WHITE PAPER

Secure Data Center Access

Authentication and Encryption

Secure Web-to-host TCP/IP access with any 'tn' server

November 2001

Table of Contents

Need for Data Center Security

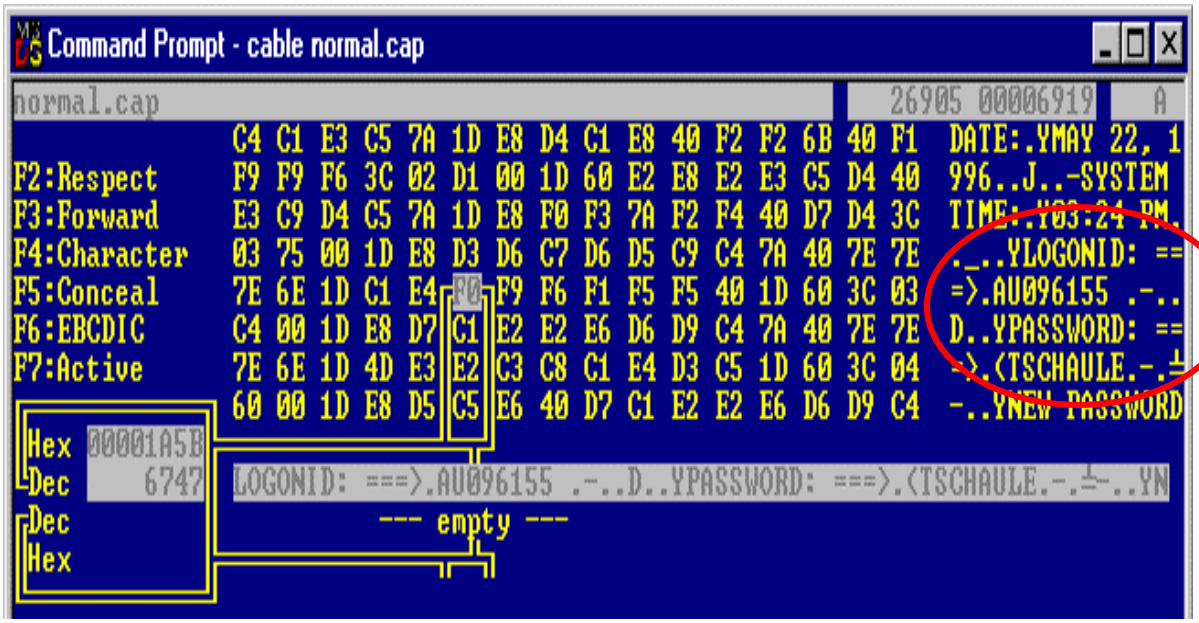
Security is, without doubt, the paramount concern when considering the provision of data center access across non-private networks – in particular the Internet. This attention to security is understandable and very appropriate. With at least 60% of vital corporate data resident on mainframes and AS/400s, data centers are the bastions of commercially sensitive assets critical for the sustenance of global enterprise. Unauthorized access to data center resources can thus result in serious financial misappropriations, loss of valuable customer records, the compromise of confidential corporate data and a general forfeiture of a competitive advantage. With so much at stake, implementing a remote access scheme that can compromise data center security can be highly hazardous to an enterprise.

While data centers have always had impressive physical security, and host applications have always required explicit user-ID/password-based logons, network security, vis-à-vis host access, was relatively lax prior to the burgeoning popularity of Web technology-based networking. The fact that the widely used tn3270(E) industry standard, the premier means for mainframe access across today's TCP/IP networks, still does not formally address security issues such as end-to-end encryption is a stark testament to the apparent disregard for networking security. Similarly, Microsoft's 'SNA Server', one of the most popular SNA gateways for realizing PC/workstation-to-host access across LAN/WAN, is devoid of any end-to-end networking security features. Networking security was not important in the past because IBM host networks, the so called SNA networks, were the epitome of private networks.

