Managed Firewall and VPN Services

PRODUCT AND SERVICES

1.1 Firewall and Virtual Private Network Services ("Managed Security") provided hereunder are in addition to other communications facilities or services, whether provided by XO or another service provider. Nothing in this Exhibit shall enhance, change or alter any such services or the terms under which they may be provided pursuant to the Agreement, which will set forth the precise services ordered hereunder, and its associated Terms and Conditions as well as this Exhibit.

1.2 XO will provide security services ("Managed Security") to the Customer based on XO's Site Survey document ("Survey Document"). The Survey Document documents the Customer's Local Area Network ("LAN") configuration, applications and IP addressing schema. It serves as the specification document for the installation of Customer Premise Equipment ("CPE") to provide the XO managed security service(s). Customer completes the Survey Document, in conjunction with an assigned XO sales engineer or XO Technical Consultant via a Customer site visit or a conference call. If the information included in the Survey Document is incomplete or incorrect or is modified after it is completed with the XO sales engineer, installation of the Managed Security services may be delayed, and XO will not be liable for such delayed installation as a result thereof.

1.3 Customer acknowledges and agrees that XO's provision of Managed Security Services as it relates to the detection and monitoring of Customer's Premise Equipment is predicated on Customer's adherence to the network configuration diagram recommended to Customer, based on the above Survey Document and Customer's security parameters; any deviation from such network configuration diagram recommendations that XO implements at the request of Customer may adversely affect the Managed Security Service(s) provided herein.

1.4 Product Descriptions

A. Firewall Services: A firewall is a combination, in whole or in part, of hardware and software which is intended to limit the exposure of a computer or computer network against unauthorized access from outside by providing a single point of entry, and a passive defense system at that point of entry by providing controlled access. The XO Managed Firewall Services are designed to provide network and resources access control and manage the public access points to a computer network. Firewall technology in itself is not foolproof and no firewall technology provides an absolute deterrent or barrier to unauthorized entry.

All XO Managed Firewall Services includes the following:

- Pre-implementation network Site Survey to determine IP addressing supported applications and network configuration in general
- Ability to rent the Customer Premise Equipment ("CPE") over the life of the contract (Purchase available on select product lines).
- On site installation by trained XO field technicians or XO approved third party vendor.
- Configuration of the security policy based on results of the Site Survey.
- Post-installation site certification.
- Free ongoing security policy change.
- 24x365 support.
- Firewall policy configuration changes 8:00 am EST - 6:00 pm EST Monday - Friday

B. Virtual Private Network Services: Virtual Private Network ("VPN") Services create a private communications network running over a public (e.g., the Internet) or shared private network (e.g., XO), interconnecting physically diverse locations, remote users and other points of access. The XO VPN Service carves private tunnels through the public Internet via tunneling protocols and encryption technology, thereby securing transmitted data streams. Customer shall elect XO VPN Services in one of the following configurations:

i VPN with third party ISP service ("Internet access"): XO provides "VPN Only" service while Customer connects to the Internet via third party provided Internet access. Firewall Service is

optional and available as a built-in function of the Service or as a stand-alone, managed dedicated firewall service by XO

ii VPN with XO Internet access: Offering includes XO managed VPN Service with a choice of dedicated Internet access methods, i.e., Dedicated Internet Access ("DIA"), Integrated Access ("IA") or Digital Subscriber Line ("DSL"). Firewall Service is optional and available as a built-in function of the service or as a stand-alone, managed dedicated firewall service by XO.

iii Customers who do not have XO Managed Firewall Services with its VPN acknowledge and understand that World Wide Web ("www") access may result in unsecured access to the corporate Network.

iv Remote Access VPN access: This Service offers Customer the ability to connect remote users to connect to the corporate VPN Network. Remote Access VPN with XO Corporate Dial provides end-users with an XO provided corporate dial account to access the Internet as well as encryption software that provides for secure transmission of data between end-user and data termination point. Remote Access VPN is also available with Remote Access Client only in instances where Customer's end-users have existing dial Internet service with a third party ISP.

C. **Remote Access VPN Service**

i Remote Access VPN service enables Customer's mobile employees or remotely connected employees to securely connect to the corporate VPN network via a software client and RADIUS authentication to the VPN tunnel terminating device located on the customer premise.

ii Is a service whereby XO extends an online graphical user interface (GUI) to a designated Customer end user Administrator who maintains full management control over the remote VPN user base.

iii Any Local Area Network (LAN) applications or services adversely impacting or disrupting the remote access VPN service are out of XO's service scope and need to be addressed and resolved by the Customer.

iv Trouble shooting by XO pertains to trouble isolation up to and including the LAN port of the security device. It does not include trouble isolation relating to Customer Local Area Network, LAN applications, desk top Operating Systems (OS) or end-user software and application incompatibilities with XO's VPN service.

