



FACTSHEET

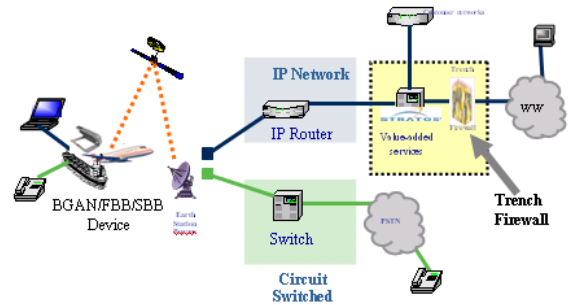
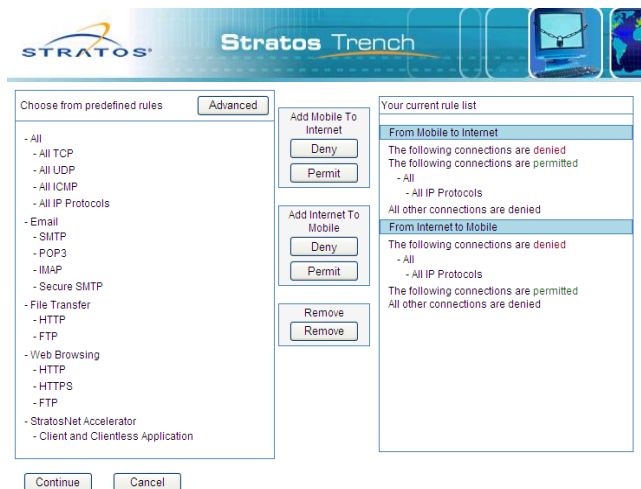
Revised: 18-Sep-09

Stratos Trench™

Customer Managed Firewall Protection for BGAN, FleetBroadband and SwiftBroadband

When accessing the Internet with BGAN, FleetBroadband or SwiftBroadband it is essential that you protect yourself against malicious Internet users. Integrated with the Stratos BGAN Infrastructure, Stratos Trench provides this security plus cost control by blocking specific traffic or applications. Accessed through the on-line interface of Stratos Dashboard, it is easy to set-up and manage your firewall protection.

network and the Internet. It allows BGAN, FleetBroadband and SwiftBroadband terminals to access the Internet while at the same time ensuring that incoming malicious traffic is blocked. Since Internet traffic is blocked *before* it goes over the satellite path you will not be charged for it – charges are levied only for IP traffic that passes over the satellite link in both directions. Using only the firewall on your computer blocks traffic after it has hit your bill, therefore Stratos Trench brings you additional cost savings.



Empower Your Network

To ensure Stratos users get the most out of BGAN, FleetBroadband and SwiftBroadband, we have developed services to increase security, save money, maintain control and offer higher flexibility in the way you access your satellite services. [NOTE: used "satellite" service here in order to avoid over-use of "BGAN, FBB and SBB"] This is done in our Value Added Infrastructure, located in close proximity to the Inmarsat BGAN Satellite Access Station (SAS). The infrastructure is situated between the BGAN IP network and the Internet, and can connect with your corporate network if required.

Protection Against Internet Threats

The Stratos Trench firewall sits between the satellite

Company Policy Enforcement

Corporate policies may place restrictions on satellite terminal use for security or cost control reasons. Stratos Trench ensures that these policies are *enforced*. A corporate administrator can implement firewall rules across all employees, while at the same time preventing employees from modifying these rules.

Read Only Role and Edit Role

If the corporate administrator has not selected the option 'updates by end-user allowed' then the end user gets the 'Read Only' role. This means he can access Stratos Trench and view his rules and traffic information, but he cannot make changes.

Stratos Trench and IP Access Options

The level of protection achieved depends upon the type of IP Access selected. When using a Public IP address (**TransparentAccess** or **NATtedAccess**), the satellite terminal is visible on the Internet.