Private networks, within reason, were safe from prying eyes, especially if implemented with 'leased lines'. SNA private networks, even when realized using public

packet switching networks [e.g. Frame Relay or X.25], were considered to be quite secure because such public network services in addition to being provided and managed by a single well respected corporation [e.g. AT&T, MCI, Sprint] also relied on continually variable routes within the overall network that made it difficult to intercept specific transactions. This complacency when it came to host networking security only started to get dented when more and more host access started to occur across LANs and public WANs that were based on open standards – in particular TCP/IP. Suddenly traffic to and from mainframes or AS/400s was no longer secure and confidential even if it contained sensitive information such as ATM machine PINs, credit card numbers, e-commerce transactions or B2B e-business dealings. Host data was flowing across non-secure networks in 'clear text'. Unscrupulous operatives could easily intercept critical information using readily available, and usually no-charge, software-based 'network sniffers'.

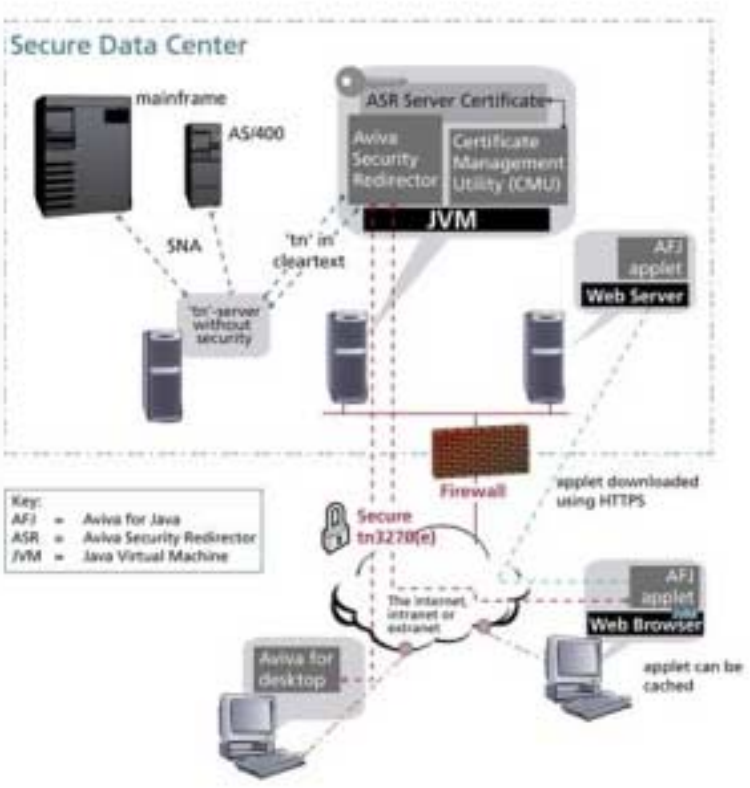
The growing popularity of using the Internet as a strategic means for corporate



User-ID and password to access a mainframe resident application flowing across a TCP/IP network, per the tn3270(E) protocol, as clear [i.e. unencrypted] text – and easily intercepted and deciphered using a readily available software 'network snuffer'.

networking exacerbated this host access security problem since the Internet is the quintessential *'by-the-people for-the-people'* public network – with no designated owner, no accountable operator or enforceable policies related to security. The end users have to provide their own end-to-end security. If they do not, the data they transmit across the Internet could easily fall into the wrong hands. Firewalls alone are not the answer.

This absence of standardized end-to-end privacy when it comes to host traffic flowing across TCP/IP-based LANs and public WANs is the rationale for host security products such as **Aviva's Security Redirector ("ASR")**. Aviva's Security Redirector for example provides extremely secure, standards-based user authentication and end-to-end encryption using 168-bit long keys for SNA traffic flowing across any TCP/IP network including intranets, B2B extranets and the Internet. The Aviva Security Redirector, which can be used with all of Aviva's highly acclaimed host access and Web-to-host solutions such as **Aviva for Desktops** and **Aviva for Java**, guarantees that data center security is not compromised due to insecure transactions across the network.



Secure data center access across the Internet, intranets or extranets with Aviva's Security Redirector that provides user authentication and end-to-end encryption.