D. **Managed Security Services:** Managed Security Services is comprised of the following components:

- Configuration management of security devices , including hardware, software, rule base changes, and XO network address changes
- Response to requests for configuration changes within one (1) business day.
- Response to alarms generated by built in facilities of each platform in a timely manner.
- Response to trouble calls caused by XO facilities

XO only manages CPE that was provided by XO and its licensors, whether purchased or rented.

1.5 Customer acknowledges and agrees that XO Managed Security Services as it relates to the monitoring of Customer's network and management of CPE is predicated on Customer's adherence to the network configuration diagram recommended to Customer, based on the above Survey Document and Customer's security parameters, including Customer's obligation to provide any out-of-band management communication line to the CPE. Any deviation from such network configuration diagram recommendations that XO implements at the request of Customer may adversely affect the Managed Security Services provided herein. Access to CPE to make requested or required changes to the security parameters, will be executed and implemented by XO only. In addition, Customer acknowledges that management of the remote access VPN service and trouble shooting & resolution of remote access VPN users is the Customer's responsibility unless the trouble issue is caused by a XO provided facility.

2.0 CPE INSTALLATION AND CERTIFICATION

2.1 Installation. Installation encompasses the preparation of the CPE for shipping, the testing of the CPE for functioning and the actual installation of the CPE at the Customer site. During the installation process, CPE is configured according to the Survey Document as well as the Customer selected security policy for the firewall (if applicable) and in accordance with CPE manufacturers' specifications. XO will use reasonable commercial efforts to coordinate installation dates with Customer. XO will install the Managed Security services between the hours of 9:00 a.m. and 6:00 p.m. Eastern Time on normal business days. If Customer requests an installation outside of this normal installation window, Customer must provide XO with a minimum of two (2) weeks prior written notice. XO will then coordinate with Customer to determine the installation date and window. In the event that Customer requests an installation to be performed outside of the normal installation window set out above and Customer does not provide XO with the requisite two (2) weeks prior written notice, then, provided that XO can accommodate the request, XO will charge Customer an expedite fee in the amount of $500.00

2.2 Certification. Billing for each site will begin after the successful Certification of the Service for each specific site. Certification is considered complete once the CPE has been positively PINGed, end-to-end connections have been tested and verified operational, XO has established management and surveillance of the CPE and the remote access VPN RADIUS is able to authenticate the Customer designated Administrator remote access VPN user. Customer acknowledges that support for VPN Services are contingent upon Customer's participation in the testing and certification process. Billing commences on a per site basis and does not rely on additional sites Certification to begin.

2.3 Lead Times. . Lead times for connectivity may vary and are dependent on a number of factors, such as selected type of Internet service, Type II Local Loop delivery date and/or proximity to XO Network facilities.

3.0 TITLE, CONTROL, USE AND RISK OF LOSS OF CPE

3.1 Title. The Services and all such related materials are for Customer's legitimate business use only. This Section shall survive termination of the Agreement and this Exhibit.

3.1.1 ***Rented CPE.*** Title to and/or ownership of any CPE provided to Customer by XO and/or its licensors under a rental option shall remain with XO or such licensors as appropriate. Customer agrees not to tamper with, modify, make error corrections, or otherwise alter any CPE provided to Customer under a lease or rental option, nor permit third parties not authorized by XO or the CPE vendor to do the same. All such leased or rented CPE must be returned to XO upon termination of the Services for any reason. Customer must contact XO within thirty (30) days of such termination (unless contacted earlier by XO) to schedule pickup of CPE, or Customer shall be deemed to have purchased such CPE and shall be invoiced for the replacement cost of such CPE.

3.2 Control and Use of CPE.

3.2.1 Customer agrees that it shall be bound by any vendor specific license terms and conditions related to any CPE. Where required by a vendor(s), such license terms shall be attached hereto as License Attachments to this Exhibit (the "License Attachment(s)"), and made a part of the Agreement. Customer acknowledges receipt of any such applicable License Attachment(s) and its responsibility to comply with the terms of such License Attachment(s) and assume all liability for compliance with such terms, including but not limited to, (a) informing all Customer end-users of the terms of the License Attachment(s); (b) monitoring use of the CPE to ensure compliance with the terms thereof; and (c) maintaining the distribution and security of any user identification and/or passwords necessary to access any CPE. XO disclaims all liability to vendors for breaches of such License Attachment(s) by Customer.

