

Kansas Department of Revenue



Presentation to Federation of Tax Administrators

August 11, 2002

Stan Black, Applications Programming Manager



Enterprise Security Officer Responsibilities

- ◆ The senior level IT security manager for the enterprise, reporting to CIO.
- ◆ Oversees the development, implementation and ongoing analysis of the IT security policies and procedures which include Physical, User, Application, System, Data, Network, and Social Engineering Security.
- ◆ Oversees or conducts security reviews, evaluations and risk assessments of existing IT systems to ensure the availability, integrity and confidentiality of stored data.
- ◆ Works with both the IT and Business communities to analyze and design new security strategies and procedures to accommodate new systems under development within the agency.
- ◆ Coordinates independent, third-party review of security measures and certification of IT controls to be in compliance with external requirements.



ESO Responsibilities Continued

- ◆ Establishes user privileges to access services and data based on business need and security qualifications and allows access only with positive user identification and authentication.
- ◆ Ensures that security-related awareness and training are provided to systems users and management.
- ◆ Represents the organization in cross-governmental activity to safeguard and validate information systems security and works with external business partners as necessary to coordinate enterprise security practices.
- ◆ Ensures that audit trails are reviewed periodically and archived for future reference.
- ◆ Initiates protective or corrective measures if a security problem is discovered. 3



Web Based Application Design Documents

Items Covered in Case Study

- ◆ Task Plan / Time Line
- ◆ Application Screen Design
- ◆ Application process Model
- ◆ Secure Internet Architecture

Items Not Covered

- ◆ Back End Processing Model Flow
- ◆ Administrative Tools
- ◆ Marketing Plan
- ◆ Testing Process
- ◆ Production Support



- Home
- Policy Library
- Vehicle
- E-Commerce
- Facts
- Property Valuation
- Alcoholic Beverage Control
- Search
- Contact Us
- Links
- Department of Revenue Home

KDOR Kansas Department of Revenue

WebPay EFT for Alcoholic Beverage Gallonage Tax

This online application provides a secure method to pay your alcoholic beverage gallonage tax. It is a safe, secure, fast and free way to pay your tax.

To access the application you will need:

- Access to the Internet with a Web browser that can handle 128-bit encryption. [Click to check our browser for 128-bit encryption](#)
- A Personal Identification Number (PIN) provided to you by the Department of Revenue

To obtain a PIN simply complete and sign the "Authorization For Electronic Funds Transfer" ([Form EF-101](#)) and mail it to the following address:

Electronic Funds Transfer Unit
Kansas Department of Revenue
915 SE Harrison St
Topeka, Kansas 66612-1508

Should you have any additional questions, please call the Kansas EFT Information Line at 785-295-6893 or 1-800-525-4901.

5



KDOR Kansas Department of Revenue

ABC Gallonage Tax EFT

Employer's Identification Number (9 digits, no dashes)

Personal Identification Number (PIN): (7 digits)

Connection Status: 128

6



ABC Gallonage Tax EFT

Tax Filing Period: Year:

Must enter dollars and cents, including decimals. Do not use dollar sign or commas.

Gallonage Tax Alcohol and Spirits:

Gallonage Tax Fermented Wine:

Gallonage Tax Light Wine:

Gallonage Tax Beer:

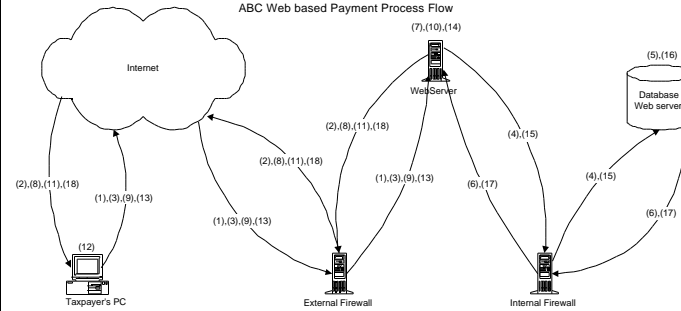
Gallonage Tax CMB:

Your total payment will be the sum of all amounts entered.

