Security Challenges & Concerns in Thin Client / Terminal Server

What is Thin Client / Terminal Server?

A thin client, also dubbed a lean or slim client, is a computer or an application that depends heavily on some other computer (its server) to fulfill its traditional computational roles. Thin client usage results in lower administrative costs and greater security. Since all processing occurs on a server and is centrally managed, the local environment is stateless and the hardware has fewer points of contact with processing activity resulting in a lower probability of error.

The technology when implemented by Microsoft is known as Terminal Server and that by Citrix is known as Citrix XenApp.

In a Terminal Server environment it can be difficult to control the individual traffic flow based on IP Address only. So to enforce policies, the security solution has to include the connection socket, service and user's identity into its ambit.

Security Challenges in Terminal Server

The primary security concerns include:

Productivity Concerns

When the end user is provided with an unbridled access, the productivity always suffers. In a stateless environment, the integrity of the data and the application is always at stake.

- **Unbridled Application Access**: By default business houses give freedom to access internally hosted as well cloud-based business critical applications like:
  - SaaS (Software as a service): Salesforce (CRM), SAP (ERP), Service Desk Management, HR applications.
  - Locally hosted: Lotus iNotes, Microsoft Outlook Web Access (OWA)
- **Uncontrolled Internet Surfing**: In absence of controlled Internet access and accountability, the end users often while away time in unproductive surfing and chatting. Unbridled and un-audited harmful and surfing, downloads, P2P usage and Instant Messaging applications eats into the precious bandwidth that powers business critical applications. Unchecked downloads leads to malware infestation. The organization needs to know who was accessing what sites and as such need a content filtering solution that can audit data for users' online behavior.

Data Security Concerns

Data security is the practice of keeping personal or corporate data protected from corruption and unauthorized access. When there is transfer of sensitive and confidential information, security concerns about data leakage or misuse do arise.

Identity – Inevitable Security Parameter

The IP Address is always static (same) for all users i.e. the terminal server’s IP address. The security enforcer solution will fail to differentiate the user’s request as it always see same IP address in all type of requests coming from Terminal server. In such a scenario where IP addresses is not longer a valid parameter to enforce security policy, establishing the identity of the user becomes more critical and inevitable.
Insider Collusion

There is an increase in cases involving “insider collusion,” by which external cybercriminals partner with insiders who agree to participate in the attack. Often in these types of attacks, a disgruntled insider with access to sensitive information will act as an enabler by providing outside cybercriminals with corporate account information, such as authentication credentials. A majority of internal breaches are caused by regular employees, as opposed to accounting personnel, system administrators or upper management, who traditionally have more access rights to sensitive data. Many times Social Engineering is used to dupe an unsuspecting user to reveal sensitive information unwittingly. These threats are prevalent in traditionally controlled IT environment, but are heightened manifolds in a stateless thin client environment.

Compliance Concerns

Compliance means managed risk in form of meaningful reports. It means taking your business where you want it to go; above all, it means having confidence and minimizing legal risks. Reporting a user’s online activity is the sure and quickest way to establishing compliance. In a stateless environment establishing identity is a major challenge.

All available solutions just provide limited control for Thin Client users, they just control the web surfing.

Cyberoam UTM - Total Security

In order to address the concerns of gaining visibility and controls on user activity in a thin client environment, Cyberoam UTM’s IP Address independent Layer 8 technology has been derived out of the need for a more robust network security paradigm which includes the user’s human identity as part of the firewall rule matching criteria.
By definition, the Layer 8 Technology treats user identity the 8th layer or the “human layer” in the OSI network protocol stack. This allows administrators to uniquely identify users, control Internet activity of these users in the network, and enable policy-setting and reporting by username. It offers instant visibility into "who is accessing what in the Thin Client environment." In doing so, it enables enterprises to meet compliance requirements in addition to facilitating instant action in case of a security breach.

Complete UTM Security Coverage

Cyberoam uses Cyberoam Authentication for Thin Client (CATC) technology to authenticate user transparently for multiple thin client servers. It also eliminates the need of any additional management device to manage multiple Cyberoam CATC deployments.
Consolidated Security Interface

The Layer 8 technology permeates through every security module of Cyberoam UTM. All security features can be centrally configured and managed from a single firewall page with complete ease. Layer 8 binds all the security features to create a single, consolidated security unit and enables the administrator to change security policies dynamically while accounting for user movement in the thin client environment.

Productivity Booster

Cyberoam’s content and application filtering feature mitigates indiscriminate Internet surfing through user and group based custom policy setting, thereby setting access limitations based on time duration and predefined blocked sites across 82+ categories.

The UTM also has a user, time and role-based bandwidth management approach which prevents users from misusing bandwidth for non-productive surfing and downloads. Instant Messaging Controls allow administrators to control who can chat with whom over text chat, webcam, file transfer. Organizations can control applications using standard Port 80, 443, non-standard ports, port hopping or tunnel through encrypted SSL traffic, ensuring Application Security. Application security encompasses usage of social applications Eg., Facebook, YouTube, iTunes, gaming, BitTorrent, P2P applications, Eg. Skype and IM applications based on Time and Layer 8 Identity-based policies.

Mitigating Malware Menace

Cyberoam provides anti-virus and anti-spyware scan in thin client environment over incoming and outgoing traffic over multiple protocols which includes HTTP, HTTPS, FTP, IM, P2P, SMTP, POP3, IMAP, VPN tunnels.

Companion to Compliance

Cyberoam’s iView logging and reporting driven by Layer 8 technology helps pinpoint precise network activity for every user. Its dashboard shows all network attacks on a single screen with up to three levels of drill-down 1000+ reports to investigate the attacks, and the users behind them. This granular and in-depth reporting enables enterprises to comply with regulatory compliance norms such as HIPAA, CIPA, PCI-DSS, GLBA, etc. The reporting module driven by 4-Eye Authentication principle ensures that administrators or other users with a high level of privileges cannot purposely or accidentally access security-critical data on the archive without the consent of a second person.
In a Nutshell

While buying an Internet security solution for Thin Client / Terminal Server the user has to keep the following point in mind:

- Select a central gateway solution that gives an inbuilt centralized management for multiple terminal servers instead of having separate thin client management solution. There are a few solutions that make it mandatory the user to buy additional components to the same effect, which will escalate the total cost of ownership.

- The Internet security solution should be as smooth as possible, to the extent that it should not entail any modification in the browser configuration.

- The internet solution ought to give the complete security coverage. It should support Identity based policy configuration for Web (HTTP/HTTPS/FTP-over-HTTP), Application Filtering (Email, P2P, IM applications and Custom applications) and Native FTP.

- The security solution should support 4-Eye Authentication to maintain key users’ privacy.

- The solution should have an On-Appliance reporting. The reporting feature should not require an additional setup and management.

- Cyberoam UTM Deployment in Terminal Server Environment.