Remote Access Security for ftServer Systems

An overview of Stratus ActiveService Network security features and controls

by Stratus Technologies
June 7, 2011
## Table of Contents

1. **Introduction** ............................................................................................................. 2
2. **ActiveService Network (ASN)** ................................................................................ 3
   2.1 Overview .................................................................................................................. 3
   2.2 ActiveService™ Network Features ......................................................................... 3
   2.3 ActiveService Manager ........................................................................................... 3
   2.4 Out of Band Management ....................................................................................... 3
   2.5 Basic Call Home Support ....................................................................................... 5
   2.6 Interactive Connection Support .............................................................................. 5
   2.7 How the ASN Works ............................................................................................... 6
   2.8 Security ................................................................................................................... 7
   2.9 Network and Data Security ..................................................................................... 7
   2.10 Description of built-in security controls .................................................................. 9
   2.11 Additional Optional Security Controls .................................................................. 11
3. **Internet Connections** ............................................................................................... 12
   3.1 Internet Call Home .................................................................................................. 12
   3.2 ASN Internet dial-in ............................................................................................... 12
   3.3 WebEX Support .................................................................................................... 13
     3.3.1 ASN/Web (WebEx) Security ............................................................................. 13
     3.3.2 How the ASN/Web works .............................................................................. 13
4. **Services and Drivers** .............................................................................................. 14
   4.1 Services .................................................................................................................... 14
   4.2 Drivers ...................................................................................................................... 14
5. **Frequently Asked Questions** .................................................................................. 15
1 Introduction

The Stratus® ftServer® system is designed to be a fault tolerant platform, dealing with just about any hardware failure it encounters without interruption. Similarly, with its hardened drivers and self monitoring software, it can successfully deal with and recover from a wide variety of software failures as well.

The goal of continuous availability for Mission Critical applications is such that simply “coping” with a hardware failure is not enough. The failure needs to be reported to Stratus so that a spare can be shipped to the site and the failed component replaced.

This automatic notification of faults to Stratus can be done in two ways. The ftServer system may connect to Stratus via dial-up over a standard analog telephone line, or by sending an encrypted package of information over the Internet to a secure server. The Stratus network that accepts this information is known as the ActiveService™ Network (ASN). All Stratus support contracts include this to one extent or another.

Similarly, just “recovering” from a software failure is not considered enough for Mission Critical applications. Knowing what caused a software failure, being able to “root cause” it and potentially put in place actions to prevent it from happening in the future is considered vital to raising the bar on the availability of mission critical applications.

This ability to trouble-shoot and root cause issues is a service that Stratus can provide as part of our more comprehensive support options. To provide this, together with more general remote troubleshooting, some form of remote access to the ftServer system is required by the Stratus Customer Service staff.

There are three methods by which it is possible to establish a remote support session on the ftServer system. The first two (and by far the preferred methods) are via the ASN. The ASN can provide Stratus Customer Service a secure connection to the customer system via a dial-up analog line or for systems connected to the Internet, via an encrypted TCP connection. The third alternative is via an internet based service we call ASN/Web (powered by WebEx). WebEx requires participation by a customer representative in the connection process.

The most secure option would be to have no remote support capabilities. While this offers the most security it will severely limit proactive and reactive support and likely increase both the number and duration of system interruptions.

This document has been developed to address the various security concerns that customers may have when considering the implementation of the Stratus ASN to support their Stratus systems.

It provides an overview of how the ASN works, and looks in detail at the various measures and options that can be put in place to minimize security risks, and their implications with regards to the level of service Stratus can provide.
2 ActiveService Network (ASN)

2.1 Overview
The ASN is a private, IP based network designed to facilitate the remote support of the Stratus ftServer product family. It allows the Stratus Technical Support Organization (TSO) to do the following:

- Allows ftServer machines to connect to the network (via the Internet or dial-up modem) to report problems and events which may need the attention of the TSO.
- Provides a secure mechanism to enable TSO engineers to connect to an ftServer system to conduct diagnostic and remedial activities.

2.2 ActiveService™ Network Features
The ASN is a secure, fault-tolerant, worldwide network that enables instantaneous, around-the-clock monitoring and troubleshooting of systems regardless of physical location. With the facilities of the ASN, authorized support professionals in Stratus Customer Assistance Centers around the world can work together to expedite the resolution of problems.