Effective Payment Date:



ABC Web based Payment Process Flow



- 1) Connection Request to Web server
- 2) Send Welcome page back to Taxpayer (SSL Encrypted)
- 3) Taxpayer Fills in FEIN and PIN and Transmits back to Web server
- 4) Web server sends FEIN & PIN to EFT server for login Validation
- 5) Web server Does one of the following:
 - A: Denies the Login(6)
 - B: Confirms the Login(8)
- 6) Web server Sends back a Login verification to Web server
- 7) Web server Does one of the following:
 - A: Send Welcome Page with Error Message to Taxpayer if login Failed (2)
 - B: Send the Payment Page to Taxpayer if Login Succeeded (8)
- 8) Web server Sends Payment Page to Taxpayer
- 9) Taxpayer Fills in and returns payment information to Web server
- 10) Web server does computations, and validates payment info and does one of the following:
 - A: Send the payment page to the taxpayer with a message explaining error(8)
 - B: Send the taxpayer verification page to the taxpayer for them to review(11)
- 11) Web server sends the taxpayer verification page to the taxpayer
- 12) The Taxpayer Does one of the following:
 - A: Taxpayer Verifies the Payment Information is correct and returns the verification Page to Web server (13)
 - B: Taxpayer notices a mistake and sends a request to Web server to Modify the payment(13)
- 13) Taxpayer Returns the Verification Page
- 14) Web server does one of the following based on the Taxpayer's last request:
 - A: Send the Payment page to back to the taxpayer for modifications(8)
 - B: Send the Payment(s) data to Web server to create the Payment(s) (15)
- 15) Web server sends the Payment(s) data to Web server to create the payment(s)
- 16) Web server Writes the Payment(s) to the Database and Generates a Confirmation Number
- 17) Web server Sends the confirmation number to Web server
- 18) Web server Creates the confirmation page and sends it to the taxpayer along with their payment information



Single Firewall Design

Benefits

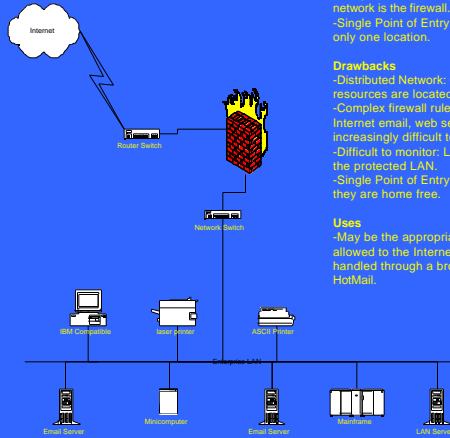
- Simple Design: All traffic in and out of your network is managed through rules established at one firewall.
- Inexpensive: The only device you are adding to the network is the firewall.
- Single Point of Entry-Requires that traffic be monitored at only one location.

Drawbacks

- Distributed Network: Only works well if all enterprise resources are located on the same LAN.
- Complex firewall rules: punching holes in the firewall for Internet email, web servers, ftp servers, etc. can become increasingly difficult to manage and understand.
- Difficult to monitor: Lots of Internet related traffic exists on the protected LAN.
- Single Point of Entry: If a hacker gets through your firewall they are home free.

Uses

- May be the appropriate solution when the only access allowed to the Internet is web browsing and Internet mail is handled through a browser based provider like AOL or HotMail.



9



Linear DMZ Firewall Design

The Linear DMZ provides an isolated Firewall to all Internet access. The DMZ should receive high traffic rate activity outside the internal LAN.

