



Proposal for the Aventail.Net Managed Services

**Prepared for:
Mike Fratto
Technical Editor
Network Computing**

Executive Summary

Who is Aventail?

Aventail is a leading provider of secure, anywhere access to Web and client/server applications. The company has years of real-world experience delivering SSL VPN products and services that help large enterprises solve the complex problems associated with extranets and remote access. Since 1996, nearly 400 corporations—including industry leaders such as DuPont, Deloitte Consulting, Ernst & Young, FMC, Mount Sinai NYU Health, and ANXeBusiness—have purchased Aventail's products and services to provide their customers, partners, and employees with secure, anywhere access to their applications. To date, more than 400,000 end users have benefited from Aventail's innovative technology.

What are the market challenges?

The way corporations conduct business has changed. Companies used to have clearly delimited network borders—employees inside, and customers and partners outside. Now, those lines are blurred. Employees access resources from outside the network, and customers and partners are an integral part of the extended enterprise. You need a single, complete secure access solution.

While IPSec-based VPN solutions are good at providing secure site-to-site connectivity, they handle only a few use cases—such as dial-up with a company PC. They can't deliver clientless, anywhere access. On the other hand, most Web access control or SSL appliance vendors can't help you extend your client/server applications.

Aventail's unique, combined proxy and SSL-based VPN technology and managed services provide a single secure solution to support all of your access scenarios. Plus, Aventail's services handle the complex security, user management, and directory challenges that arise when building and managing extranet and remote access VPNs.

What is the advantage of Aventail's products and services?

Extranet and remote access VPNs can be painful to implement and even harder to support. Typically, companies either force-fit an IPSec solution—which comes with high support costs—or they build a custom secure Web environment by replicating applications to the demilitarized zone (DMZ)—which requires a costly new development project for each application deployed.

Aventail offers a better choice. With any of our managed appliances, you avoid the costs of replicating servers to a DMZ, installing plug-ins or agents at each Web or application server, and completing extensive network configurations. Each of our managed appliances combines Web and client/server authorization, policy management and enforcement, authentication, encryption, global Internet roaming, and reporting into a single solution. Our managed appliances come with our SSL VPN management service, which includes deployment, around-the-clock system management and monitoring, Web-based security administration consoles and security administrator helpdesk support, and a service level agreement (SLA). On top of that, you can choose from valuable Aventail.Net™ managed services such as Roaming Internet Access, User Management, Directory Management, and End-User Support.

Why is Aventail different?

Secure, anywhere access to your applications.

Our clientless approach gives users easy access to Web applications. In addition, our low-impact agent makes access to client/server applications just about as easy for your users—and for your IT department. With Aventail technology, your users have hassle-

free access to anything from basic Web applications to complex corporate applications like SAP.

When we say we deliver "anywhere" access, we mean anywhere. Users can access applications from any computer with an Internet browser—from a home computer, a hotel using a broadband connection, a public kiosk, or behind a firewall on another company's network. Users will appreciate this convenience, and you won't miss the VPN client-related support calls.

Maximum security.

Our unique combination of SSL, proxy technologies, and policy management tools and services provides proven security. Aventail delivers user-level authentication with granular access control to give only the right people access to the right resources. Our proxy model eliminates any direct connections into your corporation's network resources.

Lower TCO.

To help you avoid deploying and managing multiple devices, we offer secure access to both Web and legacy applications from a single managed appliance. This integrated approach adds up to a lower TCO. Our clientless access to Web applications often eliminates the costly and tedious task of distributing and managing clients. And if your users need access to client/server applications, our low-impact agent is much easier to distribute and support than an IPsec VPN client. As a result, you get a speedy roll out, fewer support calls, and a faster ROI. Our managed appliances seamlessly integrate into your existing network, security, and application infrastructure, so you won't need to purchase additional hardware or software. Finally, our proven implementation and integration processes get your VPN up and running fast—often in under 4 weeks.

Extensive suite of managed appliances and services.

We offer the industry's most comprehensive suite of SSL VPN managed appliances and services. So whether you need an entry-level managed appliance to support hundreds of users or an enterprise-class system to support several thousand users, we've got the right solution. Each Aventail managed appliance comes with our SSL VPN management service, including deployment, around-the-clock system monitoring, and more. To further reduce your IT department's administrative burden, we also offer Aventail.Net add-on services such as User Management, Managed Directory, Roaming Internet Access, and End-User Support.

Proven technology from an experienced, focused company.

Aventail is focused on continually improving our VPN security products and services. Innovators in combining proxy and SSL VPN technology, we launched the first SSL VPN product in 1997 and the first SSL VPN service in 1999. Today, we continue to build upon the invaluable experience gained while helping numerous large companies solve complex extranet and remote access problems. Aventail provides mature solutions that have been extensively tested in the real world to ensure that they meet your needs.

