



**ProWatch Secure  
Service Description  
May 2003**

## **SERVICE DESCRIPTION**

---

ProWatch Secure services provide management and monitoring of network security technologies, reporting and consultation, and configuration modifications. NetSolve offers the following primary service options:

- Remote Intrusion Detection (RID) service for Network Intrusion Detection Systems (NIDS)
- Managed Firewall (MFW) service
- RID service for Host Intrusion Detection Systems (HIDS)

### Optional Services:

- Managed Screening Router (MSR) service for routers is desirable with any of the above service selections. RID or MFW services are a prerequisite for ordering MSR service.
- Data Management service. ProWatch Secure MFW service is a prerequisite for ordering Data Management service.
- High Availability (HA) service. Managed Firewall service is a prerequisite for ordering HA service.
- Virtual Private Network (VPN) service.
- Point-to-point Virtual Private Network (VPN). ProWatch Secure MFW or ProWatch for WANs services are a prerequisite for ordering VPN service.
- IOS based Firewall Feature Set when implemented in conjunction with NetSolve's ProWatch for WANs or Managed Screening Router Service.

# Table of Contents

<b>TABLE OF CONTENTS</b> .....	<b>3</b>
<b>1. DEFINITIONS</b> .....	<b>4</b>
1.1. REFERENCED DOCUMENTS .....	4
<b>2. NETSOLVE SERVICE OPTIONS</b> .....	<b>4</b>
2.1. COMMON SERVICES .....	5
2.1.1. <i>Reporting</i> .....	5
2.2. PRIMARY SERVICES .....	5
2.2.1. <i>Remote Intrusion Detection Service for NIDS</i> .....	5
2.2.2. <i>Managed Firewall</i> .....	6
2.2.3. <i>Remote Intrusion Detection Service for HIDS</i> .....	8
2.3. OPTIONAL SERVICES* .....	9
2.3.1. <i>Managed Screening Router (MSR)</i> .....	9
2.3.2. <i>Security Policy Development and Device Configuration</i> .....	10
2.3.3. <i>Managed Log Host</i> .....	10
2.3.4. <i>High Availability Firewall Service</i> .....	11
2.3.5. <i>VPN Implementation</i> .....	11
2.3.6. <i>IOS Firewall Feature Set</i> .....	11
<b>3. CUSTOMER RESPONSIBILITIES</b> .....	<b>12</b>
<b>4. Supported Equipment</b> .....	<b>13</b>

## 1. Definitions

**Firewall** - Security device designed to protect internal networks from unauthorized access from external sources, while allowing external users to access specific authorized public resources such as web servers, and allowing internal users access to external resources.

**IDS** – Security technology designed to monitor and analyze TCP/IP traffic by utilizing a real-time intrusion detection engine that examines each individual packet, including its header and payload, as well as its relationship to adjacent and related packets in the data stream. Immediately after the Sensor detects a policy violation, it sends an alarm to a central console. When implemented in conjunction with a router or a PIX firewall, some intrusion detection systems can be programmed to automatically respond by blocking the source of the attack from further access to the network. Some IDS systems can also be configured to terminate active TCP sessions that show characteristics of an attack.

**Host IDS** – Security software that resides on a network server designed to monitor and alarm on suspicious activity on that server and in some cases take protective action.

**VPN** – Provides private connections across a public network, such as the Internet, using encryption technology to maintain privacy.

**HA Firewall** – A HA firewall configuration is comprised of dual redundant firewalls configured for synchronization and automatic fail-over as protection against a single point of failure in the network.

**Screening Router** – A router that, through the use of access control lists, can restrict certain network traffic. When used in conjunction with a firewall or IDS, a screening router can provide a response mechanism to attacks. This is often the Internet router.

**ProWatch Exchange** – NetSolve’s network management web portal interface

**NMC** – [NetSolve] Network Management Center

**NSE** – NetSolve Security Engineer

**CSO** – [NetSolve] Customer Service Order

### 1.1. Referenced Documents

The following NetSolve documents are referenced in, and are considered part of, this Service Description:

DOCUMENT TITLE	REVISION DATE
NetSolve Moves, Adds, Changes	August 2003

## 2. NetSolve Service Options

The section below entitled Common Services applies to the ProWatch Secure RID service for NIDS, the ProWatch Secure RID service for HIDS, and the ProWatch Secure MFW. The section titled “Primary Services” contains three sections that describe the additional components of the RID service for NIDS, the MFW service, and the RID service for HIDS. The services that will be delivered will be set forth on the CSO between NetSolve and the Customer. The section titled “Optional Services” describes the Managed Screening Router, Data Management, High Availability, and Virtual Private Networking services that will be provided if purchased separately. Equipment supported by ProWatch Secure services is listed in the **Supported Equipment** section of this document.