Security Should Not Preclude Internet-based Host Access

The potential security hazards associated with using the Internet should not be used as an excuse for not considering Internet-based data center access because there are unique, incontrovertible and significant benefits to this approach – and air-tight, end-to-end security can be enforced thanks to solutions such as Aviva's Security Redirector. Just some of the proven benefits of using the Internet for data center access, as opposed to using private or public packet switching networks, include:

1. at least a 90% reduction in remote access costs!

2. Web Browser-invoked 'thin client' host access solutions [e.g. Aviva for Java] that will typically reduce installation, maintenance and upgrade costs, compared to traditional host access schemes

3. ability to easily provide '*near zero cost*' public-access 'self-service' host applications for home banking, online investing, personal travel reservation, e-commerce transactions, package tracking etc.

4. the economical implementation of electronic Customer Relationship Management (CRM) systems with worldwide reach and universal access

5. realization of standardized, inexpensive and high-efficacy B2B systems such as '*just-in-time*' Supply-Chain-Management

6. eliminate lost opportunity costs through 'near instantaneous' remote access enablement – compared to the 2 to 3 week lead-times required to provide remote access 'ports' and authorization with traditional remote access schemes

7. uniform worldwide access with the same technology and products

8. higher speed communications, maximizing transaction processing volumes, compared to the sub-56Kbps links commonly used to implement host networks in the past

9. higher end user productivity made possible through the user interface rejuvenation schemes typically provided with Browser-invoked 'thin-client' host access solutions

10. ability to transition away from the expensive IBM 3745 and 3746 FEPs used to realize SNA networks for mainframes towards much lower cost mainframe networking solutions such as IBM's OSA-Express or Cisco's 7xxx/CPAs.

Given these unparalleled and compelling benefits of Internet-based data center access it is not surprising that enterprises around the globe are anxious to migrate away from private and packet switching networks to a Web-to-host approach. The ROI, without doubt, is guaranteed, quick and spectacular. The impediment, up until now, has been the concerns about compromising data center security. Aviva has the solution.

Secure Sockets Layer – The Proven Solution

Secure transactions are obviously possible across the Internet. On any weekday over a billion dollars worth of financial transactions are securely and routinely conducted over the Internet. These transactions involve online investing, b2b funds transfer, e-commerce purchases from the likes of Amazon.com, electronic travel reservations, online banking and even electronic tax payments. The security for much of these highly sensitive transactions is provided by a highly trusted security mechanism called SECURE SOCKETS LAYER (SSL) that was developed by Web Browser pioneer Netscape Communications c. 1996.

SSL is ubiquitous on the Web. It is supported, with gusto, by all popular commercial Web Browsers [e.g. Microsoft's Internet Explorer] and Web Servers [e.g. Microsoft's Internet Information Server (IIS), the 'open software' Apache Software Foundation's Apache HTTP Server, IBM's HTTP Server etc.]. The little locked padlock icon that gets displayed at the bottom of a Web Browser window when a secure transaction is being performed indicates that the security in force has been supplied via SSL technology.

That little locked padlock icon indicates that Web Browser to Web Server security, invoked via SSL, is in effect.

Whenever the locked padlock icon is displayed, the 'address' field at the top of the Browser showing the URL invoked is likely to say 'https://www. *etc. etc.*', rather than 'http://www. *etc. etc.*'. The "s" following the HTTP denotes SSL – and in this case HTTP with SSL. Consequently SSL is not something new or rare. SSL is the basis for most of today's client-to-server security on the Web.

SSL is the basis for the Aviva Security Redirector. The Aviva Security Redirector thus ensures that mainframe and AS/400 transactions across the Internet are protected with the same proven and trusted technology used by contemporary Web-centric e-commerce and e-business applications. So think of the Aviva Security Redirector as a means of uniformly adding SSL-based end-to-end security to Web-to-host applications -- irrespective of the 'tn' server you intend to use.