RFI Response

A detailed description of the NOC, specifically regarding redundant systems and fail-over policies.

The Aventail technology platform consists of two components: A customer-premise based rack of equipment (CPE), and remote monitoring and management from a Seattle-based network operations center (NOC) and data center.

The CPE consists of a standard-sized rack of equipment, hosted at your site or your hosting partner's site. It provides the local enforcement of your access policy and the actual delivery of secure access.

All of our CPE based software runs on redundant, high-capacity servers, backed by traffic management and load balancing technologies. Key services like power and storage are designed to fail-over safely. The CPE is initially sized to accommodate your estimated user population over the first 24 months of the managed service. Because the Aventail technology platform is delivered as a managed service, essential characteristics like availability, redundancy, and scalability are our problem and not yours.

The following hardware and software services are included in the Aventail technology platform and delivered in the CPE:

Our technology platform provides authorization, encryption, and integration with directories and authentication. Modules include:

- Aventail ExtraWeb: Secure proxies for Web applications.
- Aventail Anywhere VPN: Secure proxies for enterprise client/server applications.
- High Availability. Intelligent traffic management hardware incorporated into the CPE ensures internal fail-over and load balancing between servers.
- Data Integrity. The integrity of user and policy information is verified cryptographically.
- Monitoring and Surveillance. Network and systems management probes monitor system performance, activity, and utilization.
- Directory Management. Redundant LDAP directories organize user information synchronized with a master directory.
- To manage information security risk, we run the CPE on a hardened version of UNIX, stripped of all unnecessary TCP/IP services.

Our Network Operations Center (NOC) provides around-the-clock remote support, monitoring, and management of your CPE. Located in Seattle, Washington, the NOC is an advanced, restricted-access operations center. The Data Center systems run on Solaris and NT operating systems. The Aventail Data Center is hosted at a secure location that provides for:

- Fully redundant HVAC system
- Controlled temperature and humidity environment
- Fire threat detection and suppression system
- Around-the-clock critical monitoring/disaster prevention

- Around-the-clock monitoring by NOC Engineers
- Around-the-clock security access to the facilities

Aventail's Service Delivery Disaster Recovery Plan scope is focused around three disaster scenarios:

- Loss of CPE
- Loss of Aventail.Net Data Center or connectivity to CPE
- Loss of Aventail.Net Network Operations Center or NOC connectivity to CPE

Written assurance that the service is managed in a secure and responsible manner and in keeping with industry practices.

Aventail will complete the SAS-70 certification process in 2002.

A description of support levels available, including escalation procedures and the associated costs.

Aventail offers a premium level of support to all service customers. Errors are prioritized as Level 1, Level 2, or Level 3. For Level 1 and Level 2, Aventail will respond within 15 minutes. Aventail follows the following escalation procedures for Level 1 or Level 2 errors:

If the NOC has not diagnosed the cause of the error within 15 minutes, the error will be escalated to Tier 3 engineering. Aventail Engineering resources will immediately be assigned to resolve the Error.

If the Error is not resolved within 60 minutes of notification, then the NOC will notify the NOC Manager, the Tier 3 Manager, and the Customer's designated contact.

If the Error is not resolved within 120 minutes of notification, then the NOC Manager or the Tier 3 Manager will notify the Aventail Operations Director, and the Aventail Technical Account Manager assigned to Customer.

If the Error is not resolved within 240 minutes of notification, then one or more of the Aventail Technical Account Manager, Aventail Operations Director, or NOC Manager will notify Aventail's executive staff as well as the Customer's Business Sponsor.

For Level 3, Aventail will respond within 2 hours and a fix or workaround will be delivered as soon as practical and there is no escalation procedure.

Service level agreements pertaining to service availability and support times. In addition, we need a description of remediation in the event of SLA violation.

The Aventail.Net managed services are backed by a broad set of service performance guarantees bounded by contractual commitments and backed by financial penalties. These Service Level Agreements (SLAs) cover:

- 99.9% Service Availability—The systems supporting the core operation of the service, but outside of user access, such as the availability of systems management functions.
- 4 Hour Access Policy Changes—The SLA guarantees that Aventail applies major changes to the Aventail ExtraNet and/or Aventail ExtraWeb access policies (e.g., the

addition or deletion of a new applications or user groups) within 4 hours, but changes typically are implemented within 10-15 minutes.

In the event of an SLA violation, each month in which Aventail fails to meet a Required Service Level, Aventail will provide Customer with a Service Level Credit.

A listing of certifications technicians currently have or are actively working towards and a percentage of the workforce with certifications.