## **2.1. Common Services**

Common services are defined as services that are to be delivered to the Customer in conjunction with at least one of the primary service selections listed below and will not be delivered independently. These services include:

### **2.1.1. Reporting**

NetSolve provides real-time reporting and Customer interaction through ProWatch Exchange. ProWatch Exchange is a web portal that allows the Customer to view the following detail concerning the security management of their site:

- Fault notification – real-time notification of connectivity outages and anomalies at the time of detection.
- Security event notification reports – real-time notification of malicious or otherwise relevant security event.
- Trouble Tickets – a breakdown of alarmed events along with an analysis of the severity and preventive actions taken at the time of alarm.
- Monthly Summary – the ProWatch Secure RID service will include a summary of alarmed events for the prior month.

Upon Customer or Partner request, NetSolve will participate in reviews of security events, analysis of security configuration, access policy review, and future design review consultative conference calls.

## **2.2. Primary Services**

NetSolve will implement Internet security in one or more of the following configurations for the managed site:

### **2.2.1. Remote Intrusion Detection Service for NIDS**

- Event management - NetSolve provides 24x365 monitoring for the following:
  - Fault events
    - Event-driven polling not only checks the device for connectivity, but also checks connectivity at the application layer, NetSolve's management software and NetSolve's ticketing database to ensure that the entire system is working properly. This approach is far superior to simply polling the managed device for connectivity.
    - Upon receipt of an alarm at the NMC (loss of poll access) a Trouble Ticket will be opened against the device.
    - Fault isolation procedures will be initiated.
    - NetSolve will engage secondary management channel, typically a dial-up modem, as required to expeditiously isolate root cause.
    - Customer's security contact will be notified of the event.
    - NetSolve will assist with efforts to restore service expeditiously and inform Customer of escalation and changes in fault status.
  - Security events
    - NIDS sensors are designed to detect and generate an alarm for attacks included in the technology's signature database. Upon receipt of a security alarm at the NMC:
      - > For high-level security events, either a Level 4 or Level 5 alarm as configured in the NIDS configuration file, a Trouble Ticket will be automatically opened on external threats.
      - > An initial review will determine the severity of the alarm consisting of a combination of the alarm level along with the application of knowledge of the Customer's network. If the alarm is verified, NetSolve will notify the Customer. In the event that the alarm is benign, NetSolve will follow customer defined escalation procedures. Customer's security contact will be notified of the event.

Notification of the event will take place either through NetSolve's Auto Notification process or through direct contact from the NMC Technician. The Auto Notification process allows the Customer to be notified of certain events through e-mail or pager and includes confirmation mechanisms for the receipt of the event.

- > Security event handling procedures will be initiated.
- > NMC Technicians will validate the response and conduct elementary forensics analysis and enhanced network monitoring to validate the effectiveness of the response.
- > For certain signatures, automatic response may be deactivated if it interferes with a service required during the Customer's normal course of business. Decisions regarding deactivation will be at the Customer's direction and predefined where appropriate. Response to attacks that do not have a predefined automatic response will be determined on a case-by-case basis with the Customer.
- NetSolve will work with the Customer on an on-going basis to revise alarm notification policies and procedures for detected security events.
- Configuration Management
  - Emergency modifications to the security policy, or recovery due to a device failure will be initiated within four hours of receipt of written request.
  - Emergency configuration change requests will be handled within four hours.
  - All other configuration change requests are subject to the procedures and fees established in NetSolve's Moves, Adds, Changes document. NetSolve will archive the current configuration each time NetSolve makes a configuration change.
  - In order to provide for the optimum performance and reliability of the supported components, software upgrades may be periodically required. NetSolve will:
    - Track the bug lists, release notes, and feature lists associated with each supported component and make upgrade recommendations.
    - Recommend to Customer when to upgrade to newer releases of software and firmware, and remotely install software upgrades that Customer is entitled to under applicable maintenance agreements, or upgrades provided by the manufacturer to correct defects. Recommended upgrades requiring additional software/firmware, upgraded hardware, or on-site installation as approved for purchase by the Customer, will be at Customer's expense.
- Fault and security events will be recorded in a NetSolve database to expedite historic analysis of site performance and assist in maintaining network perimeter security. This event information will be stored actively in NetSolve's database for three months. If the Customer requires historical archiving of event information beyond three months, the Data Management service is required.