3.2.2 To the extent not covered by any License Attachment(s), Customer agrees not to reverse engineer, de-compile, disassemble, translate, modify, alter or change the Services, the CPE, or any component of either, or otherwise obtain or attempt to obtain any technology (including encryption technology) or source code for any hardware or software that may be provided with the Services or CPE. Customer acknowledges that the hardware and software provided under this Exhibit or utilized with the Services provided under this

Exhibit may be subject to third party license terms, and/or U.S. export laws and regulations and that any transfer (whether directly or by products incorporating the technology) must be authorized under those laws and regulations. Customer agrees not to copy, sell, assign, transfer, sublicense, export or distribute any hardware, software, documentation or other materials that XO may provide related to the Services. Title to such software, and all related technical know-how and intellectual property rights therein are and shall remain the exclusive property of XO and/or its suppliers. Customer shall not take any action to jeopardize, limit or interfere in any manner with XO and its supplier's ownership of and rights with respect to any licensed software.

3.3 Risk of Loss of CPE. Risk of loss of CPE or damage to any CPE, provided to Customer on a rental basis as an integral part of Managed Security Services is assumed by Customer, except when such damage is caused solely by XO in the installation or maintenance of such CPE. XO retains title and all rights to such CPE.

4.0 ESCALATION PROCEDURES FOR MANAGED SECURITY SERVICES

4.1 XO Managed Security Escalation Procedures

When a Customer needs to escalate a security service incident, the following escalation procedures will be followed:

Customer contacts XO Customer Care to open a trouble ticket.

Customer Care confirms the Customer's identity as one of the authorized contacts as stated in on the Customer account

If the Customer is requesting a security configuration change and/or connectivity seems to be working properly, the caller's issue will be referred to the Security Help Desk for Level II support via a trouble ticket.

If the Security Help Desk needs more information or assistance, it may contact the appropriate vendor.

If connectivity is the problem, Customer Care will first follow the standard DIA/IA, DSL, or Dedicated Hosting repair process before escalating to the Security Help Desk otherwise the ticket will be submitted directly to the Security Help Desk.

- For Access Products connectivity issues, the repair team creates a trouble ticket to call telco carrier (LEC/IXC, leased line, and so on), then updates the Customer (when possible) with the details of their trouble ticket(s).
- Within thirty (30) minutes after situation assessment, XO will request the telco carrier to escalate internally to Manager or Duty Supervisor. If telco carrier has isolated the trouble and has ascertained Estimated Time of Repair (ETR) within two (2) hours, XO may halt escalation process at this time. If root cause is still undetected or if ETR is greater than two (2) hours, then escalation will proceed to next step.
- Within 1 hour, if root cause is not yet determined, the situation is escalated to Customer Care Team Leader, Network Operations Supervisor, or Manager on duty. The Network Operations Supervisor will escalate to the telco carrier's management, such as a Service Manager.

The Security Help Desk will resolve the situation, detailing cause, effect, and other pertinent work log information in the trouble ticket.

Once the situation is resolved, the Customer will be contacted.

4.2 Priority Levels. XO assigns priority levels to distinguish and prioritize service severity levels. The prioritization occurs as follows

If the XO NOC acts upon an alarm, initiates a maintenance service procedure, or Customer Care receives a call from a customer :

Assignment of Priority Levels

PRIORITY	DEFINITION
1	Service is down
2	Service is operating in a degraded mode and affects the Customer
3	All other tickets, such as when Service is operational but requires administrative work, or Customer inquiry.

Additionally, XO will update open trouble tickets priority levels in the following intervals:

Priority update intervals

PRIORITY LEVEL	UPDATE OF TROUBLE STATUS
1	every thirty (30) minutes
2	every two (2) hours
3	every business day or at the time defined for action

Escalation Levels and Intervals

For all problems that are not resolved within the intervals allotted for each service type, the chart below identifies the order and intervals for internal management notification.