2.3 ActiveService Manager
The ActiveService Manager (ASM) is a global, real-time information portal accessible to customers with ftServer systems covered by an ftService agreement. This Web-based interface lets service partners and customers participate in the service process first-hand. A designated ASM administrator specifies appropriate levels of access for staff. Authorized users can maintain their own profiles, add and update new issues, escalate events, and view Stratus’ Global Case Manager database to track issues pertaining to Stratus servers within their own company.

2.4 Out of Band Management
Most ftServer systems are sold with a Service Management Module (SMM). These modules come in various forms depending on the server model. The SMM may be a PCI card, a board that plugs into a DIMM-style slot or a Baseboard Management Controller (BMC) chip. Operating on independent power and network connections, the SMM allows remote communication between the ftServer system and the Stratus ASN allowing Stratus customer support personnel to troubleshoot and diagnose problems regardless of the system's state. That is, Stratus' ftServer systems equipped with these devices need not be booted up with the operating system — or even powered on — to permit access to the server for troubleshooting.

The SMM enables a Stratus service engineer to remotely power on/off or reset/reboot the system; they also manage the security of incoming and outgoing communications through the ASN or customer maintenance network. It is important to note that the SMM operates independently of the host operating system. Connections made between the access adapter and the ASN Hub employ multiple layers of authentication. Stratus offers built-in monitoring and support for all ftServer family models as well as one of the following adapters:

- ftServer Access Adapter (ftSAA)
  This PCI card contains a processor, an Ethernet port, modem and video support for the system console. It runs its own operating system and is independent of the ftServer system. It has the ability to control main power to various components of the ftServer system as well as monitor the boot process. It can detect a hung host OS and initiate a reboot of the host OS to facilitate rapid recovery.

Stratus or the Administrator may connect to this device via the Maintenance Ethernet network connection or Stratus may connect via the modem to perform various troubleshooting or diagnostic procedures. Access is User Id and Password protected and the User Id and Password are under Administrator control. The ftServer Access Adapter is not offered by Stratus on new ftServer models but is fully supported by Stratus.
Remote Access Security for ftServer Support

Figure 1: ftSAA

Virtual Technician Module (VTM)

Stratus’ second-generation remote access adapter frees up PCI capacity by using a DIMM-style slot instead of a PCI slot. This VTM also provides embedded video support for the system console and an Ethernet port. No internal modem exists in this VTM but it can utilize a Stratus backplane mounted ASN modem (see Figure 2).

The VTM also adds the ability to connect the ftServer system to an ASN Hub over the Internet using an IP network running over a secure HTTP TCP tunnel. This provides performance and reliability advantages compared with a dial-up phone connection. The DIMM-slot style VTM is not offered by Stratus on new ftServer models but is fully supported by Stratus.

Figure 2: VTM Card being retained by two white tabs
Remote Access Security for ftServer Support

- **BMC (VTM)**
  
  Stratus’ third-generation remote access adapter is built into the Baseboard Management Controller which comes with every system. Like the DIMM-style Virtual Technician Module it makes use of the system’s modem (see Figure 3), embedded video, and Ethernet.

![Figure 3: System modem](image)

2.5 **Basic Call Home Support**

Basic Call Home Support allows a customer’s ftServer system to deposit alarm messages with Stratus to advise of system problems, configuration changes and other events significant in the support of the customer's system. As stated in the Introduction “simply “coping” with a hardware failure is not enough”. To achieve the goal of continuous availability, any hardware failure must be rapidly identified and corrected to provide fault tolerant system operation. With Basic Call Home Support a failure of this type would cause an alarm to be sent to Stratus alerting Customer Service Engineers that action must be taken to insure the system is operating properly and any failed parts are correctly identified and replaced.

Call Home Support can be accomplished over private dial-up telephone lines or via the Internet.

2.6 **Interactive Connection Support**

Interactive Connection Support provides the ability for Stratus Customer Service Engineers to make a two way secure connection to the customer’s system where they can then access the SMM or establish a remote terminal session to perform live troubleshooting or monitoring or to login to the Operating System. This connection may be established over analog telephone lines or if the specific hardware and release of the ftSSS software support it, over an encrypted internet connection.

Interactive Connection Support is mandatory for the higher levels of Stratus ftServer support offerings. The support engineers would use the connection to establish a remote Terminal Session on the ftServer system, logging into a specific Stratus account to perform whatever support activity is required.

Interactive Connection Support does entail some security exposure for the customer however this is mitigated by careful management and the inherent security features of the ASN, which will be discussed in more detail later.
2.7 How the ASN Works

A. Real Time Alerts (RTA) Internet Call Home Server authenticates calling machine based on serial number and model code. Utilizes a no-interface web form for additional security. This technology securely delivers the call-home message to Stratus via 128-bit SSL (Secure Sockets Layer).