### **2.2.2. Managed Firewall**

- NetSolve provides 24x365 monitoring of the following:
  - Fault events
    - Event-driven polling not only checks the device for connectivity, but also checks connectivity at the application layer, NetSolve's management software and NetSolve's ticketing database to ensure that the entire system is working properly. This approach is far superior to simply polling the managed device for connectivity.
    - Upon receipt of an alarm at the NMC (loss of poll access) a Trouble Ticket will be opened against the device.
    - Fault isolation procedures will be initiated.

- NetSolve will engage secondary management channel, typically a dial-up modem, as required to expeditiously isolate root cause.
- Customer's security contact will be notified of the event.
- NetSolve will assist with efforts to restore service expeditiously and inform Customer of escalation and changes in fault status.
- Security events
  - Firewalls are monitored for malicious activity on a Customer's network. Upon detection of such activity, a Trouble Ticket is opened in the NMC.
  - Customer's security contact will be notified of the event.
  - Security event handling procedures will be initiated.
- NetSolve will work with the Customer on an ongoing basis to revise alarm notification policies and procedures for detected activities.
  - NetSolve provides the following additional services in support of the NetSolve Managed Firewall Service:
    - If Customer has purchased the optional point-to-point VPN on a firewall, NetSolve will open a Trouble Ticket for the following IPsec VPN events:
      - > VPN tunnel failures
      - > Authentication failures
      - > Security Association rejections
    - For the PIX Firewall, NetSolve will also open a Trouble Ticket for the following scalability and lifecycle events:
      - > Memory errors
      - > Resource over-utilization
      - > Unacceptable loads
      - > Internal logic errors
- Configuration Management
  - Emergency modifications to the access policy, or recovery due to a device failure will be initiated within four hours of receipt of written request.
  - All other configuration change requests are subject to the procedures and fees established in NetSolve's Moves, Adds, Changes document.
  - NetSolve will archive the current configuration each time NetSolve makes a configuration change.
  - In order to provide for the optimum performance and reliability of the supported components, software upgrades may be periodically required. NetSolve will:
    - Track the bug lists, release notes, and feature lists associated with each supported component and make upgrade recommendations.
    - Recommend to Customer when to upgrade to newer releases of software and firmware, and remotely install software upgrades that Customer is entitled to under applicable maintenance agreements, or that is provided by the manufacturer to correct defects. Recommended upgrades requiring additional software/firmware, additional or upgraded hardware, or on-site installation as approved for purchase by the Customer, will be at Customer's expense.

- Fault and security events will be recorded in a NetSolve database to expedite historic analysis of site performance and assist in maintaining network perimeter security. This event information will be stored actively in NetSolve's database for three months. If the Customer requires historical archiving of event information beyond three months, the Data Management service must be purchased.

### **2.2.3. Remote Intrusion Detection Service for HIDS**

- Event management - NetSolve provides 24x365 monitoring for the following:
  - Fault events
    - Event-driven polling not only checks the device for connectivity, but also checks connectivity at the application layer, NetSolve's management software and NetSolve's ticketing database to ensure that the entire system is working properly. This approach is far superior to simply polling the managed device for connectivity. Upon receipt of an alarm at the NMC (loss of poll access) a Trouble Ticket will be opened against the device.
    - Fault isolation procedures will be initiated.
    - Customer's security contact will be notified of the event.
    - NetSolve will assist with efforts to restore the service expeditiously and inform Customer of escalation and changes in fault status.
  - Security events
    - HIDS are designed to detect and generate an alarm for attacks included in the technology's signature database and shield the protected operating system or application from behavior that violates the security profile established by the customer. If the system is running in monitoring mode an alarm will be generated upon detection of an attack and a security alarm will be delivered to the NMC. If the system is running in protection mode the attack will be prevented and then an alarm will be generated and delivered to the NMC. Upon receipt of an alarm the following procedures will be followed:
      - > For pre-defined high-level security events a Trouble Ticket will be automatically opened.
      - > An initial review will determine the severity of the alarm consisting of a combination of the alarm level along with the application of knowledge of the Customer's network and the applications running on the server. If the alarm is verified, NetSolve will notify the Customer. In the event that the alarm is benign, the ticket will be closed without notifying the Customer.
      - > Customer's security contact will be notified of the event. Notification of the event will take place either through NetSolve's Auto Notification process or through direct contact from the NMC Technician. The Auto Notification process allows the Customer to be notified of certain events through e-mail or pager and includes confirmation mechanisms for the receipt of the event.
      - > Security event handling procedures will be initiated.
      - > NMC Technicians will validate the response and conduct elementary forensics analysis and enhanced network monitoring to validate the effectiveness of the response.
      - > For certain signatures, automatic response may be deactivated if it interferes with a service required during the Customer's normal course of business. Decisions regarding deactivation will be at the Customer's direction and predefined where appropriate. Response to attacks that do not have a predefined automatic response will be determined on a case-by-case basis with the Customer.
    - NetSolve will work with the Customer on an on-going basis to revise alarm notification policies and procedures for detected security events.
- Configuration Management