Severity Level	Team Leader	Manager	Director	Vice President
Priority 1	1 Hour	2 Hours	4 Hours	8 Hours
Priority 2	2 Hours	4 Hours	8 Hours	12 Hours

Status on every ticket - call within the first hour
P1 - call first hour, then as necessary or every 2 hours after that
P2 - call first hour, then as necessary or every 4 hours after that
P3 - call first hour, then as necessary or every 24 hours after that or upon resolution

Escalating tickets
P1 - can start escalating after 1 hour of ticket being opened, and every hour on the hour after that or as needed
P2 - can start escalating after 4 hours of ticket being opened, and every hour on the hour after that or as needed

P3 - can start escalating after 8 hours of ticket being opened, and every hour on the hour after that or as needed

5.0 FEES AND BILLING

Pricing for Services provided pursuant to this Exhibit shall be in accordance with the Customer Quote provided by XO, which shall be provided with and made part of this Exhibit. All Flat Rated Monthly Recurring Charges ("MRC") invoices shall be billed one (1) month in advance. Pricing discounts may be associated with the level of term commitment the Customer selects. Billing shall commence upon the earlier of: (a) the Service Commencement Date (as defined Section 10.1 below); or (b) fifteen (15) business days after XO notifies Customer of a firm date for installation of any required CPE and provisioning of the Services. Additionally, if Customer fails to allow or accept installation when an XO technician arrives as scheduled to install Services, Customer may be charged the standard, non-recurring installation charge for the Service.

6.0 MONTHLY REPORTING

6.1 Managed Security Reporting. XO monitors the CPE and manages the XO VPN Service and provides the following online reporting to Customers for the Cisco based service:

6.1.1 ***Bandwidth Usage Reporting.*** XO Dedicated Internet access (DIA) Service provides a graphical view/image of average utilized bandwidth per Access Circuit provided by XO called XOStats which is available online.

7.0 DEMARC

7.1 Customer agrees that the demarcation point, i.e., the physical interface point between the Customer Local Area Network ("LAN") and the Service Provider Wide Area Network ("WAN"), is the point which separates the Customer LAN and the Service Provider WAN. Typical demarcation points are considered to be RJ-x, Ethernet hand-off interfaces or Telco Smartjack.

7.2 XO is responsible for managing and troubleshooting up to the demarcation point that separates the Customer's LAN and the XO managed service point including the CPE. Any issues beyond the demarcation point, LAN-facing and relating to or originating from the Customer LAN and having an impact on the XO Managed Security Service is the responsibility of the Customer.

7.3 XO shall not, in any way, be responsible for the configuration, installation, management, maintenance, troubleshooting or support of Customer owned or managed servers, applications, Operating Systems, workstations or Network devices residing on the Customer's LAN.

8.0 RESPONSIBILITIES

8.1 XO is responsible for:

- Initial consultation for Network design, including:
  - Network assessment via Site Survey document and all its associated network information;
  - Topology review;
  - Network feasibility & network design; and
  - Recommendation of CPE including routers, VPN gateways and firewalls.
- Ordering of local loops where applicable & working with other telecommunications carriers to obtain Type II local loops where required.
- Ordering of CPE.
- Preparation of CPE for Network implementation.
- Shipping CPE to local XO field office for installation or directly to Customer location, as required.
- Onsite installation of CPE.
- Test, Turn-Up & Certification of all Network sites.

- Troubleshooting and resolving issues pertaining to the Managed Security Device, up to and including the LAN Ethernet port
- Troubleshooting and resolving issues pertaining to the WAN connectivity
- If there appears to be an issue with the Managed Security features, XO will
    - Ensure that the Managed Security Device is up and operational
    - Ensure that any VPN tunnels are up and operational
    - Ensure that traffic is passing through the Managed Security Device
    - Ensure that network address translation (NAT), if provisioned, is functioning correctly
    - Ensure that firewall filtering policies, if provisioned, are functioning
    - Ensure that DHCP, if provisioned, is functioning
    - Ensure that VPN Client remote access, if provisioned, is functioning
    - Ensure the latency is within specified boundaries set forth by the XO DIA Service Level Agreement
- At Customer's request, XO may assist in troubleshooting beyond the LAN port and VPN configuration, with the following guidelines:
    - XO is limited to troubleshooting only from the Managed Security device (router or firewall)
    - XO will not be responsible for repairing any device or application other than the XO-owned and Managed Security devices. If Customer has another XO managed service, the troubleshooting and repair of that service will fall under the Terms and Conditions governing such other managed service
        - For example, if it is determined that an FTP server has a virus, Customer will be responsible for removing the virus from that server
    - If Customer requests the troubleshooting services set forth above, and XO has agreed to provide such services, XO will charge Customer in four (4) hour increments at a rate of $500.00 per four (4) hour increment
        - For example, if Customer requests that XO assist them in troubleshooting their email application and it takes XO three (3) hours to pinpoint the application issue, Customer will be charged a fee of $500.00. If it takes XO five (5) hours, Customer will be charged a fee of $1,000.00.
    - Notwithstanding the foregoing, if, after the issue has been resolved, it is determined that the issue was due to XO (e.g., configuration, CPE or WAN issue), Customer will not be charged for the troubleshooting service.
    - XO reserves the right not to offer this type of troubleshooting service, or to cease providing such service, to any customer for any reason
- If a machine on Customer's LAN is infected with a virus or worm, XO will cooperate with Customer to close the affected port on the Firewall. As outlined above, Customer may request XO to help identify the infected machine(s), but XO will in no way be responsible for removing the virus or worm from the infected machine(s) or patching those machine(s).
- Being responsible for latency across the VPN (from XO PoP to XO PoP, as outlined in the XO DIA Terms and Conditions), provided that both ends of the VPN utilize XO Dedicated Internet Access
- Acting as Level 2 support for VPN Remote Access Customer Administrator - XO will only open trouble tickets for the Customer Administrator
- Configuration Change Management of VPN and Firewall devices.
- 24x365 Network monitoring of access Circuits and CPE
- Respond to all Move-Add-Change requests, some of which may require a new installation of Service.
- Scheduled maintenance of software & hardware
- Trouble ticket management, including: logging and tracking & escalation of Customer reported Service troubles.
- Service management, including: management of CPE management devices , RADIUS servers, and software, patches & maintenance of the XO network.
- Escalation process management: XO ensures to keep required escalation paths maintained and in synch with existing business processes.