What You Get with SSL

SSL is a Transport Layer [i.e. Layer 4] protocol. As such it provides authentication, integrity and data privacy for applications running above the TCP Layer [i.e. Layer 3]. SSL supports Digital Certificates – where a digital certificate is an electronic credential issued by a trustworthy organization [e.g. VeriSign] and vouches for an entities' identity following repeated password-based verification conducted using Public Key Infrastructure (PKI) mechanisms. Digital certificates are considered by most experts to provide a very high degree of certainty as to a claimant's identity.

Given that SSL works between a client and a server, SSL uses digital certificates to authenticate the server and the client – where client authentication may in some cases be optional. This authentication process, which is achieved via what is referred to as an 'SSL Handshake', typically requires a User-ID/password exchange – with the User-ID and password being conveyed in encrypted mode using a public key. Following this authentication process, the SSL protocol sets about negotiating a common encryption scheme acceptable both to the client and the server. SSL *per se* does not do end-to-end data encryption.

Providing end-to-end, client-to-server encryption was never a goal of the SSL protocol. There are well established industry standards [e.g. 56-bit DES and 168-bit triple DES] and commercial ciphers [e.g. RSA Security] for enforcing end-to-end security. What SSL does is negotiate an encryption scheme acceptable both to the server and the client [e.g. triple-DES] – and then invoke this mutually accepted encryption scheme for encrypting the data flowing between the client and the server. Thus the security services provided by SSL can be summarized as: server authentication via digital certificates, optional client authentication with digital certificates, acceptable encryption scheme

negotiation between the server and the client, and invoking the accepted encryption scheme to ensure that the data flowing between the client and the server is indeed encrypted on an end-to-end basis.