B. ASM servers provide an encrypted web site and require a password to access.

C. Stratus Firewall protects Stratus LAN against unwanted internet traffic.

D. Customer Service Agents are authenticated by ASN connection software prior to access of Customer machines.

   Customer Service Agents are further authenticated by an RSA Secure ID two-factor authentication facility (requires the use of a hardware key – or token – generator.

E. ASN Router protects Stratus and ASN networks against unwanted traffic from an ASN access point.

F. ASN Hub uses packet filtering and port filtering to secure ASN connections against each other.

G. Service Management Module (identified as SMM in the diagram) requires proprietary connection negotiation algorithm, utilizes callback, and requires multiple username / passwords.

H. ftServer system security is entirely under the control of the customer. Stratus personnel require customer issued credentials to access.

I. Customer firewall protects Customer’s LAN from unwanted Internet traffic.

ASN modern dial up connections initiated by Stratus are established via a “call back” process. An “enquiry” call is made from Stratus to the ftServer system at which time a username and password is supplied. The ftServer system breaks the connection then validates the username and password against an internal database under the control of the customer. If valid, the ftServer system then dials an ASN Hub at a preconfigured phone number. The ftServer system then presents valid system serial number and password prior to being granted access to the ASN. If this validation is successful, then the ASN Hub looks for and
Remote Access Security for ftServer Support

completes the connection to the Stratus Customer Service Engineer. This prevents an unauthorized person in possession of the ftServer system’s phone number (and even username/password) from connecting to the site from an unauthorized location.

ASN Internet connections initiated by Stratus are similar but a little different. The diagram below outlines the steps of this connection process. The first step (not shown) is: 0) Stratus Customer Service Engineer requests a connection to a customer ftServer system. 1) The ftServer system continuously polls the Hub (once every configured interval) via a secure encrypted HTTPS connection. 2) The ftServer system must provide its credentials and if they are successfully validated then the connection request is passed back to the ftServer system. 3) The ftServer system prepares to set up SSL connection. 4) The Hub software modifies network routing tables appropriately and tunnels IP traffic between Stratus and the ftServer system through the SSL connection.

Figure 4: Internet dial-in conceptual overview

2.8 Security
There are a wide range of security measures that are built within the design of the ASN and available for implementation by the customer to provide additional peace of mind. Each of these is described below. For the optional ones, the implications to the support process are also outlined.

2.9 Network and Data Security
Security must always be a priority where mission-critical servers and applications are concerned. Stratus has a track record in security that spans some 25 years of remote service delivery.

The ActiveService Network incorporates multiple layers of security technologies and practices to protect the networks of connected customers, as well as Stratus, from being breached. The safeguards begin inside Stratus Customer Assistance Centers:

- All customer service data is maintained by Stratus on a secure database. Access to the database is tightly controlled via customized applications.
Remote Access Security for ftServer Support

- Physical equipment is kept in secured locations; all are within secure Stratus properties and the support servers and network hardware themselves reside in locked computer facilities.

- The servers are connected to a separate dedicated domain; access from the Stratus corporate domain is only granted to authorized administrators.

- Service network functionality is protected against unauthorized access within Stratus by a strong two factor authentication system. The RSA SecureID® technology relies on something the user knows (a user-generated PIN) combined with something the user has (a program-generated, constantly changing token identifier) – providing a much more robust level of identity and access control than reusable passwords.

From there, ASN security maintains the safety and privacy of connections between Stratus Customer Assistance Centers and customers’ systems. Internet call-home facilities use 128-bit encryption (SSL) and a public certificate authority which validates the authenticity of the Stratus Internet server.

Dial-up connections for call home are established through a Stratus-enhanced process which adds mandatory, custom-coded authentication and negotiation steps including:

- Additional proprietary IP address assignment
- Encrypted CHAP password negotiation
- Proprietary validation of system ID PROM values, including serial number and model code, against corresponding information stored on the Stratus ASN Hub

All authorized internal users of the Stratus ActiveService Network using an ASN connection for customer support activities are authenticated as follows:

- Two-factor authentication using RSA SecureID tokens to gain access to the Stratus ASN.
- Special ASN authentication to ensure the user is an authorized customer service employee with the need to make a remote support connection
- Additional ftServer system site access restrictions as configured by the customer