Section 8.2 XO is NOT responsible for:

- Ensuring that Customer's applications are performing properly across the VPN
- Latency across the VPN if either end of the VPN does not utilize XO Dedicated Internet Access

- Resolving incompatibilities between Customer workstations and the Cisco VPN software
- Being in any way responsible for the applications within the Customer's LAN or traversing the VPN.
- Opening trouble tickets for remote access end users.

8.3 Customer is responsible for:

- Designating a technical point of contact to work with XO to lend support for a successful implementation.
- Providing XO with all required Network information to successfully complete the Site Survey as a basis for the Service implementation.
- Enabling XO field personnel or XO designated party to access the premise(s) as required for Site Survey or CPE installation & trouble shooting.
- Cooperate in scheduling installations as required by XO field personnel.
- Providing XO with a complete list of LAN applications.
- All server configurations.
- Directing the XO engineers to open necessary ports according to how their servers are configured.
- Providing LANs that use the TCP/IP protocols required for connectivity to the XO network.
- Configuring, cabling, installation and support of Customer LAN and providing necessary application software for such applications
- Application support for Customer LAN and all its servers and LAN hosts.
- IT support and troubleshooting on Customer owned servers, workstations and Network devices.
- Configuration, management, maintenance, and support of any equipment not expressly provided by XO for use with the XO Managed Security.
- Designating an Administrator support contact for all remote access VPN end users and providing support to remote access VPN end users - XO will not open trouble tickets for end-users that utilize the remote access VPN
- Reviewing the FAQ on the Cisco remote access client at: http://www.cisco.com/warp/public/471/vpnclientfaq.pdf
- The performance of its applications across the network
- Providing and maintaining inside wiring facilities to extend the leased line circuit from the DEMARC point of entrance to the location where the CPE is to be installed.
- Configuration Change Management: Customer will need to open a trouble ticket with XO Customer Care and provide all required configuration change information for assessment and impact onto the Customer Network. After evaluating, XO will provide recommendations, and if deemed feasible, XO will implement such changes. Furthermore, Customer needs to notify XO of any configuration changes on the Customer LAN Network. Such configuration changes may have negative impact on provided XO Services and require evaluation before Customer implements such changes.
- Customer is required to provide an Out of Band ("OOB") dedicated POTS line and ongoing maintenance when using third party ISP services to connect to the Internet as well as keeping the OOB line operational for trouble shooting by XO managed security personnel.

8.3 Network trouble-shooting responsibilities:

- For Customers utilizing XO CPE on a Rent or Purchase Basis (Purchase applicable to XO DIA service only): The Customer is responsible for addressing and resolving any Network troubles residing on the LAN Network side of the demarcation point including the Customer managed CPE. Any Network troubles residing on the WAN side of the demarcation point, i.e., the Wide Area Network or Service Provider Network, are the responsibility of the Service Provider.