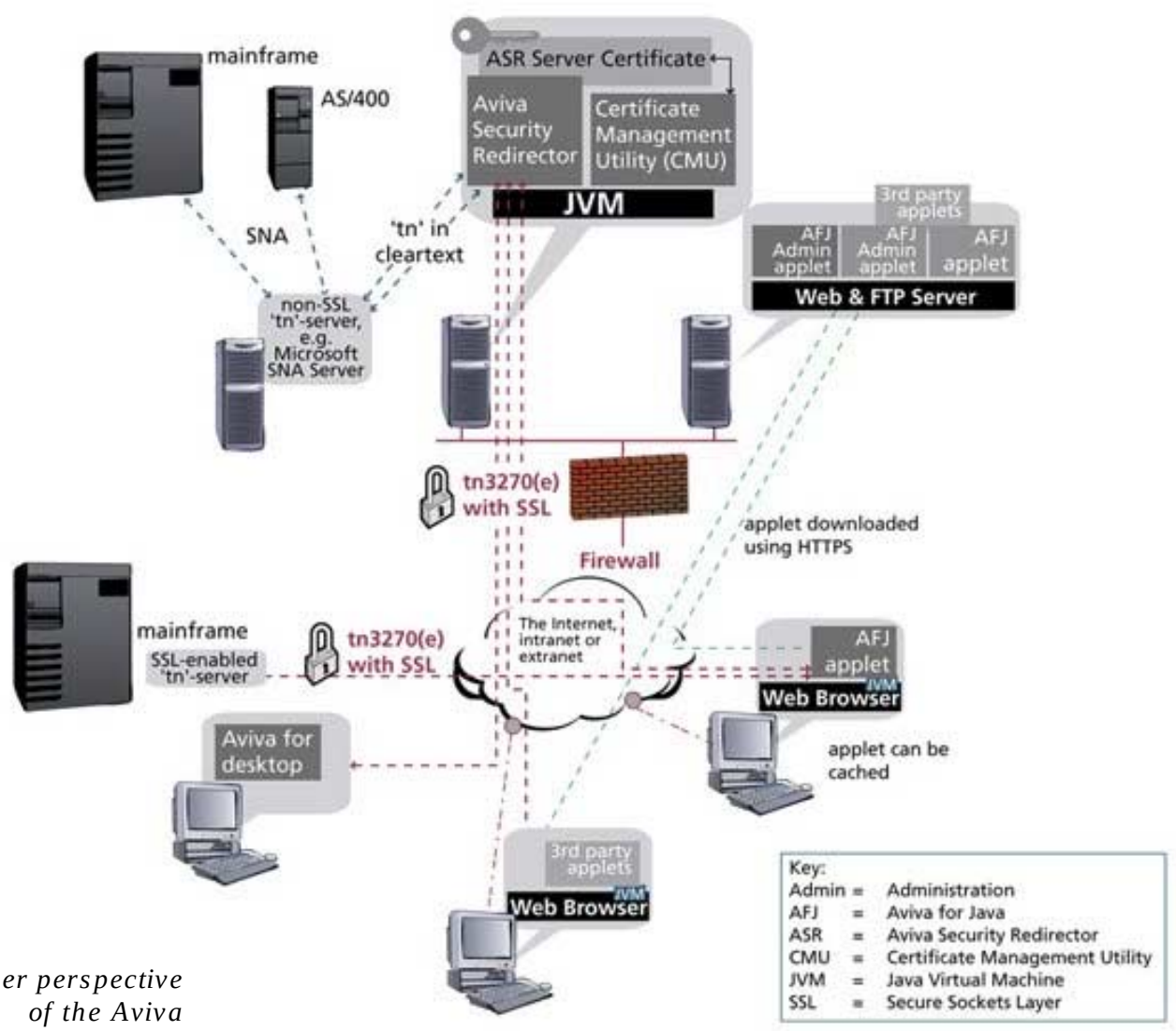
SSL and 'tn'-based Host Access

The initial Web-to-host products hit the market during the latter half of 1996. By 1997 many companies were becoming convinced of the irrefutable cost benefits of 'thin-client' based Web-to-host access across the Internet. However, the 'tn' standards that specified the optimum protocols for data center access across TCP/IP networks did not as yet include any security mechanisms whatsoever! IBM, which obviously has a huge vested interest in ensuring unimpeded data center access, took the bull by the horns at this juncture and added SSL v3.0 based server authentication and end-to-end encryption to its Java applet-based Web-to-host offering in late 1997. By mid-1998 most other leading vendors, including Aviva Solutions [then known as Eicon Technology], followed IBM's lead.

Today, SSL, without question, is the *de facto* standard for 'tn'-based data center access. Some 'tn' servers, in particular IBM's family of cross-platform Communications Server products, do include built-in SSL authentication and encryption technology. However, others, in particular Microsoft's highly popular SNA Server, do not currently support SSL – primarily because the 'tn' standards still do not mandate the compulsory provision of security. Right now the IETF Working Group responsible for the 'tn' standards has essentially handed over the issue to another group dealing with Transport Layer security. The outcome of this is going to be that the standard will eventually advocate 'tn' security per a standard referred to as "Transport Layer Security" (TLS). This is not a problem since it has already been determined that TLS v1.0 will be compatible with SSL 3.0. Thus SSL is the security standard for 'tn'.