- Emergency modifications to the security policy, or recovery due to a device failure will be initiated within four hours of receipt of written request.
- Emergency configuration change requests will be handled within four hours.
- All other configuration change requests are subject to the procedures and fees established in **NetSolve's Moves, Adds, Changes** document. NetSolve will archive the current configuration each time NetSolve makes a configuration change.
- In order to provide for the optimum performance and reliability of the supported components, software upgrades may be periodically required. NetSolve will:
  - Track the bug lists, release notes, and feature lists associated with each supported component and make upgrade recommendations.
  - Recommend to Customer when to upgrade to newer releases of software, and remotely install software upgrades that Customer is entitled to under applicable maintenance agreements, or upgrades provided by the manufacturer to correct defects. Recommended upgrades requiring additional software/firmware, upgraded hardware, or on-site installation as approved for purchase by the Customer, will be at Customer's expense.
- Fault and security events will be recorded in a NetSolve database to expedite historic analysis of site performance and assist in maintaining network perimeter security. This event information will be stored actively in NetSolve's database for three months.

## **2.3. Optional Services\***

### **2.3.1. Managed Screening Router (MSR)**

- NetSolve provides 24x365 monitoring for the following:
  - Fault events
    - Event-driven polling not only checks the device for connectivity, but also checks connectivity at the application layer, NetSolve's management software and NetSolve's ticketing database to ensure that the entire system is working properly. This approach is far superior to simply polling the managed device for connectivity.
    - Upon receipt of an alarm at the NMC (loss of poll access) a Trouble Ticket will be opened against the device.
    - Fault isolation procedures will be initiated.
    - NetSolve will engage secondary management channel, typically a dial-up modem, as required to expeditiously isolate root cause.
    - Customer's security contact will be notified of the event.
  - NetSolve will assist with efforts to restore service expeditiously and inform Customer of escalation and changes in fault status.
  - NetSolve will provide scheduled support of the following Monday – Friday during the hours of 8AM-5PM Central time:
  - Configuration Management
    - The administration of Customer access lists on the router on a limited basis as agreed to between Customer and NetSolve.
    - Archival of the current configurations.
    - Management of the communication channel between router and IDS device for RID Customers only.

- All configuration change requests are subject to the procedures and fees established in NetSolve's Moves, Adds, Changes document.
- Life-Cycle Management - In order to provide optimum performance and reliability of the supported components, software upgrades may be periodically required. NetSolve will:
  - Track the bug lists, release notes, and feature lists associated with each supported component and make upgrade recommendations.
  - Recommend to the Customer when to upgrade to newer releases of software and firmware, and remotely install software upgrades that Customer is entitled to under applicable maintenance agreements, or that is provided by the manufacturer to correct defects. Recommended upgrades requiring additional software/firmware, additional or upgraded hardware, or on-site installation as approved for purchase by the Customer, will be at Customer's expense.

### **2.3.2. Security Policy Development and Device Configuration**

NetSolve:

- May coordinate with the Customer to develop an access control policy based on the business requirements set forth by the Customer. The Customer may also develop an access policy in conjunction with one of NetSolve's partners or they can develop it internally.
- May develop configurations for devices to be managed that represent and enforce the recommended access control policy. The Customer may also develop these configurations in conjunction with one of NetSolve's partners or they can develop them internally in coordination with NetSolve.
- May pre-configure all devices to be managed with the configurations developed. The Customer may also work with a partner or configure these devices internally.
- Will establish an encrypted channel for fault detection and alarm notification to the NMC.

