# Securing a Network to Prevent Call Fraud

AccessLine SIP Trunking service uses the public Internet to connect the AccessLine Network to your customers PBX. This can create opportunities for fraud THAT CAN BE PREVENTED. Internet criminals can scan the public internet for applications that make phone calls. Once they detect these applications they then attempt to crack the authentication credentials. Once they have pirated the device or authentication credentials they have the ability to make phone calls, which the customer will be charged for.

## AccessLine Requirement: How to Protect the Phone System

SIP-based VOIP enabled PBX or SIP phones connected to AccessLine’s Service via our SIP trunking service MUST be installed in a secure **trusted** zone behind a Firewall and not exposed to the public internet. This means the PBX or SIP phones should never be put into a router's DMZ. The firewall must block all inbound internet traffic to the PBX or SIP phones. You do not have to block outbound traffic from your private network to the internet, but Network-Address-Translation, or “NAT” must be enabled. NAT allows the AccessLine Service to send calls to the PBX or SIP Phones. If the firewall has multiple NAT settings, you must select the NAT setting that “Address Restricted” and not “Endpoint Independent”. If you do want to limit outbound internet traffic on the firewall, then you need to open SIP related ports on the firewall to allow AccessLine’s Service to function properly. (See Appendix – SIP Firewall Ports)



## Obligations: T&Cs

The SIP Trunking Terms and Conditions states the following:

Customer understands that the use of the Services requires a network firewall at the Customer premises. Customers must deploy firewalls designed to enhance security for SIP-based VoIP applications and services. Any fraudulent use of Customer's Services due to a lack of acceptable firewall security is solely the responsibility of Customer, and AccessLine will not credit customer for these charges. Customer hereby indemnifies AccessLine against any responsibility for damages, consequential or otherwise that arise from an unprotected network. Customer also acknowledges that AccessLine may block without notice traffic reported by its carriers as potentially fraudulent.

## International Calling Must Be Requested on the Order Form

To further protect your customer, when you order services you have the option to enable or disable international and high cost areas (see appendix of high cost areas). If a customer does opt to disable international calling, this feature can be enabled at a later time.

## AccessLine Fraud Monitoring

The AccessLine NOC monitors call patterns to international (and high cost) locations on an hourly basis. If any customer exceeds the call thresholds for any international areas, AccessLine will disable international calling, and send an email notification to customer informing them that international calling has been disabled based on possible fraudulent activity. To protect the customer, we will not enable International calling until the account holder has given AccessLine authorization.

In addition, AccessLine scans the network of connected devices to determine if any of our SIP endpoints are open to the public internet. If an endpoint (phone, phone system or gateway) is determined to be open to the public Internet, a notification will be sent to the customer and CIP informing them they are not in compliance with AccessLine’s T&C’s and are required to secure the SIP endpoints behind a firewall.

# Appendix –North American High Cost Areas

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NPA** | **Country** |  |   |   |
| 684 | American Samoa |   | 671 | Guam |
| 264 | Anguilla |   | 876 | Jamaica |
| 268 | Antigua and Barbuda |   | 664 | Montserrat |
| 242 | Bahamas |   | 787 | Puerto Rico |
| 246 | Barbados |   | 939 | Puerto Rico |
| 441 | Bermuda |   | 670 | Saipan |
| 284 | British Virgin Island |   | 721 | Saint Maarten |
| 345 | Cayman Islands |   | 869 | ST. Kitts/Nevis |
| 767 | Dominica |   | 758 | ST. Lucia |
| 809 | Dominican Republic |   | 784 | St. Vincent |
| 829 | Dominican Republic |   | 868 | Trinidad and Tobago- |
| 849 | Dominican Republic |   | 649 | Turks & Caicos Island |
| 473 | Grenada |   | 340 | U.S. Virgin Islands |

# Appendix – SIP Firewall Ports

Protocol Port(s) Protocol Port(s)
UDP 5060 UDP 30000 - 50000
UDP 6060 TCP 6061