Authorization Control

Firewall protection is another essential element of keeping the worldwide ASN network secure. This includes:

- A firewall that protects customer and the ASN networks against unauthorized and/or unexpected transmissions via the remote service link
- A firewall that protects individual customer connections from each other
- A firewall that protects the ASN network from any unauthorized or unexpected transmissions to or from the Stratus corporate network
- Ability of the customer to manually enable/disable service connections to and from the system at any time

Centralized user access control mechanisms provide ways to manage ASN access privileges. They ensure that ASN users can only tap into the resources that are relevant for maintaining customer service level agreements. At the same time, they bar ASN users from accessing resources that they are not entitled to use. ASN authorization and management controls include:

- Direct access to the ASN is restricted to Stratus internal employees from secured Stratus business premises. Stratus service employees are prohibited from connecting to the ASN via a remote PPP dial-in or VPN connection.
- Stratus maintains a centralized security database that defines the authorization profile for each user.
  - The employee must use a valid Stratus domain password.
  - The domain account must be registered as a valid customer service user.
- Stratus ASN user profiles are segmented into five levels of controlled access privileges.
Remote Access Security for ftServer Support

- Administrator: reserved for internal users responsible for maintaining ASN network resources.
- Privileged: reserved for specialized internal users with a need to access and troubleshoot customer ftServer systems.
- General: reserved for internal users with ASN general access (access to customer ftServer systems directly from the ASN is prohibited).
- Partner: reserved for external customer service users with a need to access service information on his or her installed customer locations (access to customer ftServer systems directly from the ASN is prohibited).
- Customer: reserved for Stratus customer employees with a need to access service information concerning his or her global sites (access to customer ftServer systems directly via the ASN is prohibited).

Accounting Control

Stratus’ accounting policy provides a method for connecting and sending security information used for billing, auditing and service level reporting. Accounting policy elements include:

- A call-tracking database tracks user identities, usages, dates, and resources accessed.
- Activity logs are created and maintained for all ASN connections to customer sites.
- Logs are available for customer access via the ActiveService Manager Web site.
- Activity logs are reviewed quarterly to detect evidence of unauthorized access.

2.10 Description of built-in security controls

Figure 5: Secure ActiveService Network
The ActiveService™ Network has several layers of security built in to its design:

- **ASN Hub Login Security**: Multiple levels of Username and Password are required to access the machine and are restricted to a few selected operations personnel.

- **ASN Hub Domain Security**: ASN Hub machines exist in a special “ASN” domain, which is protected from the primary corporate domains. This limits direct access to the ASN infrastructure within Stratus to explicitly authorized users.

- **ASN Hub Firewalls**: The ASN Hub is physically installed behind a firewall/router to restrict access between the Stratus network and the ASN. Stratus ASN facilities are also fully protected by the Stratus Corporate firewall. This ensures that IP traffic which is not specifically required for the ASN will be blocked.

- **ASN Inbound Traffic Proxy Server**: The ASN utilizes an inbound proxy server for acceptance of HTTPS packets to the ASN network. This proxy server resides in the Stratus DMZ and forwards traffic to ASN Hub servers behind firewalls within the Stratus Network. The proxy servers allow for an externally facing Internet presence while keeping systems that need to process the traffic for that presence safely residing behind firewalls which secure the servers from hacking attempts.

- **ASN Hub IP Filtering**: The ASN Hub uses an active IP filter to ensure that routing between unauthorized destinations is not allowed. By default, no routing between the ASN Hub and any connected destination (including Stratus Network and Customer destinations) is allowed. When a properly authenticated (details below) connection request is received, either from a Customer Site or a Stratus Engineer, specific routing between the Customer Site and the appropriate Stratus destination is allowed for the duration of the connection.

- **ASN Authentication**: Incoming Site Connection Requests are validated by the ASN connection service by comparing the submitted model number, serial number and password against a database prepared internally against manufacturing, delivery and customer service records.

  Call Home Message submissions are validated against the customer service internal site database. Exceptions are reported to the Hub system administrator(s) via E-mail. Stratus Support personnel requesting connections to customer sites for troubleshooting purposes are validated by the ASN connection service against a list of known users. Any users of the ASN Hub hardware itself (there are very few as only operations personnel require this access) are authenticated against a special restricted ASN list.

- **RSA Secured ID Authentication**: All Stratus Support personnel who request a connection to a customer site via the ASN are required to be authenticated by a strong two-factor authentication

- **ASN Connection Security**: To request a connection to a customer machine via the ASN, Stratus Support personnel must have a special username and password. This username / password is authenticated by the ASN software itself.