9.0 CUSTOMER'S REPRESENTATIONS & WARRANTIES

9.1 Customer agrees, represents and warrants that:

(a) It has full power and authority (including full corporate power and authority) to execute and deliver this Exhibit and to perform its obligations hereunder; and

(b) It has carefully reviewed the Agreement, and that its use of the Service rendered hereunder shall be designed, installed, furnished and in all respects provided and maintained in conformance and compliance with applicable federal, state and local laws, administrative and regulatory requirements and any other authorities having jurisdiction over the subject matter of this Agreement and it shall be responsible for applying for, obtaining and maintaining all registrations and certifications which may be required by such authorities.

9.2 Customer understands that, should it request or make any changes to its Firewall or VPN equipment or Services, that such changes may result in a lower level of security and may allow unsecured access to its Network. In the event of any such change, Customer acknowledges and agrees that it shall assume all risks and liabilities associated with or resulting from any such changes.

10.0 TERM AND TERMINATION

10.1 Service Commencement Date. XO will notify Customer that the Managed Security Services are installed or connected, successfully tested and available for Customer use, and if XO is installing any CPE, the CPE has been installed and certified (the "Service Commencement Date"). Customer agrees to cooperate with XO to accomplish Firewall and VPN Service activation by providing access to Customer's premises and facilitating testing and Firewall and VPN Service delivery requirements. XO shall not be liable for any damages whatsoever resulting from delays in meeting requested or specified service dates, or inability to provide Managed Security which are beyond Service Provider's control.

10.2 Term. The term shall be indicated on the Service Order, Managed Security Services are available in one (1) year, two (2) year and three (3) year term commitment options beginning on the Service Commencement Date. Unless XO has already provided notice of its intent to terminate this Agreement, XO will notify Customer, in writing, at least sixty (60) days prior to the expiration of the Term, regarding the pending expiration of this Managed Security Service and the automatic month-to-month renewal of the Agreement if no action is taken prior to expiration. If you notify XO of your decision to cancel this Agreement within the notice period provided, actual termination of the Managed Security Service may not occur until thirty (30) days after receipt of your notification.

10.3 Termination and Cancellation Charges. If Customer defaults in fulfilling any material obligation of the Agreement or this Exhibit, XO shall have the right to terminate the Agreement or this Exhibit and the Customer shall pay XO, in addition to any other amounts then owing under the Agreement, a cancellation charge, including all nonrecurring charges, equal to seventy-five percent (75%) of all recurring charges for the remainder of the service contract term. These charges are intended to establish liquidated damages in the event of early termination, are not intended as a penalty and are, therefore, understood by Customer to be reflected in the price of the Services hereunder.

11.0 SERVICE LEVEL AGREEMENTS ("SLA") AND ASSOCIATED CREDITS

XO VPN bundles which incorporate XO Dedicated Internet Access ("DIA") adhere to XO DIA Service Level Agreements and Credit policies as set forth at www.xo.com/legal. The terms and conditions of the SLAs, which may be updated from time to time, are hereby incorporated by reference and made a part of this Agreement. The Customer agrees to check back to the SLA website periodically to review any changes to the SLA.

12.0 DISCLAIMER AND LIMITATION OF LIABILITY

12.1 CUSTOMER ACKNOWLEDGES THAT DATA TRANSMISSION SECURITY SERVICES SUCH AS THOSE PROVIDED UNDER THIS EXHIBIT ARE NOT FOOLPROOF AND, THEREFORE, ARE NOT GUARANTEED. IN ADDITION TO THE DISCLAIMERS AND LIMITATIONS SET FORTH IN THE AGREEMENT, NEITHER XO NOR ITS SUPPLIERS WILL BE LIABLE FOR ANY DAMAGES (INCLUDING, WITHOUT LIMITATION, ANY LOSS OR DAMAGE TO DATA) RELATING TO OR ARISING FROM THE USE OF THE SERVICES PROVIDED HEREUNDER (THIS EXCLUSION DOES NOT APPLY TO ANY

SERVICE WARRANTIES OR SERVICE LEVEL AGREEMENTS FOR ANY COMMUNICATION SERVICES PROVIDED BY XO UNDER THE AGREEMENT).

12.2 CUSTOMER UNDERSTANDS AND AGREES THAT XO IS PROVIDING SERVICES, AND ANY RELATED HARDWARE, SOFTWARE AND DOCUMENTATION TO CUSTOMER AND CUSTOMER HEREBY WAIVES ANY LIABILITY AGAINST XO AND AGREES TO HOLD XO HARMLESS FROM ANY AND ALL LIABILITY ARISING FROM LOSS OR DAMAGE DUE TO DELAY OF SERVICE COMMENCEMENT OR INABILITY TO PROVIDE THE SERVICE, FAILURE OF ALL OR PART OF THE SERVICE, INCLUDING ANY BETA SERVICE, OR ANY RELATED SERVICE PROVIDED HEREUNDER.

