the detailed process necessary to correctly configure the SSL VPN to work with CRYPTO-Shield and any variety of authentication tokens, using the Juniper Networks SSL VPN as an example.



Overview

- Authentication Process
- Authorization Process
- Configuration of CRYPTO-Server with SSL VPN
- The Configuration Process
- CRYPTO-Server Configuration
- Example using Juniper Secure Access
- Connecting to the SSL VPN Client

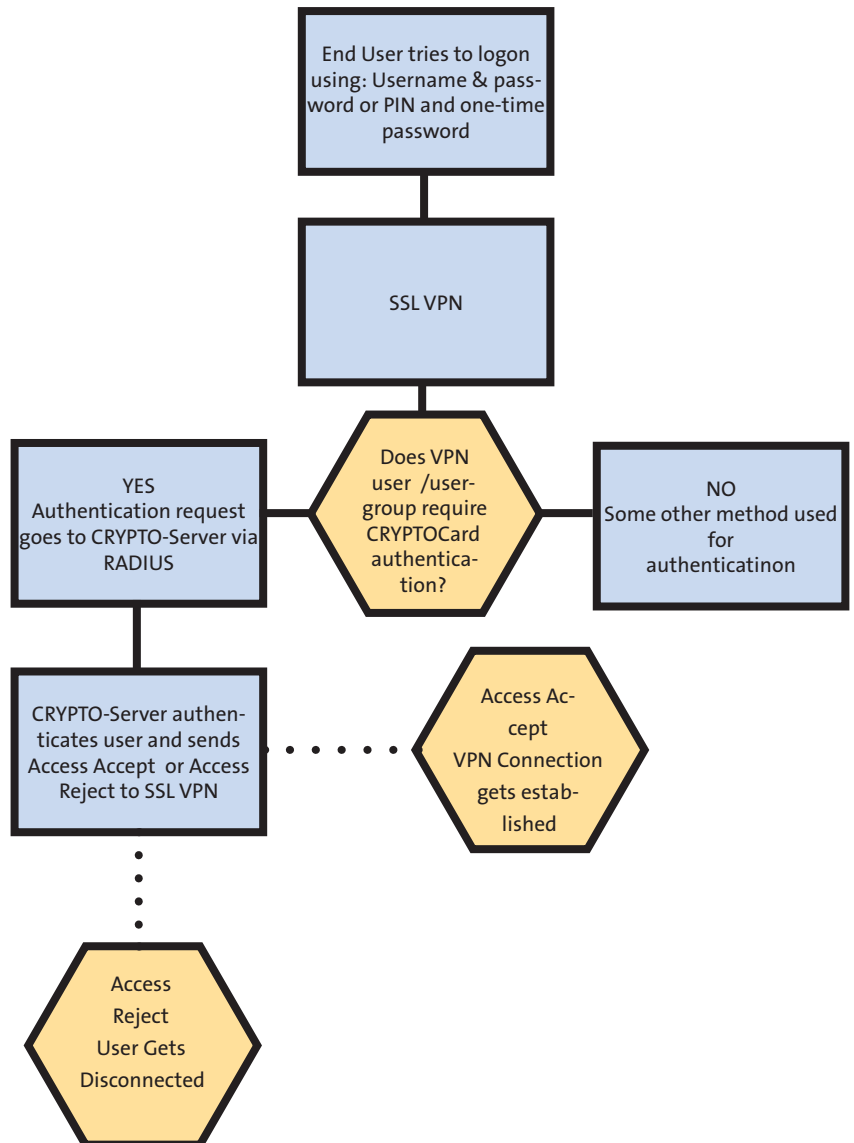
The Authentication Process

Authentication ensures only those who have access are permitted to connect to the network. A user initiates a connection to the SSL VPN. If the flow is not permitted by filters on the SSL VPN then attempt will be silently discarded and the user will not be allowed to connect. If the flow is permitted by the filters then the SSL VPN will issue an access-request to CRYPTO-Server. If CRYPTO-Server is not reachable within a specified number of retries and allotted time interval then the SSL VPN will reject the logon. If CRYPTO-Server is reachable then it will query LDAP/Active Directory to verify that the user is valid.

If not valid, CRYPTO-Server issues an “access-reject” to the SSL VPN and the user can not connect. If valid, CRYPTO-Server will do one of the following, depending upon the authentication parameters designated for this user:

- a) Locate the token(s) in the token repository that are active for the user.
- b) If no active tokens exist, check for the “static password permitted” flag. If permitted, validate static password against LDAP.
- c) If no active tokens exist and a static password is not permitted, issue access-reject.