- **Proprietary Connection Protocol**: While the ASN dial up connection is based on Windows Routing and Remote Access Service (RRAS), additional mandatory proprietary handshaking logic has been added to the connection process such that casual users would not be able to connect to the Hub.

- **ASN Logging**: Various ASN processes create log records of activity. For example, each connection to a customer site is logged (who connected, when, and for how long). Each user access to an ASN connection is similarly logged. These two logs are visible to customers using the Stratus ASM facility; Note that these records are aggregated to the Atlas Database and maintained historically (though subject to periodic archiving).
Secure Internet Functionality: Interactive connections between Stratus ASN Hubs and customer systems over the Internet are made using HTTPS which establishes a secure TCP tunnel. This provides simplicity, performance, and reliability advantages compared with a dial-up phone connection.

2.11 Additional Optional Security Controls
On the customer site itself, the customer is responsible for the security of their machine, and there are a number of additional steps that they can take to reduce the risk of unauthorized access and to gain assurance about unauthorized activity once logged in.

- **Air Gap:** The risk of unauthorized connections over the ASN can be totally eliminated by simply pulling the phone cable out of the modem when not required. The obvious disadvantage is that in the event of a Stratus support engineer requiring access to investigate a problem, someone would have to physically re-plug the cable to allow access. For unmanned sites, this is impractical, particularly if access is required in the middle of the night. It also can incorporate a delay into the support process, which for a mission critical server may well be unacceptable. Doing this would also necessitate the ftServer system sending its call-home alerts over the Internet, as without the cable in place, it would be unable to place a service call using the phone.

- **Disable modem’s ability to receive incoming calls. (Call-in Enable):** It is possible for the customer to enable or disable the modem’s ability to receive incoming calls without interfering with the ftServer system’s ability to deposit alerts to Stratus. The disadvantage of this method is that it still requires the customer to re-enable the modem prior to Stratus being able to dial in, resulting in a potential delay to support being provided — again, not ideal for a mission critical server.

- **Enabling/Disabling of the Stratus login:** When Stratus dials into an ftServer system to provide support, they effectively establish a remote terminal session on the box. Another way to prevent unauthorized access is to either disable the Stratus login, or to change the password, only enabling it when Stratus has been asked to dial in. The disadvantages of this method are identical to the above.

- **Local logging and monitoring of Stratus Login:** Stratus require a Local Administrator level login to provide their remote support as many of the support activities that the Stratus TSO might need to perform are such that they require this highest level of access. Built into Windows are a number of measures that can be taken to ensure that the Stratus account is suitably restricted in terms of access to data and network, as well as its activity logged to provide an audit trail of Stratus support activity. Through appropriate use of Group Policies, a high level of security over the Stratus login can be achieved.

- **Internet Proxy Server:** Systems that wish to use Internet features such as Call Home delivery or Internet Interactive connections can configure their systems to access the Internet through an Internet Proxy server as a security measure. The proxy server acts as a gateway through which traffic passes between the customer network and the Internet. This gateway shields the customer system from many internet threats.
3 Internet Connections

Customer sites need to access Verisign URL in order to verify the SSL certificate and to get the latest certificate revocation lists. Stratus currently uses Verisign as a trusted Certificate Authority vendor.

Note that the IP address for the Verisign hosts may change at any time. When debugging access problems please ensure that the IP addresses are still current. The Stratus inetcallhome server located in Maynard has a ‘failover’ server in Phoenix which is on a different network. The numeric IP address should not be used or hardcoded unless absolutely necessary for firewall configuration.

3.1 Internet Call Home

To facilitate Internet call home delivery, Stratus maintains a web server which accepts call home messages. This facility is secured as follows:

- By nature, the transaction is “one way”, from the ftServer system to the Internet Call Home facility. The exposure to the ftServer system is minimal and can be managed by various facilities on the customer’s network (i.e. firewalls, proxy servers, etc.).

- The call home transaction is encrypted using SSL (Secure Sockets Layer) to prevent unauthorized interception of the call home messages’ content.

- The Internet Call Home Server is verified on the ftServer system prior to transmission by the Verisign Authentication service (for more information, see http://www.verisign.com/)

- Each connection to the Internet Call Home server is validated by Stratus to ensure that only a valid ftServer system, properly registered with Stratus Customer Service is able to be used.

Sites that are configured to deposit call home alarm messages via the Internet should have the following outbound ports opened either globally or for the ftServer system interface that has access to the Internet or (if a proxy is being used) for the proxy’s network access.