Benefits

- Very Secure - "2 Door" approach. The Most valuable network assets are protected behind two firewalls that must be breached.
- Establishes DMZ - All traffic in and out of your network is managed through rules established at the backend firewall. DMZ traffic is managed at the forward firewall.
- Segments Network - Reduces Internet-based traffic on the enterprise LAN.
- Access to Shared Resources - Mainframes and other shared resources can exist in the DMZ allowing them to be shared with other parts of the enterprise without allowing their traffic on your network.

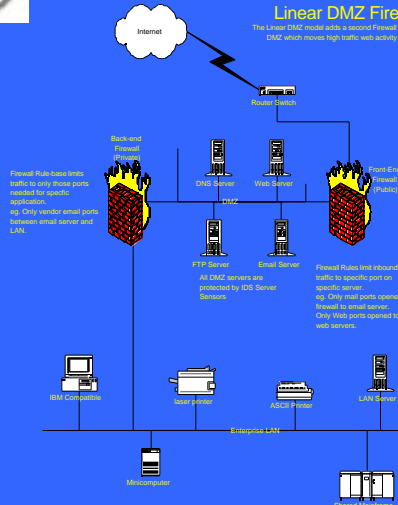
Drawbacks

- Complexity - IP Routing Rules for Firewalls can be difficult to manage for multiple DMZ applications.
- Complex firewall rules - Holes are required in back-end firewall for access between DMZ applications and network assets and data.
- More Expensive - Requires 2 Firewalls.
- Traffic Management - User browser traffic is all routed through the DMZ.
- Failover - Dynamic failover would require 2 backup firewalls. Manual failover using 1 backup firewall more practical. Dynamic failover requires an actively running firewall configured with the same rule base and a high availability module to be sitting idle until failure of the primary firewall. Manual failover requires a non-active firewall with no rule base. This firewall would be put in the place of a failed firewall and quickly setup from backup configuration files with same IP addresses, routing table, and rule base as the failed firewall.

Uses

- A very secure solution that may be suitable for relatively static environments. In dynamic environments it may become difficult to effectively manage changes to the DMZ due to complex routing requirements.

IDS Network monitored between the Firewalls and the Enterprise Network-checks traffic attempting access to the net. No Network monitoring on DMZ/IDS is Server-based monitoring Server activity.

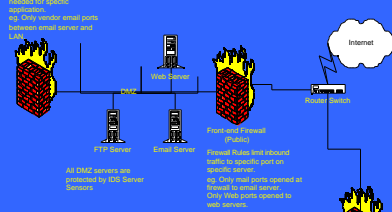


10



Multiple Firewall Design

Back-end Firewall (Firewall)
Firewall Rule-base limits traffic to only those ports needed for specific services.
eg. Only render email ports open to mail server and LAN.



Front-end Firewall (Firewall)
Firewall Rule-base limits traffic to specific ports on specific servers.
eg. Only mail ports opened at DMZ to mail server. Only Web ports opened to web servers.

All DMZ servers are protected by IDS Server Sensors.

DMZ Server, Mail Mailbox, Mail Server, Mail Transfer, LAN Server, Microcomputer, Mainframe

- Benefits**
- Very Secure** - "2 Door" approach. The Most valuable network assets are protected behind two firewalls that must be breached. Separating user TCP/IP traffic from DMZ traffic allows for better monitoring of the DMZ and Enterprise LAN for suspicious activity.
 - Unbreak DMZ** - All Application and email traffic in and out of your network is managed through rules established at the front-end firewall. DMZ traffic is managed at the front-end firewall.
 - Segment Network** - Reduces Internet-based traffic on the enterprise LAN. Browser-based traffic routed through 3rd firewall. Easier to manage performance sizing by separating browser and application traffic.
 - Access to Shared Resources** - Mainframes, DNS and other shared resources can be accessed through the user firewall allowing them to be shared with other parts of the enterprise without allowing their traffic to your network or exposing the DMZ.
- Drawbacks**
- Complexity** - IP Routing Rules for Firewalls can be difficult to manage for multiple DMZ applications.
 - Complex firewall rules** - Rules are required in back-end firewall for access between DMZ applications and network assets and data.
 - More Expensive** - Requires 3 Firewalls.
 - Follower** - Dynamic follower requires 3 backup firewalls. Manual follower using 1 backup firewall more practical. Dynamic follower requires an backup routing firewall configured with the same rule base as each primary firewall, sitting idle until failure of a primary firewall. Manual follower requires a non-active firewall with no rule base. This firewall would be put in the place of a failed firewall and quickly swap from backup configuration files with same IP addresses, routing table, and rule base as the failed firewall.