### **2.3.3. Managed Log Host**

- NetSolve will provide 24x365 monitoring for the following:
  - Fault events –
    - Event-driven polling not only checks the device for connectivity, but also checks connectivity, the application layer, NetSolve's management software and NetSolve's ticketing database to ensure that the entire system is working properly. This approach is far superior to simply polling the managed device for connectivity.
    - Upon receipt of an alarm at the NMC (loss of poll access) a Trouble Ticket will be opened against the device.
    - Fault isolation procedures will be initiated.
    - NetSolve will engage secondary management channel, typically a dial-up modem, as required to expeditiously isolate root cause.
    - Customer's security contact will be notified of the event.
  - NetSolve will assist with efforts to restore service expeditiously and inform Customer of escalation and changes in fault status.
- NetSolve will provide scheduled support of the following Monday – Friday during the hours of 8AM-5PM Central time:
  - Configuration Management
    - The administration of Customer access lists on the router on a limited basis as agreed to between the Customer and NetSolve.

- Management of the communication channel between the Data Management Server and IDS device for RID Customers only.
- All configuration change requests are subject to the procedures and fees established in NetSolve's Moves, Adds, Changes document.

Managed Log Host is an optional service for the NIDS, HIDS and MFW services. NetSolve collects firewall and IDS log data to enable more in-depth analysis and troubleshooting of service denials. NetSolve currently maintains three months of active security event data. If the Customer desires the ability to archive and maintain historical event data, they can accomplish this by purchasing the Managed Log Host service. In addition to historical archives of security data, the Log Host will maintain data that is not transferred to NetSolve, such as full syslog outputs from a firewall. This data allows for more complete troubleshooting and security analysis on a firewall.

#### **2.3.4. High Availability Firewall Service**

HA service is an optional MFW service. The HA service allows the Customer to maintain two firewalls in parallel with identical configurations. In the event that the primary firewall fails, the secondary firewall is designed to begin regulating traffic in a stateful manner without interruption to the network services. NetSolve will maintain the software and configurations for the failover firewall in the same way as described for the MFW above. In the event of a failover, NetSolve will open a Trouble Ticket and notify the Customer.

#### **2.3.5. VPN Implementation**

NetSolve will perform the following VPN implementation services when purchased separately:

- Manage the installation and configuration of VPN IPsec services for the managed firewall.
  - VPN implementation will only be provided to or from devices that are managed under ProWatch Secure services or ProWatch for WANs services.
- Manage the installation and configuration of VPN IPsec services for each firewall.
- Manage the implementation and verify operation of IPsec encryption operation to all firewalls.
- Internet work verification of data transmission of the IPsec tunneling protocol (only done once).
- VPN implementation for routers is described in the **ProWatch for WANs – Service Description**.

#### **2.3.6. IOS Firewall Feature Set**

NetSolve will provide configuration support for Cisco's IOS based Firewall Feature Set when implemented in conjunction with NetSolve's ProWatch for WANs or Managed Internet Router Service.

The Cisco Firewall Feature Set provides firewall functionality for network perimeters using a Cisco router. For this offering, NetSolve will support a single "outside" (WAN) interface, and up to two "inside" (LAN) interfaces and will provide configuration and archiving services for the Firewall Feature Set. Configuration services will implement a security policy in accordance with the needs and environment of the customer. NetSolve will not perform monitoring of Firewall Feature Set or monitoring for security events generated by Firewall Feature Set. NetSolve will not log any events generated by Firewall Feature Set and will not provide any Customer Notification of events generated by Firewall Feature Set.

NetSolve will support up to 5 configuration change requests per month. The customer will be charged a \$25 configuration fee for all configuration changes after the 5<sup>th</sup> change in any given month. All configuration change requests are subject to the procedures and fees established in NetSolve's Moves, Adds, Changes document. NetSolve will archive the current configuration each time NetSolve makes a configuration change.