If the user has an active token CRYPTO-Server will verify the user’s One-Time password (OTP) against the expected OTP and a “reject”, “challenge”, or “accept” message along with any other configured attributes and values will be returned. A reject message will cause the SSL VPN to deny user access. CRYPTO-Server will store RADIUS accounting logs and token authentication logs for all authentication attempts.



The Authorization Process

Authorization is the process of determining if a user account has access to specific resources. Authentication handles the “who” of network access, and authorization handles the “what”, “when”, “where”, and “how” of network access. Although many organizations use Active Directory for authorization, CRYPTO-Server has the ability to perform this function. When a CRYPTOCARD user has the ability to authenticate to the CRYPTO-Server they do not automatically receive the right to access all of the CRYPTOCARD-protected resources on a network. CRYPTO-Server is able to control certain authorization properties for certain CRYPTOCARD users.

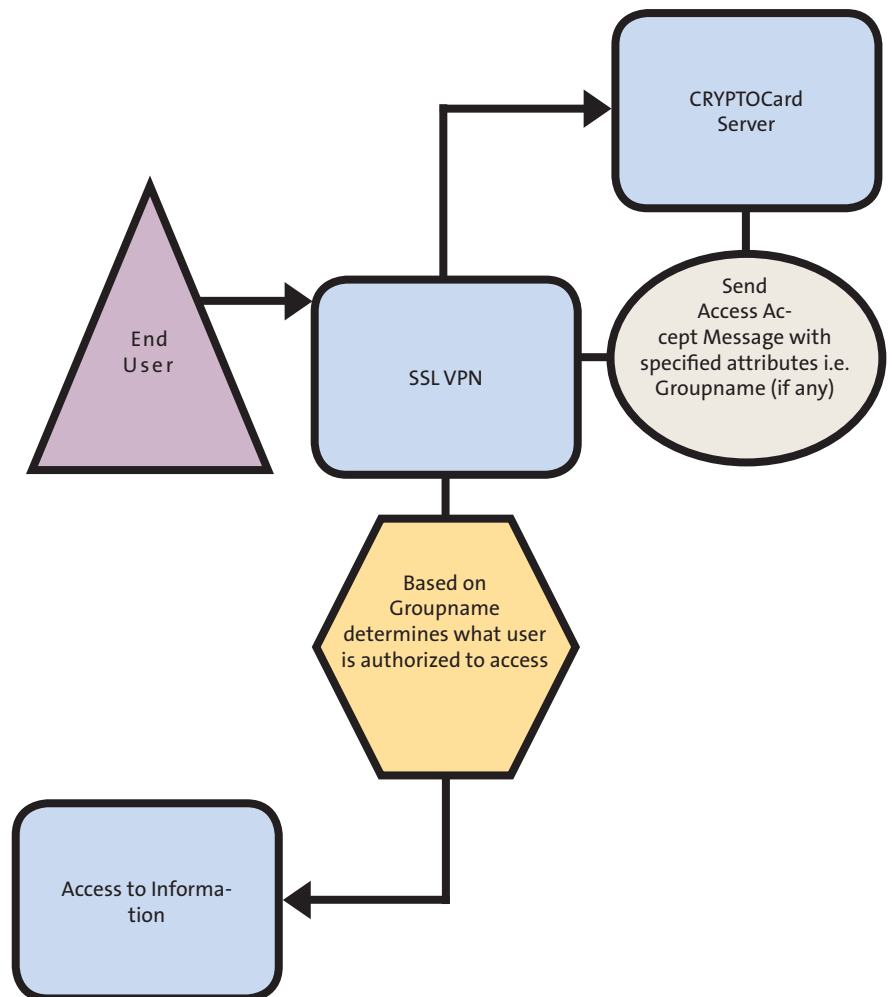
The Process

Most Users use Active Directory (LDAP) for providing authorization however, should you choose to use CRYPTOCARD to specify authorization groups the following process would take place:

