

# Security Prime

## Managed Internet Security Service

---

### Overview

The Security Prime service combines dynamic packet filtering, advanced user authentication, and logging to provide network and Internet security.

A Proteon GTX1000 Secure router, external CSU/DSU, and CRYPTOCards are provided as part of the Security Prime service.

A custom site security profile will be designed in conjunction with your site security officer and PSINet's Managed Services Group (MSG). This profile will then be installed, managed, and maintained by MSG at the direction of your site security officer.

### Dynamic Packet Filtering

Dynamic filters are installed in response to a pattern of traffic. Thus, holes in the router can be opened or closed in response to particular events.

For example, if static filters are used for outgoing Domain Name Service requests, the router must accept all inbound traffic using the UDP protocol in order to receive the answer.

On the other hand, when dynamic filters are used, the router accepts incoming packets only when it expects a response to outgoing requests. This minimizes the traffic the router will accept and the security risk. Dynamic filters also have usage timers that allow them to be dropped from the router configuration after a period of time.

### Advanced User Authentication

Dynamic filtering allows us to tailor access with custom user profiles for individuals who use CRYPTOCards.

For example, if you are traveling and need to gain telnet access to a server at your site, you need to use the CRYPTOCARD to authenticate yourself and respond to the router's challenge.

If your response is correct, the router opens a rule in memory for your current session (the user profile). In our telnet example, this rule allows incoming telnet to the internal server from the IP address you just authenticated from.

After 5 minutes of inactivity, the user profile is dropped. If you wish to continue, you need to log in and authenticate again. (The time period is configurable.)

*Please see "How to use CRYPTOCards" for further details.*

## Logging

Daily security reports are e-mailed to your site security officer. The reports show failed attempts at connections with the source IP address, destination IP address, and port (service).

These reports should be reviewed by your site security officer since MSG **does not** regularly review the logs. Anything unusual should be brought to the attention of MSG.

## Installation

The equipment is shipped to your site preconfigured with no security implemented. The security policy will be installed after connectivity to the router has been established.

While awaiting the circuit installation, please fill out the Site Security Profile included with this service guide and return it to MSG.

Any questions or discussions about the Site Security Profile should be directed to MSG. Contact information is shown below.

## Contacting MSG

MSG should be contacted for security issues, security policy definition, security policy changes, and any issues relating to the equipment provided with the Security Prime service.

PSINet Support	<b>(518) 283-8860</b> Follow the options for the Managed Services Group.
Corporate Installations FAX	<b>(518) 286-2544</b>
E-mail	<b>spart@psi.com</b>

## Making Security Implementation Changes

Any security policy changes need to be formally requested by a listed site security officer. The change must come in the form of a written request, either in electronic mail to spart@psi.com or by fax. Phone requests will not be accepted, although we will be happy to discuss the changes over the phone with the site security officer.

## Locked CRYPTOCards

If you are unable to enter the correct PIN within six attempts, the card becomes locked. This feature erases the DES key along with all other information stored in the access control card. The access control card must be returned to the keymaster at PSINet for reprogramming.

Send locked cards to :

PSINet Inc.  
Attn: Keymaster  
44983 Knoll Square  
Ashburn, VA 20147

## CRYPTOCARD Loss or Theft

Notify PSINet's Managed Services Group as quickly as possible if a card is lost or stolen. The user information on the authentication servers must be changed to maintain security. E-mail your message to:

**spart@psi.com.**

## CRYPTOCARD Replacement

There is a charge for lost, stolen or damaged access control cards. Details are outlined in the Security Prime service option contract.

Requests for replacement cards should be directed to:

PSINet Inc.  
Attn: Keymaster  
44983 Knoll Square  
Ashburn, VA 20147

## Batteries

The batteries in the CRYPTOCARD should last up to three years.

When the unit's batteries require replacement, new batteries can be purchased at any retail electronics outlet.

Batteries should be changed one at a time so that the DES keys stored in the card's flash memory are not erased.

***If both batteries are removed at the same time, the card will have to be reprogrammed by the PSINet keymaster.***

## How to use CRYPTOCards

---

### To use your CRYPTOCard for the first time:

When the cards are first shipped to your site, the PIN (Personal Identification Number) will be 1111. You must change the PIN before you can open a Telnet session to your secured network.

1. Turn the CRYPTOCard on and enter the initial PIN (1111).

You will be forced to change the PIN.

2. Key a number at least four digits in length, then press ENT.

The card will now asks you to verify your choice.

3. Re-key the same PIN and press ENT again.

The card is now ready to be used.

***Please do not forget the PIN since it is not possible to recover it. If you do forget the PIN, the card must be reprogrammed.***

*See the Locked CRYPTOCards section for reprogramming details.*

### To use the CRYPTOCard to access your site LAN:

1. Open a telnet session to the Serial IP address of the Proteon router.

2. When the router prompts you for a User ID, please enter the serial number on the back of the CRYPTOCard.

3. When you are prompted for a password, just press <ENTER>.

The router now issues a challenge.

4. Press the CH/MAC key on the CRYPTOCard and then enter the challenge into the card followed by the ENT key.

The CRYPTOCard produces a response consisting of alphanumeric characters.

5. Enter the response to the router.

If the response is correct, your Telnet session to the router will close. You are no longer connected to the Proteon router.

6. Now open a session directly to the machine you are trying to reach.

For example, if you need to FTP to an internal FTP server, open an FTP session directly to the internal FTP server.