### **3. Customer Responsibilities**

Customer responsibilities are as follows in connection with NetSolve's ProWatch Secure service:

- Provide equipment (including related software).
- NetSolve recommends that the Customer purchase maintenance services for the managed devices. The Customer is responsible for hardware and software maintenance of the devices.
- Purchase from NetSolve secondary management channel equipment, typically a modem and appropriate cables, as defined by NetSolve.
- Provide a dedicated 1FB (analog) dial line for out-of-band management access to the equipment.
- Where applicable, provide the Internet access connection (Internet service must be arranged separately by Customer with the service provider of the Customer's choice).
- Maintain the Internet connection. The primary fault isolation services do not extend to maintenance of DNS server.
- Manage the host operating system on the device the HIDS agent is installed on.
- Be responsible for the timely delivery of information required for the configuration of the equipment to be managed including existing Internet security policy, alarm notification policies and procedures, network maps, existing equipment configurations, and inputs on configuring the sensitivity of the system in conformity with the Customer's security objectives.
- Designate a security contact(s) for NetSolve to communicate with regarding security and managed equipment issues. All communications between NetSolve and the Customer regarding security and equipment matters will be through this security contact. The Customer must provide NetSolve with escalation procedures in the event that the designated security contact is unavailable.
- Provide assistance to NetSolve to determine alarm notification policies and procedures.
- Provide all required LAN connections for the security equipment.
- Be responsible for establishing and maintaining physical security of the security equipment and the Customer's LAN/WAN.
- Notify NetSolve 72-hours in advance of any internal or external network hardware and software changes that may affect communications through the firewall or NIDS sensor.
- Be responsible for management of any server or application with which the firewall interacts, such as an authentication server, and administration of security profiles for individual users and groups.
- Agree and consent to the allowance to conduct non-destructive probes of the Customer's network to determine vulnerability state.
- Agree to preserve NetSolve's right to the statistics derived from historic security events and the right to publish these statistics after they have been sanitized of any references to Customer specific information.
- Be responsible for management of the perimeter router (unless the Customer has purchased MSR services from NetSolve above).

EXCLUSIVE WARRANTY AND EXCLUSIVE REMEDY BECAUSE OF THE CONTINUOUS EVOLUTION OF THE SOPHISTICATION OF "HACKERS", NETSOLVE DOES NOT, AND IT IS ACKNOWLEDGED THAT NETSOLVE CANNOT MAKE ANY WARRANTY OR REPRESENTATION THAT ANY SYSTEM ATTACK OR INTRUSION WILL BE DETECTED OR PREVENTED, NOR DOES NETSOLVE REPRESENT THAT ANY LICENSED ITEMS ARE ERROR FREE.

WITH RESPECT TO PRODUCTS PURCHASED FROM NETSOLVE, IF ANY, NETSOLVE'S EXCLUSIVE LIMITED WARRANTY IS THAT, FOR A PERIOD OF ONE YEAR FOLLOWING

DELIVERY, THE PRODUCTS, UNDER NORMAL USE AND SERVICE, WILL SUBSTANTIALLY PERFORM ALL OF THE FUNCTIONS DESCRIBED IN THE SPECIFICATIONS FOR THE PRODUCTS. IN THE EVENT NETSOLVE BREACHES THIS WARRANTY, CUSTOMER'S EXCLUSIVE REMEDY SHALL BE, AT NETSOLVE'S OPTION AND EXPENSE, (i) TO HAVE NETSOLVE CORRECT ANY DISCREPANCY IN PERFORMANCE THAT MATERIALLY IMPAIRS THE FUNCTIONALITY OF THE PRODUCTS, OR (ii) NETSOLVE SHALL REFUND THE PRICE PAID TO NETSOLVE FOR THE PRODUCTS.

CUSTOMER ASSUMES FULL RESPONSIBILITY FOR THE CONTROL AND USE OF THE DATA CONTAINED IN ANY REPORTS PROVIDED BY NETSOLVE HEREUNDER. CUSTOMER ACKNOWLEDGES THE POTENTIAL PRIVACY AND OTHER ISSUES ASSOCIATED WITH THE COLLECTION AND USE OF THIS DATA. NETSOLVE WILL NOT, UNDER ANY CIRCUMSTANCES, BE LIABLE TO ANY PARTY FOR ANY INDIRECT, CONSEQUENTIAL, INCIDENTAL, PUNITIVE OR OTHER SPECIAL TYPES OF DAMAGES, EVEN IF SUCH DAMAGES RESULT FROM THE BREACH OR OTHER FAULT OF NETSOLVE.

