

Supporting One–Time Passwords on ISDN

Document ID: 9395

Introduction

Prerequisites

Requirements

Components Used

Conventions

Implement Token Card Support on ISDN

Basic ISDN Authentication Options

Synchronize PPP Sessions with Token Users

PC–based TA Users

LAN–based ISDN Routers

Double Authentication

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document provides information on support for one–time passwords for ISDN connections.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Implement Token Card Support on ISDN

Ensure that these requirements are met before you implement token card support for ISDN.

- Support for both PC–based ISDN TA and LAN–based ISDN routers.
- Public Switched Telephone Network (PSTN) connections to the Novell Access Server (NAS) require one–time password (OTP) authentication when it is possible.

The implementation of Token Card support, such as RSA SecurID/access control entry (ACE)/Server, offers several design challenges. To understand these challenges, review the fundamentals of the security environment for ISDN connections.

Basic ISDN Authentication Options

In most designs, PPP is used to encapsulate datagrams over ISDN B-channels (other datagram encapsulations are not discussed in this document).

Current PPP implementations offer two primary authentication methods: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

- PAP passes the user name and password to the authenticatee in cleartext to the authenticator.
- CHAP uses a three-way handshake. The authenticator passes the user name and a challenge seed to the authenticatee. The authenticatee uses the seed received and the required password to generate a response. The authenticatee then sends the user name and the CHAP response to the authenticator for approval.

The primary advantage of CHAP is that it never sends the password over the wire, which makes it impervious to sniffer attacks.

CHAP cannot be used to support transport of a token-generated OTP unless the token vendor specifically supports CHAP by accepting the CHAP seed and CHAP response. Since OTPs are impervious to sniffer attacks by their very nature, no Token Card vendor supports CHAP.

When using async (modem) connections over the PSTN, the user can be authenticated using a character-mode login session. However, with ISDN dialup the PPP connection terminates on a synchronous interface on the NAS. This does not support character-mode login sessions. With ISDN dialup connections, authentication of the dialup user must be done with PPP (PAP or CHAP).

Note that neither PAP nor CHAP support token management for setting new-pin, next-token mode, or token challenging. These settings must be accounted for when designing OTP solutions. For example, an out-of-band method (such as async dialup in terminal mode or a Telnet to a NAS while on-site) must be used to set new-pin. Next-token mode must be shut off for PAP users.

Synchronize PPP Sessions with Token Users

When PPP sessions are to be authenticated using an OTP, the user must be requested to provide the token-generated OTP. There are challenges when the user connects with a PC-based TA or a LAN-based router.

PC-based TA Users

PPP sessions for TA users are typically terminated at the user PC. This allows the user to control the PPP session in the same manner as async (modem) dialup connections by connecting and disconnecting the session as needed. This procedure allows the user to enter their OTP for transport using PAP.

However, if the second B-channel is designed to come up automatically, the user must be prompted for a new OTP for the second B-channel. PC PPP software does not collect the second OTP, and instead tries to use the same password used for the primary B-channel. The Token Card server denies the reuse of an OTP by design. Cisco Secure ACS for UNIX, version 2.2 and later, and Cisco Secure ACS for Windows, version 2.1 and later, perform TokenCaching to support the use of the same OTP on the second B-channel. This option requires the Authentication, Authorization, and Accounting (AAA) server to maintain state information about the token user's connection. TokenCaching via ascii login during callback is supported in Cisco Secure ACS for Windows release 2.3(3) and later.

For more information on TokenCaching, the recommended solution for supporting two B-channels for PC TA users, refer to the TokenCaching Design and Implementation Guide.

LAN-based ISDN Routers

PPP sessions for LAN-based ISDN router users are terminated at the router. The router must be configured with the PPP authentication password. ISDN (and PPP) connections are automatically set up and torn down by the ISDN router based on *interesting* traffic and Dial-on-Demand Routing (DDR) logic in the router.

There is one primary challenge with this type of connection for Token Card support. The user with the token is not at the end of the PPP connection, but on a machine connected via Ethernet to the ISDN router. How is the OTP collected from the user for the ISDN session?

Technically, the token user can Telnet (or connect with an RS-232) to the ISDN router and override the automatic DDR behavior by taking direct control of the ISDN connections (and configuring the OTP for each connection). This solution can be accomplished with the user interface provided by the router vendor. If this solution is used, PAP must be used (for transport of the OTP) and can be combined with TokenCaching at the central site to provide secondary B-channel support.

Double Authentication

Token Card support for ISDN DDR routers can be implemented with Double Authentication (this feature was introduced in Cisco IOS® Software Release 11.3). This method eliminates the need for the user to set the PPP password on the router by using two stages of authentication: hardware authentication and user authentication.

Hardware authentication occurs over the PPP session using a fixed password (preferably CHAP). This method causes a virtual-access interface to be set up on the NAS with an access control list that allows the remote devices to Telnet to a single IP address only.

User authentication occurs over a Telnet session using a token-generated OTP. Once authenticated, the remote user enters the **access-profile** command, which reconfigures the virtual-access interface to remove the access control list.

For more information, refer to the Double Authentication Design and Implementation Guide.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [Cisco Secure ACS for UNIX Support Page](#)
 - [Documentation for Cisco Secure ACS for UNIX](#)
 - [TACACS/TACACS+ Support Page](#)
 - [TACACS+ in IOS Documentation](#)
 - [Technical Support – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 14, 2009

Document ID: 9395