12.3 XO PROVIDES, AND CUSTOMER HEREBY ACCEPTS, ANY XO OR THIRD PARTY HARDWARE OR SOFTWARE PROVIDED TO OR USED BY CUSTOMER IN CONNECTION WITH THE SERVICES "AS IS" WITH NO EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF ANY KIND, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE. NOTHING HEREIN SHALL BE INTERPRETED TO ENHANCE OR CREATE ANY WARRANTY WITH RESPECT TO ANY THIRD PARTY SOFTWARE. XO DISCLAIMS ANY AND ALL LIABILITY ARISING OUT OF THE DELIVERY, INSTALLATION, SUPPORT OR USE OF ANY SOFTWARE. XO ASSUMES NO OBLIGATION TO CORRECT ERRORS IN ANY SOFTWARE. CUSTOMER UNDERSTANDS AND ACCEPTS ALL RESPONSIBILITY FOR ANY SOFTWARE MEETING CUSTOMER'S REQUIREMENTS OR EXPECTATIONS.

12.4 NEITHER XO NOR ANY OTHER PARTY MAKES ANY WARRANTIES EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. XO'S LIABILITY IN CONNECTION WITH THIS AGREEMENT, WHETHER IN CONTRACT, TORT OR OTHERWISE, SHALL NOT EXCEED THE AGGREGATE FEES, IF ANY, PAID BY CUSTOMER TO XO UNDER THIS AGREEMENT. IN NO EVENT SHALL XO OR ANY OF ITS LICENSORS BE LIABLE FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OF ANY KIND. THIS PROVISION LIMITING DAMAGES IS IN ADDITION TO ANY DISCLAIMERS AND LIMITATIONS ON LIABILITY IN THE AGREEMENT.

EXHIBIT S
END USER LICENSE AND SOFTWARE WARRANTY

PLEASE READ THIS SOFTWARE LICENSE CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE.

BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS LICENSE. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE, THEN (A) DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND, OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL PURCHASER.

The following terms govern your use of the Software except to the extent a particular program (a) is the subject of a separate written agreement with Cisco or (b) includes a separate "click-on" license agreement as part of the installation and/or download process. To the extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be (1) the written agreement, (2) the click-on agreement, and (3) this Software License.

License. Subject to the terms and conditions of and except as otherwise provided in this Agreement, Cisco Systems, Inc. or the Cisco Systems, Inc. subsidiary licensing the Software, if sale is not directly by Cisco Systems, Inc. ("Cisco"), and its suppliers grant to Customer ("Customer") a nonexclusive and nontransferable license to use the specific Cisco program modules, feature set(s) or feature(s) for which Customer has paid the required license fees (the "Software"), in object code form only. In addition, the foregoing license shall also be subject to the following limitations, as applicable:

- Unless otherwise expressly provided in the documentation, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable documentation permits installation on non-Cisco equipment) for communication with Cisco equipment owned or leased by Customer;
- Customer's use of the Software shall be limited to use on a single hardware chassis, on a single central processing unit, as applicable, or use on such greater number of chassises or central processing units as Customer may have paid Cisco the required license fee; and
- Customer's use of the Software shall also be limited, as applicable and set forth in Customer's purchase order or in Cisco's product catalog, user documentation, or web site, to a maximum number of (a) seats (i.e. users with access to the installed Software), (b) concurrent users, sessions, ports, and/or issued and outstanding IP addresses, and/or (c) central processing unit cycles or instructions per second. Customer's use of the Software shall also be limited by any other restrictions set forth in Customer's purchase order or in Cisco's product catalog, user documentation or web site for the Software.

NOTE: For evaluation or beta copies for which Cisco does not charge a license fee, the above requirement to pay a license fee does not apply.

General Limitations. Except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:

(i) transfer, assign or sublicense its license rights to any other person, or use the Software on unauthorized or secondhand Cisco equipment, and any such attempted transfer, assignment or sublicense shall be void;

(ii) make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or to permit third parties to do the same; or

(iii) decompile, decrypt, reverse engineer, disassemble or otherwise reduce the Software to human-readable form to gain access to trade secrets or confidential information in the Software.

To the extent required by law, at Customer's request, Cisco shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of Cisco's applicable fee. Customer shall observe strict obligations of confidentiality with respect to such information.

