

---

## ★ Security Prime Site Security Profile ★

---

The information you provide will be used to design a custom security configuration for your site. The Security Prime Site Security Profile contains the following sections:

### ★ Security Officer Information

Security Officer Information is used to verify identity when requesting filter changes or discussing site security issues.

### ★ Firewall Information

The firewall section specifies what is going to be filtered on the Security Prime router, that is, what packets will be allowed to pass and which will be rejected. These restrictions apply to general Internet users who do not have an access control card.

### ★ User Profiles

User profiles specify what privileges access control holders have after authentication.

For example, you can leave inbound Telnet as the default of 'No' in the firewall section, but check Telnet (to allow it) in the user profile section. By choosing these options, any external user who does not have a card will *not* be able to Telnet into the LAN. However, an access control card holder *will* be able to Telnet into the LAN after completing the authentication process.

**We have included one user profile sheet with this survey. Please make as many copies as you need.**

**It is important to note that your Security Prime router has no security configured on it when it is shipped. All security configuration is done by a member of Managed Services after we receive this profile.**

**Please fax completed form to PSINet Corporate Installations:  
(518) 283-8904**

## Security Officer Information

---

These are the ONLY individuals who will be able to request changes to any filters at your Security Prime site. We recommend you have at least two contacts to allow for instances when one of the contacts is out of the office or otherwise unreachable\*.

**Account ID:** \_\_\_\_\_

### Primary Security Officer

**Name** \_\_\_\_\_

**Phone** \_\_\_\_\_

**E-mail** \_\_\_\_\_

**Signature** \_\_\_\_\_

**Date** \_\_\_\_\_

### Other Security Officers

**Name** \_\_\_\_\_

**Phone** \_\_\_\_\_

**E-mail** \_\_\_\_\_

**Signature** \_\_\_\_\_

**Date** \_\_\_\_\_

\*If you need more room please indicate additions on a separate sheet of paper.

## Firewall

---

Use this section to build the dynamic packet filters which will be applied to the router.

With inbound services, a default of 'No' is assumed.

If the traffic restriction applies only to a specific IP address, please fill in that IP address. Otherwise, we will assume it applies to the entire network.

**By default, all outbound TCP services are allowed.** If you want to limit outbound TCP services or IP addresses which have access to outbound TCP services, please list your requirements on a separate sheet of paper.

## Common Services & Utilities

Service	Inbound		IP Address (If left blank, we assume all.)
	Yes	No (default)	
Telnet	<input type="checkbox"/>	<input type="checkbox"/>	_____
FTP	<input type="checkbox"/>	<input type="checkbox"/>	_____
WWW	<input type="checkbox"/>	<input type="checkbox"/>	_____
SSL	<input type="checkbox"/>	<input type="checkbox"/>	_____
Winframe	<input type="checkbox"/>	<input type="checkbox"/>	_____
Oracle	<input type="checkbox"/>	<input type="checkbox"/>	_____
Whois	<input type="checkbox"/>	<input type="checkbox"/>	_____
Finger	<input type="checkbox"/>	<input type="checkbox"/>	_____
PPTP	<input type="checkbox"/>	<input type="checkbox"/>	_____
POP	<input type="checkbox"/>	<input type="checkbox"/>	_____

## SNMP

PSINet will provide you with daily and weekly bandwidth utilization reports if desired.

Would you like PSINet to poll the router using SNMP?  Yes  No

E-mail reports to: \_\_\_\_\_

## E-mail

Will you be sending and receiving SMTP e-mail through the Security Prime router?  Yes  
 No

IP address(es) of the SMTP gateway(s): \_\_\_\_\_

## USENET News server

Have you purchased a USENET news feed from PSINet?  Yes  No

IP Address(es) of your news server(s): \_\_\_\_\_

## Name Service

Are you providing primary name service for any domains?  Yes  No

IP address of the name server(s): \_\_\_\_\_

## Time Protocols

Service	Inbound		IP Address (If left blank, we assume all.)
	Yes	No (default)	
daytime	<input type="checkbox"/>	<input type="checkbox"/>	_____
rdate	<input type="checkbox"/>	<input type="checkbox"/>	_____

NTP is another possible time protocol, but it must be allowed both inbound and outbound to utilize it.

Do you plan to use NTP?  Yes  No

To which IP address(es): \_\_\_\_\_

## Ping, Traceroute, & ICMP

Service	Outbound		Inbound		IP Address (If left blank, we assume all.)
	Yes (default)	No	Yes	No	
ping	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> (default)	<input type="checkbox"/>	_____
traceroute	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> (default)	_____

## Special Requests

There are many additional services you may want to allow through your Security Prime router. The following are a few examples of protocols and applications that MSG can allow through the firewall. As the Internet grows, new applications are developed and the list of possibilities will grow. Please list any additional requests on the following page. Keep in mind that your Site Security contact can make additions or changes in the future by contacting a MSG engineer.

Application/ Protocol	Request Specifics (To where, from where, etc.)
CuSeeMe	_____
Timbuktu	_____
RealAudio	_____
PCAnywhere	_____

## ***Additional Requests***

List of restricted sites by IP address (if applicable):

Please list any other additional requests that have not yet been addressed:

## User Profiles For Access Control Cards

---

Please list the serial numbers of your Access Control Cards:

1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_
4. \_\_\_\_\_
5. \_\_\_\_\_

The default profile for CryptoCards is to allow access on **all** ports to **all** internal addresses. If you would like to limit ports by IP address or by CryptoCard please comment below:

## Using Access Control Cards

---

**Note:** First you must be logged on to the Internet. You **cannot** use a CryptoCard from inside of your LAN.

### **Method 1:**

Works for all Security Prime accounts.

1. Telnet to the NxNetworks (formerly Proteon/OpenRoute) router serial IP.
2. You will be prompted for a login. This is the serial number of the card.
3. You will then be prompted for a password. Just press 'Enter' here.
4. The router will give you a challenge. It will be a string of digits. Press the 'CH/MAC' button on the access control card and then proceed to enter the challenge into the card.
5. The card will produce a response to the challenge. It will be a string composed of both digits and letters. Enter the response to the router.
6. If successful, the telnet session to the router will close. You are no longer connected.
7. At this point, and only at this point, you are able to connect into your LAN by opening up a new connection to the host you wish to reach. For example, if telnet is allowed for CryptoCard users, you can open a telnet connection directly to the internal machine you wish to connect to.

### **Method 2:**

Works only with OpenRoute 3.0 or later code on NxNetworks (Proteon GT-62) routers.

1. Connect to the router's serial IP address with a web browser.
2. Enter the serial number of the card in the Login box. Leave the Password box blank. Click on the 'Authenticate' button.
3. The browser will return a challenge. It will be a string of digits. Press the 'CH/MAC' button on the access control card and then proceed to enter the challenge into the card.
4. The card will produce a response to the challenge. It will be a string composed of both digits and letters. Enter the response in the box on the browser and click 'Authenticate'.
5. If successful, the browser will flash an "Authentication Successful" message.
6. At this point, and only at this point, you are able to connect into your LAN by opening up a new connection to the host you wish to reach. For example, if telnet is allowed for CryptoCard users, you can open a telnet connection directly to the internal machine you wish to connect to.