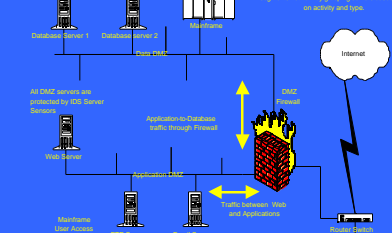
Uses
-A very secure solution that may be suitable for relatively stable environments. In dynamic environments it may become difficult to effectively manage changes to the DMZ due to complex routing requirements. Accessing shared assets through separate user Firewall improves load management and security monitoring and simplifies routing configurations.

IDS Network monitored between the Firewalls and the Enterprise Network-checks traffic attempting access to the net. No Network monitoring on DMZ-IDS is Server-based monitoring Server activity.



Multiple DMZ Design

Select IP routing configuration complexity by placing DMZ using single firewall sensor implemented by groups servers based on activity and type.



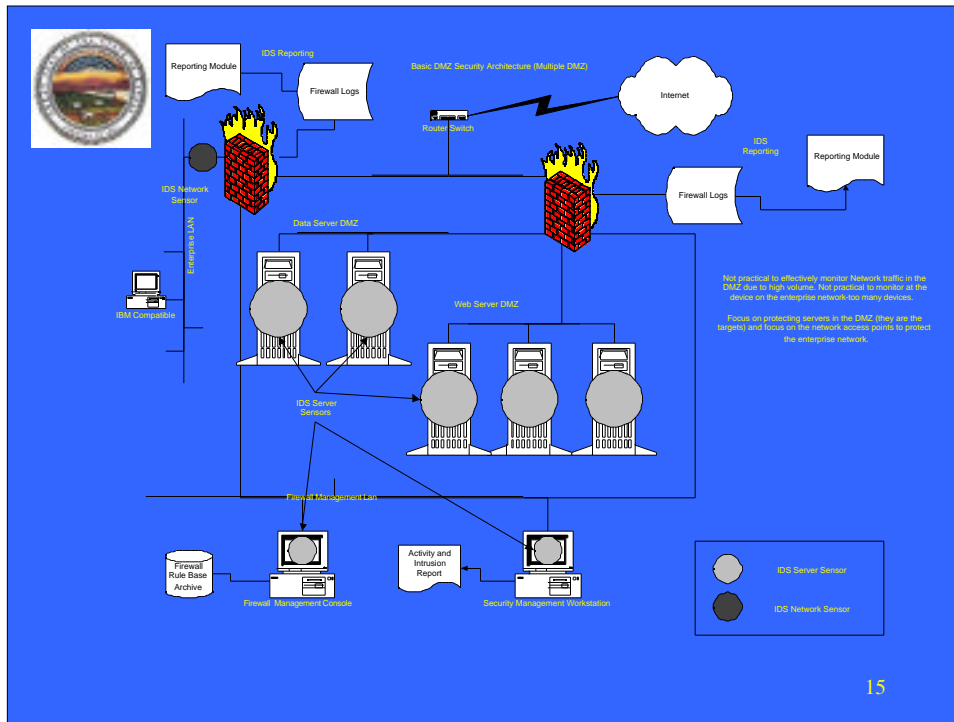
All DMZ services are protected by IDS Server Sensors.