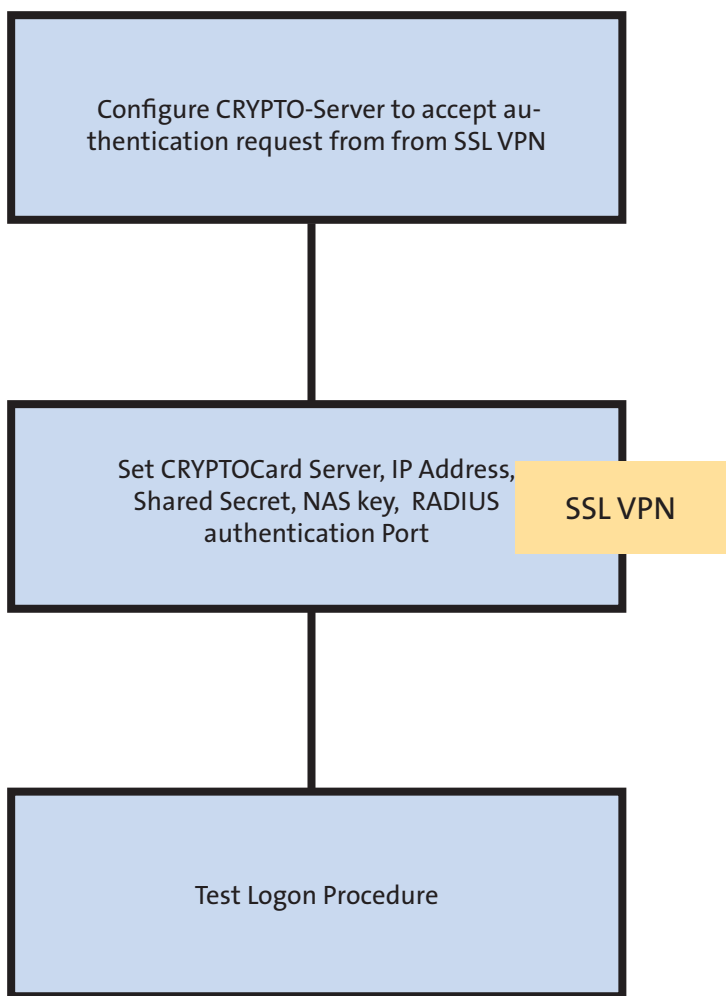
When CRYPTO-Server receives a logon request from the SSL VPN, it responds with information that allows the SSL VPN to decide which specific resources the user has access. For example, a group can be configured on the SSL VPN, with details about what time users in that group are granted network access to. When a CRYPTOCARD user authenticates the CRYPTO-Server can pass back a group name that matches the one configured in the SSL VPN, and the SSL VPN will limit the users’ access based on that group configuration.

Configuration

Authorization attributes can be set in CRYPTO-Server at the user or group level. Attributes applied at the group level automatically apply to all users in the group. Attributes applied to a user take precedence over attributes applied at the group level.



Configuration of CRYPTO-Server with an SSL VPN



The Configuration Process

The first stage in the configuration process is to configure CRYPTO-Server to accept RADIUS communications from the SSL VPN and define which RADIUS clients are allowed to connect and the shared secret they must use.

On a RADIUS client enabled VPN device the following are required to send authentication requests to CRYPTO-Server:

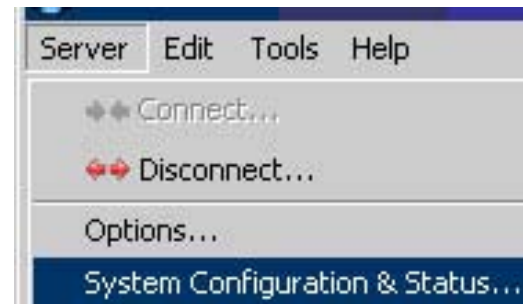
- IP address of primary CRYPTO-Server
- RADIUS authentication port (default 1812)
- Shared Secret to communicate with CRYPTO-Server
- Accounting Port (1813)

- If configuring a secondary CRYPTO-Server:
- IP address of secondary CRYPTO-Server
 - RADIUS authentication port (default 1812)
 - Shared Secret to communicate with CRYPTO-Server
 - Accounting Port (1813)

Verify above applications are performing properly by conducting a trial logon procedure.

CRYPTO-Server Configuration

To use the CRYPTO-Server as your RADIUS server verify that it is configured to accept RADIUS communications from the SSL VPN. Connect to the CRYPTO-Server using the Console and choose Server -> System Configuration & Status...from the menu



In the "Entity" column choose "RadiusProtocol". Next look at the "Value" corresponding to the key "NAS.2". The value of this key defines which RADIUS clients are allowed to connect to the CRYPTO-Server and the shared secret they must use.

A screenshot of the 'Configuration' window in the CRYPTO-Server. The window has two tabs: 'Configuration' and 'Status'. The 'Configuration' tab is active, showing a table with three columns: 'Entity', 'Key', and 'Value'. The 'RadiusProtocol' entity is selected, and the 'NAS.2' key is highlighted in blue. The value for 'NAS.2' is '192.168.21.1,192.168.21.254,,testing123,false,PAPCHAP'.