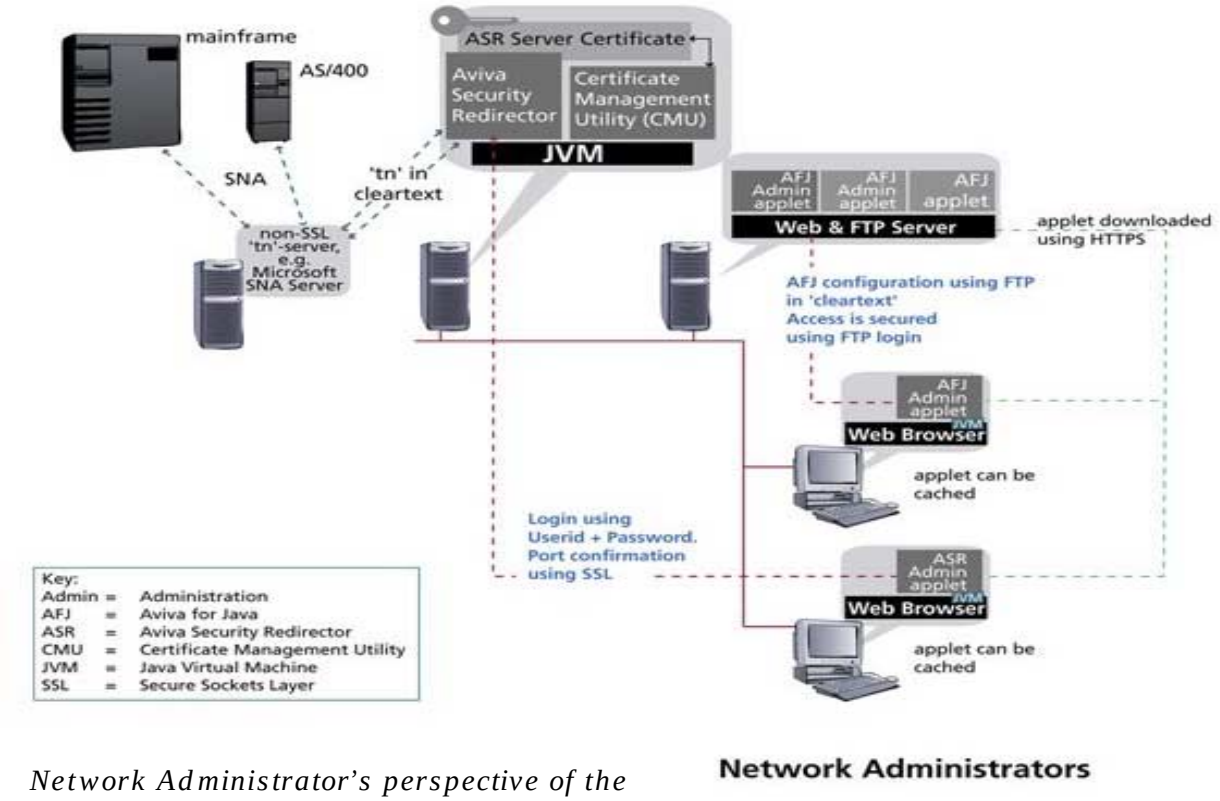
The Aviva Security Redirector

The Aviva Security Redirector is a platform-independent, Java-based, generalized solution for SSL-based security for 'tn' traffic. It is a highly proven, trusted solution for providing uncompromised security for mainframe and AS/400 traffic flowing across intranets, VPNs, B2B extranets and the Internet. It works with all of Aviva's host access and Web-to-host offerings.



User perspective of the Aviva Security Redirector in action.

The Aviva Security Redirector works with any and all 'tn' servers. It can also work, concurrently, with multiple disparate 'tn' servers. That is the beauty and strength of this data center security solution. There is no need to upgrade, change or rationalize your existing 'tn' servers. The Aviva Security Redirector can be easily incorporated into any existing 'tn' configuration or be an integral part of any new installation.



Network Administrator's perspective of the Aviva Security Redirector deployment and operations.

Think of the Aviva Security Redirector as a shield that foils unauthorized access to host data. With the Aviva Security Redirector in place you will no longer have to worry about sensitive host traffic being intercepted or monitored while traversing the Internet. The Aviva Security Redirector, in conjunction with other standard security measures like Firewalls, makes Internet-based host access more secure than what was possible with traditional packet switching public networks.

About Aviva Solutions, Inc.

Aviva Solutions has been a leader in host access software since 1984. It specializes in developing and marketing leading edge, innovative, feature-rich host integration and Web-to-host solutions for enterprises with mainframes, AS/400s or Unix/Linux servers.

Aviva Solutions helps enterprises that wish to develop new b2b and b2c opportunities that gainfully leverage their existing host applications with zero risk and minimum additional investment – thus delivering quick and high ROI. Security, as illustrated by the Aviva Security Redirector, is Aviva's other area of expertise and specialization. Aviva Solutions can help customers implement solutions that securely deliver host data to PCs, Web Browsers, mobile devices or new e-applications using technologies spanning HTML, XML, WAP and XSLT.

In marked contrast to many other vendors, Aviva Solutions offers a complete homogeneous and integrated family of products that enables the systematic evolution into e-business securely, easily, quickly and affordably. Aviva products have earned an enviable reputation for their simplicity of installation, ease of use and high reliability.

Visit www.avivasolutions.com for more information.