<table>
<thead>
<tr>
<th>URL</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>inetcallhome.stratus.com</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>svrsecure-crl.verisign.com</td>
<td>TCP</td>
<td>80</td>
</tr>
<tr>
<td>svrsecure-aia.verisign.com</td>
<td>TCP</td>
<td>80</td>
</tr>
</tbody>
</table>

3.2 ASN Internet dial-in

For ftServer systems equipped with the Virtual Technician Module (VTM), Secure Encrypted HTTPS connections are possible. The ASN Secure Encrypted HTTPS connection provides a secure bidirectional internet connection between the ftServer system and Stratus Customer Service using proven industry standard technology including 128 bit SSL encryption and a strong two-factor authentication. The ASN internet connection implementation uses a strong two-factor authentication protection method.

- Customer ftServer system polls Stratus with encrypted messages periodically.
- A certificate authority is used to verify connection to/from Stratus.
- Customer’s ftServer system is always the initiator of the SSL connection.
- The ASN logs all connections and all users to provide an instant and perpetual on-line record of system access to the customer.
- All Stratus ASN infrastructures are located within secured Stratus facilities.

Sites that are configured for dial-up using VTM internet protocol should have the following outbound ports opened either globally or for both of the VTM addresses (since either VTM may make the connection) or (if a proxy is being used) for the proxy’s network access:

<table>
<thead>
<tr>
<th>URL</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>inettunnel.ecacsupport.com</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>svrsecure-crl.verisign.com</td>
<td>TCP</td>
<td>80</td>
</tr>
<tr>
<td>svrsecure-aia.verisign.com</td>
<td>TCP</td>
<td>80</td>
</tr>
</tbody>
</table>
3.3 WebEX Support
Stratus Support personnel may also connect to an ftServer system via WebEx. WebEx uses Secure Sockets Layer (SSL) encryption.

ASN/Web gives Stratus the ability to remotely logon to a customer’s ftServer system in an environment in which the customer may visually monitor all activities performed by the Stratus Support personnel. It should be noted that use of this facility requires that a Customer representative with Administrator privileges be present (either physically or via a remote connection) at the ftServer system in question. This facility also requires that the ftServer OS be running.

3.3.1 ASN/Web (WebEx) Security
The ASN/Web uses Secure Sockets Layer (SSL) encryption to secure the transmission over the Internet. Only a host connecting through a specific ASN/Web server will be able to make a secure connection. Access to your ftServer system is only possible with your approval. You must first call into the ASN/Web server and connect to the specified ASN/Web session number. You may stay on the system and monitor all actions that take place over the connection and can disconnect at any time.

3.3.2 How the ASN/Web works
ASN/Web (powered by WebEx) maintains servers connected to the Internet that can host interactive remote support sessions.

A Stratus Service Engineer (SSE) connects to the ASN/Web server and establishes a secure remote support session. The SSE notifies you with the URL and the connection number for the session.

Figure 6: Collaborative Sessions

With your approval the Stratus Engineer can access your system via remote control. The engineer can interact with the host operating system, applications and transfer files, etc. At all times you will be able to see all actions that take place and you can terminate the connection at any time.

ASN/Web can also support collaborative troubleshooting sessions. With your approval, operating system, networking, application vendors and other experts can simultaneously participate in the remote support session.
4 Services and Drivers

The following services and drivers are needed for the ftServer ASN to function properly. This is not a list of all required services and drivers for an ftServer system; it is only a subset specific to the operation of the ASN and alarm reporting.

Please note that in newer releases (release 5.0 and newer) of the Automated Uptime Layer (AUL) software the phrase “Stratus ftServer system” has been replaced with “ftSys” so in the older release it would say “Stratus ftServer system Alarm” and in newer releases it would be “ftSys Alarm”. (The AsnService did not exist prior to release 5.0 and as such has always been named ftSys AsnService.)