Entity	Key	Value
CapProtocol	Access.Class	com.cryptocard.cryptoadmin.capservice.EJBServerAccess
Console	AcctLog	Accounting.log
HttpProtocol	AuthLog	Authentication.log
HttpsProtocol	AuthLog.Level	both
LDAPDatabase...	DebugLog	Debug.log
LDAPDatabase...	DebugLog.Enabled	true
LDAPDatabase...	EmptyAttributes	no
Logging	Host	127.0.0.1, CC_RADIUS_PROTOCOL, 1812, 1813
MSWindows.Lo...	Local.Company	organization1
Mailer	LogAcct.Attributes	1,NAS-IP-Address,5,27,28,29,30,31,32,33,61,62,40,41,42,43
MgtServer	LogAuth.Attributes	1,2,3,NAS-IP-Address,5,6,7,8,24,25,30,31,32,33,60,61,62
ProductManager...	Lookup.Prefix	ejb/cryptocard
PtclServer	MaxSessions	1000
RSAExpirationR...	NAS.1	127.0.0.1, 127.0.0.1, loopback,testing123, false, PAPCHAP
RadiusProtocol	NAS.2	192.168.21.1,192.168.21.254,,testing123,false,PAPCHAP

The highlighted area is the IP address and shared secret of the Juniper SSL VPN which needs to match your configuration within the device. The syntax is described in the CRYPTO-Server Admin Guide.

SSL VPN Configuration (example using Juniper Secure Access)

In order for the SSL VPN to authenticate CRYPTOCARD token users, RADIUS authentication must be enabled. To add the RADIUS server complete the following:
 Choose System -> Signing In -> Authentication/Authorization Servers from the SSL VPN Administrators Console.



From the dropdown box next to the New heading choose "Radius Server", and click on the "New Server..." button.



Fill in the information for the Primary CRYPTO-Server in the New Radius Server page.

Security >
New Radius Server

Name: Label to reference this server.

Radius Server: Name or IP address

Authentication Port:

Shared Secret:

Accounting Port: Port used for Radius accounting, if applicable

Timeout: seconds

Retries:

Users authenticate using tokens or one-time passwords
Notes: If you select this, JVS will send the user's authentication method as "token" if you use SAML, and this credential will not be used in automatic SSO to backend applications.

Fill in information for the Replica CRYPTO-Server, if one exists.

Backup server

Radius Server: Name or IP address

Authentication Port:

Shared Secret:

Accounting Port: Port used for Radius accounting, if applicable

Connect using the SSL VPN Client

Once the SSL VPN has been configured correctly with the proper RADIUS server information, the end-user should be able to connect via a browser to access network resources using their CRYPTOCard token.

- Enter the CRYPTOCard username
- Enter PIN if required
- Generate a one-time password from the CRYPTOCard token.

This process will vary based on authentication token chosen:

KT-1—

An event based token which generates new one-time password each time token is activated by pressing the button beside the LCD display.

RB-1—

One-time password is displayed when user is authenticated by entering their PIN using the numeric pinpad.

SC-1—

Connect smartcard to receiving device to access software application. Enter PIN to generate a one-time password.

SC-3—

Software implementation of the RB-1 hardware token installed on a USB packaged smart card. Ideal for organizations that want the advantages and flexibility of hardware tokens with the convenience and integration of software tokens. The SC-3 can also store digital certificates for PKI applications.

ST-1 —

Enter PIN into authentication software application and a one-time password is generated.

BB-

Generates a one-time password on the BlackBerry which can be copied to the login screen.

Once the SSL VPN has verified the username and one-time password with the CRYPTO-Server the connection will be established and the user will receive access to the network. The configuration process described in this document uses the Juniper Networks SSL VPN as an example, but other SSL VPNs are configured in a similar manner.



Welcome to the Secure Access SSL VPN

Username
Password

Please sign in to begin your secure session.

CRYPTOCard North America

340 March Road
Suite 600
Ottawa, Ontario
K2K 2E4 Canada

Toll Free: 800-307-7042
Tel: +1-613-599-2441
Fax: +1-613-599-2442
E-mail: info@cryptocard.com

www.cryptocard.com

CRYPTOCard Europe

Eden Park, Ham Green
Bristol BS20 0EB,
United Kingdom

Tel: +44 870 7077 700
Fax: +44 870 7077 711
E-mail: info@cryptocard.com

www.cryptocard.co.uk

CRYPTOCard and CRYPTO-Server are registered trademarks or trademarks of CRYPTOCard Inc. in Canada, the U.S.A. and/or other countries. Microsoft and Windows are registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries. All other trademarks mentioned herein are the property of their respective owners.
© 2006 CRYPTOCard Inc.
All rights reserved.

20070626