BEYOND THE HORIZON®

Stratos Trench default is to block any unsolicited traffic from the Internet to this terminal. If this protection is too strict, the user can define his own Trench Rule Set to allow specific traffic from the Internet to the terminal. [NOTE: incorporated the last 2 sentences into the "Configure the Trench Rule Set section]

When using a private IP address (**RegularAccess**) the satellite terminal is not visible from outside the network. The private address is dynamically allocated to the terminal each time it logs onto the network with Stratos Trench taking care of the necessary address translation. This mechanism ensures that the terminal cannot be reached from the Internet by unsolicited traffic.

Terminals using **BusinessAccess** are effectively part of the customer's network, so protection from the Internet is handled within the customer's network according to their security policy. The Stratos Trench firewall is therefore not part of BusinessAccess though Trench CDRs are available.

The Stratos Trench User Interface

Via the easy to use, on-line interface, you can:

- Configure firewall rules
- View current and historical traffic

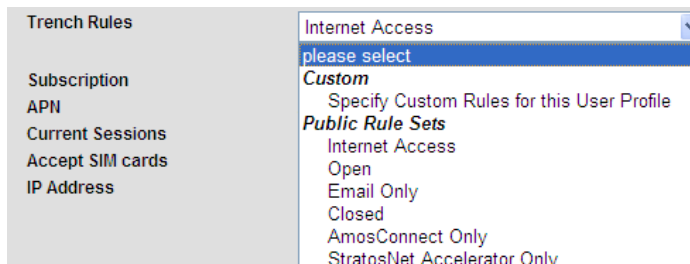
Configure the Trench Rule Set

It is easy to specify what traffic is allowed from the User terminal. For example:

- Permit only email and block Web browsing
- Permit only Web browsing to the corporate website
- Permit only AmosConnect traffic

There are 3 ways to specify or select Firewall rules:

1. **Public Rule Sets:** These are created by Stratos and can be chosen for all SIM cards. For example Internet Access or Email only
2. **Private Rule Sets:** These are created by the customer giving complete control over the IP Address, Protocol, Port and Subnet values when applying a rule to a configuration and can be set on all the User Profiles that belong to the same customer. You set this up and then simply use this rule set on any SIM card.
3. **Custom Rules:** These are individual rules which are created by the customer, they apply only to one User Profile.



Status: Viewing Current and Historical Activities

The Status option of Stratos Trench provides detailed information on the data sessions that are in progress as well as historical sessions. The information provided is specific to the Stratos Network and Value Added Services. This information is not available in the general Inmarsat BGAN LaunchPad, therefore providing additional detailed troubleshooting support.

Trench Current Activity Report

Session Status	Start	Sample	Access Type	IP Address
Active	15 Sep 2009 18:47:33	18 Sep 2009 13:20:49	Transparent Access	212.165.66.
Active	17 Sep 2009 07:20:36	18 Sep 2009 13:20:40	Transparent Access	212.165.69.

Trench Historic Activity Report

Start	End	Terminate Cause	Access Type	IP Address
18 Sep 2009 04:12:14	18 Sep 2009 04:13:50	User Request	Transparent Access	216.86.250.
18 Sep 2009 04:06:56	18 Sep 2009 06:06:33	User Request	Regular Access	10.166.104.

Access to Stratos Trench

Users can view and modify (if allowed) the Stratos Trench firewall rules from their BGAN terminal, Stratos Dashboard or the Internet using a browser. Stratos provides login name and password upon registration.

About Stratos

Stratos is the world's trusted leader for vital communications. With more than a century of service, Stratos offers the most powerful and extensive portfolio of remote communications solutions including mobile and fixed satellite and microwave services. More than 20,000 customers use Stratos products and industry-leading value-added services to optimize communications performance. Stratos serves U.S. and international government, military, first responder, NGO, oil and gas, industrial, maritime, aeronautical, enterprise, and media users on seven continents and across the world's oceans. For more information visit www.stratosglobal.com.

For more information please contact Stratos:

Toll Free (N. America): 1 800 563 2255
 Worldwide: +1 709 748 4226
 TTY: +1 709 748 4884
 Fax (Worldwide): +1 709 748 4320
 E-mail: info@stratosglobal.com
 Web Site: www.stratosglobal.com