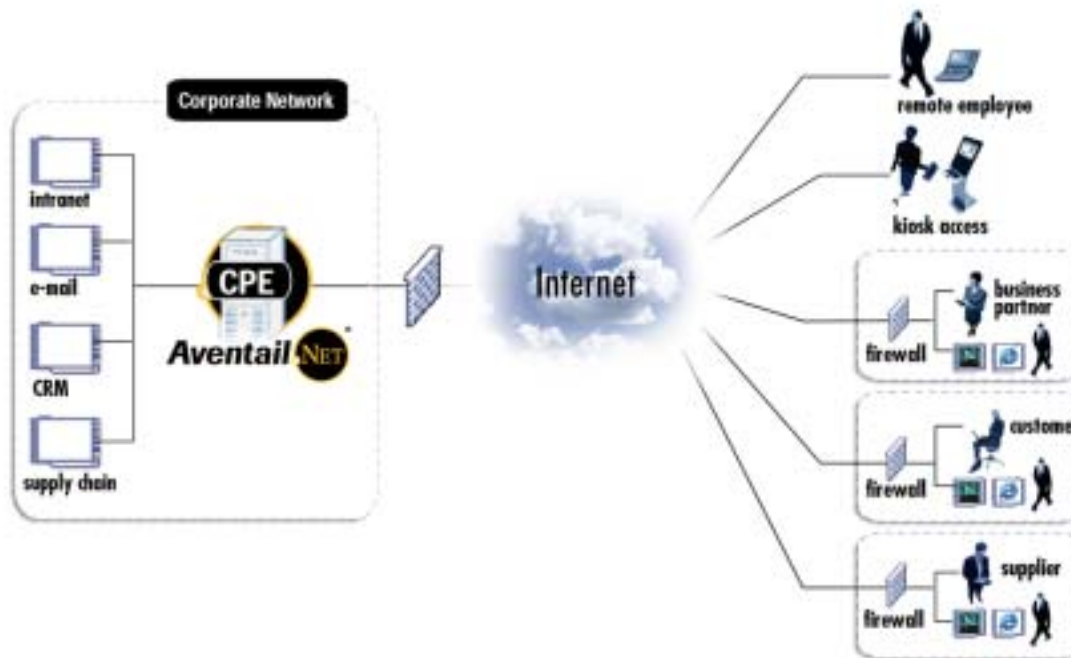
20-30% of Aventail's operations and engineering technicians currently have or are actively working towards the following certifications: MSCE, CCNA, and/or CISSP.

Pricing broken out by fixed and variable costs on a periodic bases. Please provide pricing denoting initial installation price and an ongoing costs for a user base of 1,000.

The initial installation price for the Aventail SA-1000 is \$25K with an ongoing fee of \$5/per user, per month. Additional fees apply for directory management and synchronization, end-user support, help desk to help desk support, and multi-nodes.

The Aventail.Net™ Managed Services

Aventail defines secure access in a comprehensive way, which we solve with our integrated platform. Our services are built upon the vision of Anywhere Access: any user, from any device, from any network. We look forward to working with Network Computing in addressing your specific needs for secure, anywhere access.



Aventail takes a modular approach to its services. That way, you can purchase exactly the services you need to address your business issues and still know that each service module is fully integrated with the others you require.

All Aventail.Net services start with our Aventail technology platform as their foundation. While not a standalone service, the Aventail technology platform contains the central technological and operational elements delivered with all the services, such as our appliances and our round-the-clock service monitoring. Because our services are standardized on the Aventail technology platform, Aventail can bring its customers into full production in as few as 4 weeks, making your time to benefit as short as possible.

On top of the Aventail technology platform are add-on services – Aventail.Net Managed Directory, Aventail.Net User Management, Aventail.Net End-User Support, and Aventail.Net Roaming Internet Access – so we can more fully meet your specific needs.

This modular structure enables us to propose a solution particular to the needs of Network Computing.

Service Deployment Timeline

As part of every managed appliance, Aventail provides a project team to implement the service. In every implementation, an appliance is installed and configured according to the customer needs and requirements. Known as the service deployment project, it consists of on-site and remote activities for planning, design, implementation, test, and rollout. Depending on the Aventail solution – the Aventail SA-1000 or the Aventail SA-9000 – customers can be activated in as little as 4 weeks. Should the customer require additional time due to organization or business reasons, the customer has the option to purchase additional consulting services.

Project Phases

The service deployment process consists of the following six phases:

Requirements. Gather information from both the business and technical perspective to enable accurate development of a design that meets current needs and can scale beyond the lifecycle of the current project.

Design. Develop a detailed solution that meets requirements including hardware needs, capacity planning, likely future requirements, and functional processes.

Configure and Test. Implement hardware/software and build a test environment to test applications selected by customer (as identified on the Customer Application List form) for managed service functionality.

Deployment. Install the production hardware/software into customer's data center environment.

Validate. Develop and provide critical customer documentation. Provide validation of all managed services Web sites. Confirm readiness for production startup with the customer.

Production. Enroll the first end user group per rollout plan. Introduce Aventail.Net network operations procedures and contacts.