Upgrades and Additional Copies. For purposes of this Agreement, "Software" shall include (and the terms and conditions of this Agreement shall apply to) any upgrades, updates, bug fixes or modified versions (collectively, "Upgrades") or backup copies of the Software licensed or provided to Customer by Cisco or an authorized distributor for which Customer has paid the applicable license fees. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY SUCH ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL S OFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE; (2) USE OF UPGRADES IS LIMITED TO CISCO EQUIPMENT FOR WHICH CUSTOMER IS

THE ORIGINAL END USER PURCHASER OR LESSEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) USE OF ADDITIONAL COPIES IS LIMITED TO BACKUP PURPOSES ONLY.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in this Agreement, Customer shall not make any copies or duplicates or any Software without the prior written permission of Cisco. Customer may make such backup copies of the Software as may be necessary for Customer's lawful use, provided Customer affixes to such copies all copyright, confidentiality, and proprietary notices that appear on the original.

Protection of Information. Customer agrees that aspects of the Software and associated documentation, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of Cisco. Customer shall not disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior written consent of Cisco. Customer shall implement reasonable security measures to protect such trade secrets and copyrighted material. Title to Software and documentation shall remain solely with Cisco.

Term and Termination. This License is effective until terminated. Customer may terminate this License at any time by destroying all copies of Software including any documentation. Customer's rights under this License will terminate immediately without notice from Cisco if Customer fails to comply with any provision of this License. Upon termination, Customer must destroy all copies of Software in its possession or control.

Customer Records. Customer grants to Cisco and its independent accountants the right to examine Customer's books, records and accounts during Customer's normal business hours to verify compliance with this Agreement. In the event such audit discloses non-compliance with this Agreement, Customer shall promptly pay to Cisco the appropriate licensee fees.

Export. Software, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software.

U.S. Government End Users. The Software and associated software documentation qualify as "commercial items," as that term is defined at 48 C.F.R. 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in 48 C.F.R. 12.212. Consistent with 48 C.F.R.12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4, Licensee will provide to Government end user, or, if this Agreement is direct Government end user will acquire, the Software and software documentation with only those rights set forth herein that apply to non-governmental customers. Use of this Software and software documentation constitutes agreement by the government entity that the computer software and computer software documentation is commercial, and constitutes acceptance of the rights and restrictions herein.

Limited Warranty. Cisco Systems, Inc. or the Cisco Systems, Inc. subsidiary licensing the Software, if sale is not directly by Cisco Systems, Inc. ("Cisco") warrants that commencing from the date of delivery to Customer (but in case of resale by a Cisco reseller, commencing not more than ninety (90) days after original shipment by Cisco), and continuing for a period of the longer of (a) ninety (90) days or (b) the period set forth in the Warranty Card accompanying the Product (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (b) the Software substantially conforms to its published specifications. The date of shipment of a Product by Cisco is set forth on the packaging material in which the Product is shipped. Except for the foregoing, the Software is provided AS IS. This limited warranty extends only to the Customer who is the original licensee. Customer's sole and exclusive remedy and the entire liability of Cisco and its suppliers under this limited warranty will be, at Cisco or its service center's option, repair, replacement, or refund of the Software if reported (or, upon request, returned) to the party supplying the Software to Customer, if different than Cisco. In no event does Cisco warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Cisco does not warrant that the Software or any equipment, system or network on which the Software is used will be free of vulnerability to intrusion or attack.

Restrictions. This warranty does not apply if the Product (a) has been altered, except by Cisco, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Cisco, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; or (d) is licensed, for beta, evaluation, testing or demonstration purposes for which Cisco does not receive a payment of purchase price or license fee.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT

ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS, WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

General Terms Applicable to the Limited Warranty Statement and Software License Disclaimer of Liabilities. IN NO EVENT WILL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Cisco's or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

The Warranty and the Software License shall be governed by and construed in accordance with the laws of the State of California, without reference to principles of conflict of laws, provided that for Customers located in a member state of the European Union, Norway or Switzerland, English law shall apply. The United Nations Convention on the International Sale of Goods shall not apply. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Warranty and the Software License shall remain in full force and effect. Except as expressly provided herein, the Software License constitutes the entire agreement between the parties with respect to the license of the Software and supersedes any conflicting or additional terms contained in the purchase order

If Customer has entered into a contract directly with Cisco for supply of the Products subject to this warranty, the terms of that contract shall supersede any terms of this Warranty or the Warranty Card, or the Software License, which are inconsistent with that contract. Customer acknowledges that: the Internet URL address and the web pages referred to in this document may be updated by Cisco from time to time; the version in effect at the date of