CUSTOMER ASSUMES FULL RESPONSIBILITY TO BACK-UP AND/OR OTHERWISE PROTECT ALL DATA AGAINST LOSS, DAMAGE, OR DESTRUCTION, EXCEPT FOR SECURITY CONFIGURATION DATA WHICH WILL BE BACKED-UP BY NETSOLVE.

WITH RESPECT TO SERVICES, NETSOLVE'S EXCLUSIVE WARRANTY IS THAT THE SERVICES SHALL BE PERFORMED IN A WORKMANLIKE FASHION. IN ANY MONTH IN WHICH CUSTOMER, IN CUSTOMER'S SOLE OPINION, BELIEVES NETSOLVE HAS BREACHED THIS WARRANTY, NETSOLVE WILL CREDIT CUSTOMER UP TO ONE-HUNDRED PERCENT (100%) OF THE SERVICE FEES FOR THAT MONTH FOR THE PROWATCH SECURE SERVICES. IN ORDER TO RECEIVE THIS CREDIT, CUSTOMER MUST NOTIFY NETSOLVE IN WRITING WITHIN THIRTY (30) DAYS FOLLOWING THE END OF THE MONTH THE SERVICES WERE PROVIDED STATING (i) THE REASON CUSTOMER IS DISSATISFIED WITH THE SERVICES AND (ii) THE AMOUNT OF THE SERVICE FEES CUSTOMER REQUESTS TO BE CREDITED. UPON RECEIPT OF SUCH NOTICE, NETSOLVE WILL CREDIT CUSTOMER THE REQUESTED AMOUNT (UP TO THE LIMITS ABOVE) ON THE NEXT BILLING CYCLE. THIS CREDIT WILL CONSTITUTE CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR BREACH OF WARRANTY. NETSOLVE SHALL NOT BE OBLIGATED TO CREDIT CUSTOMER AN AGGREGATE AMOUNT EXCEEDING TWO MONTH'S SERVICE FEES IN ANY TWELVE MONTH PERIOD, OR AN AGGREGATE AMOUNT EXCEEDING THREE MONTH'S SERVICE FEES IN ANY EIGHTEEN (18) MONTH PERIOD, BUT MAY ELECT TO DO SO BASED ON CUSTOMER'S REQUEST.

Software License. NetSolve grants Customer a non-exclusive, non-transferable license to use all software and firmware associated with the ProWatch Secure Intrusion Detection and Response services ("Software"), subject to the following conditions: (i) Customer may use Software only for its intended purposes, (ii) Customer may not copy, disclose, modify, decompile, disassemble, translate, or reverse engineer the Software; (iii) Customer shall honor all manufacturers' license requirements regarding Software, if any; and (iv) in the event of a default by Customer of the terms of the agreement between Customer and NetSolve or this Service Description, the Software License is immediately terminated and Customer will return all Software to NetSolve.

#### 4. Supported Equipment

The following is the list of devices supported by NetSolve's ProWatch Secure services:

Manufacturer	Manufacturer Model	Special Instructions
Firewalls	<b>4.1. <u>Cisco Secure PIX 501</u></b> <b>4.2. <u>Cisco Secure PIX 506</u></b> <b>4.3. <u>Cisco Secure PIX 515</u></b> <b>4.4. <u>Cisco Secure PIX 520</u></b> <b>4.5. <u>Cisco Secure PIX 525</u></b> <b>4.6. <u>Cisco Secure PIX 535</u></b>	<b>Software version 5.x.x or later, DES licenses</b>  <b>required</b>
	CheckPoint Firewall-1 on Nokia Appliance IP110, IP120, IP330, IP440, IP530, IP650, IP740  <b>Checkpoint Firewall-1 on Intrusion.com Appliance</b> PDS 2000 Series PDS 5000 Series  <b>Checkpoint Firewall-1 on SPARC Server</b>	<b>Solaris version 2.6 or later. CheckPoint Firewall-1 must be installed as "Distributed"</b>
Intrusion Detection Systems	<b>Cisco Secure IDS 4210</b> <b>Cisco Secure IDS 4230</b> <b>Cisco Secure IDS 4235</b> <b>Cisco Secure IDS 4250</b>	<b>Software version 2.5 or later</b> <b>IOS 12.x or later</b>
Managed Internet Routers	<b>Cisco 17xx, 2xxx, 3xxx, 4xxx, 7xxx series routers</b>	<b>IOS 12.x or later</b>