4.1 Services

- **Stratus ftServer Maintenance and Diagnostics (MAD):** Provides maintenance and diagnostic capabilities for managing fault-tolerance.
- **Stratus ftServer Inventory:** Manages the inventory of hardware and software associated with the server.
- **Stratus ftServer Alarm:** Used to notify various sources including Technical Support of alarm conditions.
- **ftSys AsnService:** Manages the tunnel connection for internet dial-in on the newer 2600, 4500 & 6310 ftServer systems.
- **Stratus ftServer Policy:** Identifies alarm conditions by filtering and correlating hardware and software events.
- **Stratus ftServer RAS:** Handles dialup connections to ASN Hub for alerts. This service is only used where modems are utilized and there are no VTMs in the system.
- **Stratus ftServer RPC Provider:** Manages the WMI callhome configuration and status.
- **Stratus ftServer SSN:** Provides configuration and routing management for VTMs.
- **Virtual Disk Service (Microsoft):** Provides management services for disks, volumes, file systems, and storage arrays.
- **Remote Access Connection Manager (Microsoft):** Manages dial-up and virtual private network (VPN) connections from this computer to the Internet or other remote networks. If this service is disabled, any services that explicitly depend on it will fail to start.
- **Telephony (Microsoft):** Provides Telephony API (TAPI) support for programs that control telephony devices on the local computer and, through the LAN, on servers that are also running the service.

4.2 Drivers

**Stratus ASN Tunnel Driver:** Establishes and manages the ASN tunnel connection between the ftServer system and Stratus ASN network.
5  Frequently Asked Questions

Why would Stratus require Dial in or secure encrypted HTTPS Access?
Although the ftServer system has been designed for continuous availability, there are occasions when Stratus will need to dial in to the box, either to verify the ftServer system’s self diagnosis, or to assist in the resolution of a software related issue. Without the facility to login to the ftServer system, Stratus’s ability to provide support is severely compromised and the resolution of technical issues simply through discussion with the customer’s own technical staff becomes much more problematic and may significantly increase the time it takes to resolve the issue.

What options do I have to restrict Stratus dialing in?
There are several, including a physical Air Gap (unplugging the modem cable), software disabling of the modem’s ability to receive calls and simply disabling the Stratus login. These are discussed in more detail in section 2.1.4.

What system(s) does Stratus use to perform their remote support?
Upon establishing a remote terminal session via the ASN, the support staff typically uses the ftSMC, general Windows administration tools, windbg (for dump analysis) and some Stratus specific tools which can be found on the ftServer system under c:/program files/stratus/customerservice. (Starting in release 5.0, “stratus” has been changed to ‘ftSys” so the path would be c:/program files/ftSys/customerservice.)

What auditing of support activity is there?
The ASN logs connections (in terms of who, when and for how long) on both the ftServer system itself and on the Stratus Atlas database – viewable via the ActiveService Manager web-portal. Other generic Windows logging can be enabled to track activity on the ftServer system itself while logged in.

How much access does Stratus have to my network and the files in it?
Stratus access is restricted to what you’ve provided with the login ID. It is the customer’s responsibility to assign the correct level of authorization to the Stratus login. A local administrator account is required to provide support, but this does not imply access at domain level. Like any other Windows login, it is possible to restrict the access of the Stratus login using standard Group Policies.

What encryption standards do you use? Where do you use encryption? How many bits are used in your encryption algorithm?
Stratus utilizes 128 bit SSL encryption for the Internet connections. Most transmissions via dial up (with the exception of CHAP user Id and Password authentication are not encrypted as they occur over private phone lines and are not judged to be at risk.

When a user is authenticated what processes are used?
Incoming Site Connection Requests are validated by the ASN connection service by comparing the submitted model number, serial number and password against a database prepared internally against manufacturing, delivery and customer service records.

Call Home Message submissions are validated against the customer service internal site database. Exceptions are brought to the attention of the system administrator.
Stratus Customer Service Engineers requesting connections to customer sites for troubleshooting purposes must provide proper User ID and Password and are validated by the ASN connection service against a list of known users. Additionally, they are further authenticated by an RSA SecureID two-factor authentication facility requiring the use of a hardware key (token) generator.

Any users of the ASN HUB hardware itself (there are very few as only operations personnel require this access) are authenticated against a special restricted ASN windows domain list.
Customer Service users accessing a customer ftServer system are validated by both the ftSAA or VTM and the customer’s Windows OS (both of which are under the customer’s control)

**What are your provisions for detecting and responding to “Hacking” or denial of service (DDOS) attacks?**
Stratus employs an Intrusion Prevention System that notifies network engineers who are on call 24x7.

**What ports are proposed for use on our firewall? What Protocols?**
The following is a list of URLs and ports that may need to be opened:

<table>
<thead>
<tr>
<th>URL</th>
<th>Port</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>inetcallhome.stratus.com</td>
<td>TCP 443</td>
<td>Internet Call Home</td>
</tr>
<tr>
<td>srvsecure-crl.verisign.com</td>
<td>TCP 80</td>
<td>Internet Call Home</td>
</tr>
<tr>
<td>srvsecure-aia.verisign.com</td>
<td>TCP 80</td>
<td>Internet Call Home</td>
</tr>
<tr>
<td>inettunnel.ecacsupport.com</td>
<td>TCP 443</td>
<td>Internet Dial In</td>
</tr>
</tbody>
</table>

Customer sites need to access the Verisign URL in order to verify the SSL certificate and to get the latest certificate revocation lists. Stratus currently uses Verisign as its trusted Certificate Authority vendor.

**Where is the user record or identification defined? Who defines the user? Who maintains those records?**
ASN User records and passwords are defined and maintained by Stratus Customer Service Operations. These are maintained in a secure Oracle Database at Stratus headquarters. Customer ftServer system user accounts and passwords are maintained by the owner of the ftServer system (i.e. the customer);

**Where are access attempts by an unauthorized user logged?**
The ASN hub maintains logs for successful and failed access attempts; Attempts to access ASN hubs via the dial-in modems are logged by Windows RRAS.

**Are there lockout features prohibiting repeated attempts to break a password? How is this established? What are the options available? Who monitors those logs? Who is notified of questionable activity?**
Standard Windows Server mechanisms are used by Stratus and available for use by Customers (on the ftServer system).

**Does the system log off inactive users? What time settings are available and how are they established?**
The ASN has a provision for breaking idle connections after a configurable amount of time. The security policies of the customer ftServer system are under the control of the individual customers who own them.

**What is the registration process for establishing a new user account? Do you use passwords and Ids, do you use PIN’s, SSL, or a combination of methods?**
New Customer user accounts are established by inputs from several business processes, as detailed below:

When an ftServer system is manufactured, information on the model and serial number is maintained in a database which feeds into the Customer Service master site list; When an ftServer system is purchased and shipped, information generated from the order processing systems feeds into Customer Service and augments the previous information from Manufacturing;

When an ftServer system is installed, further information about the specific installation is added to the above information. All information mentioned here is required to establish an SSN account for a customer. And, finally, as new accounts are primarily established by processes internal to Stratus, SSL or PIN is not required. eCAC, the Stratus Web based call system for customers employs SSL encryption.
Does the user make live updates to the production database? Or are they providing us with a transaction-based approach?
The ASN updates the production database indirectly. Call Home messages are deposited onto an ASN hub where they are vetted by several processes. Following processing on the hub, they are “handed off” to a database interface server which performs final checks and updates the production database. Note that the production database features full revision history on all critical tables.

How do we handle routine maintenance of the ASN Hubs? Does the system have to be off-line to conduct it?
Most maintenance is conducted without significant downtime. It is occasionally necessary to bring down a local ASN Hub however this does not affect ASN service as the remaining hubs are able to accommodate any user worldwide.

What limits or activity thresholds are available to track unusual activity on a member or customer’s account?
Connection records and other logs are logged by both manual and automated processes. Suspicious activity is dealt with as it is encountered.

What are your backup and recovery capabilities? When was your last test? What were the results?
Stratus has fault tolerant (as one might expect) capabilities for all mission critical customer service functions. The Customer Service database (which includes critical ASN information) has several backups. The primary backup is a replicated database which is continuously kept up to date and is able to serve as the primary database on a moment’s notice. A “hot standby” database is also maintained in an alternate location which can be put in service within minutes. Daily data backups are also conducted.

The Stratus ASN currently consists of over a dozen ASN hubs located worldwide. Any one ASN hub is fully capable of providing support to any customer’s ftServer system worldwide. All hubs are part of the Stratus (private) wide area network and are managed from our Maynard operations center.

How do the security features differ for Linux ftServer systems?
All security features implemented for Windows ftServer systems are present in the Linux implementation. CHAP and SSL encryption are used to secure sensitive data. Other features such as the call-back mechanism are identical to their Windows counterparts.

Has Stratus tested their server to ensure that connection attempts without valid site id are rejected?
Yes. This has been tested and evaluated by a third party security audit firm.

Is it possible to submit an authentication request with an altered password, serial number, and second password? Can we observer an authentication attempt in order to watch it fail? Has Stratus tested this?
Yes it is possible and Stratus can arrange to alter this information for a test. Yes Stratus has performed this test.

Does Stratus ASN Hub mask customers IP addresses?
The IP addresses known to the ASN during the connection are Stratus addresses which are temporarily assigned to the customer ftServer system only for the duration of the connection.