DMZ Server 1, DMZ Server 2, Mailbox, Mail Server, Mail Transfer, LAN Server, IBM Compatible, Application, Microcomputer, Mainframe

- Benefits**
- Resource Isolation** - Communication between front-end web applications and backend data servers, even mainframes, is isolated from enterprise network and user traffic. Don't have to punch those holes in User Firewall.
 - Simplified DMZ configuration** - Using a single firewall to establish multiple DMZ's reduces the routing complexity and cost of multiple linear DMZ's.
 - Intrusion Security** - Single network point to monitor traffic to and from the multiple DMZ's.
 - Cost Effective** - Single firewall to purchase and manage for multiple DMZ's.
- Drawbacks**
- Intrusion Security?** - May be less secure than Linear DMZ's. Only need to hack a single firewall to access entire network. Although routing rule complexity of multiple linear DMZ's is more likely to introduce unknown or unseen vulnerabilities through configuration mistakes.
 - Physical Limits** - DMZ number limited by the number of network interfaces available in the firewall.
 - Single Point of Failure** - Single firewall at the hub of enterprises web-based application portfolio.

Uses
-A secure solution that may be suitable for relatively stable environments. In dynamic environments it may become difficult to effectively manage changes to the DMZ due to complex routing requirements. Accessing shared assets through separate user Firewall improves load management and security monitoring and simplifies routing configurations.

IDS Network monitored between the Firewalls and the Enterprise Network-checks traffic attempting access to the net. No Network monitoring on DMZ-IDS is Server-based monitoring Server activity.



Server Management Single Platform vs Multi-Platform

- ◆ Single Platform- Large server hosting multiple applications
 - Benefits**
 - ◆ Single server to manage
 - ◆ Fewer number of software licenses and configurations to manage
 - ◆ Simple firewall rule base
 - Challenges**
 - ◆ Server maintenance shuts down all applications
 - ◆ Load management difficult as application portfolio increases

- ◆ Multi-Platform-individual servers for each application
 - Benefits**
 - ◆ Servers sized specifically for unique application
 - ◆ Server maintenance brings down only one application
 - Challenges**
 - ◆ Multiple software licenses
 - ◆ Multiple firewall rules to manage



Domain Name Management Considerations

- ◆ Unique Domain Name for each application
 - ◆ Provides maximum flexibility for business community naming preferences.
 - ◆ Allows maximum application branding
 - ◆ Requires multiple domain name registrations
 - ◆ Requires multiple server security certificates

- ◆ Hierarchical Domain Naming
 - ◆ Brings all applications under single domain name structure
 - ◆ Reduces flexibility for business community naming preferences
 - ◆ Limits application branding
 - ◆ Standardizes naming convention
 - ◆ Requires single domain name registration
 - ◆ Requires single server security certificate

17



Port Management Problem Areas

- ◆ OTS and custom software often uses OS ports that are not clearly identified. Locking down ports at the firewall becomes trial and error. *Application developers must learn and clearly identify all services/ports that an application uses. Default of opening up all ports between devices reduces security.*
- ◆ To allow proper application flow through firewalls, required services/ports must be identified on a per server basis if the application accesses multiple protected hosts. *Firewall rule base supports port management at the device level.*
- ◆ Servers' patch levels must be checked at least weekly to insure any new hacks identified for open ports have been patched against. *Typically patches are applied after three days of general availability. This keeps the server farm current, but limits the installation of unstable security patches.*
- ◆ IDS signature files must be updated at least a weekly to insure any new hacks against open ports are identified. *Intrusion detection is only as current as the signature file.*

18



WEB CYBER Threat: Casing the Establishment - Probing

◆ **Typical Intrusion Types**

- ◆ **Footprinting** - Technique used to gather basic information about your network: Determine IP ranges, Domain Names, etc. (www.arin.net, whois, nslookup, traceroute, etc.)
- ◆ **Scanning** - Techniques designed to determine what operating systems and ports are running and reachable through the Internet. (fping, nmap, strobe, netcat, etc.)
- ◆ **Enumeration** - Technique to reach further into the network to identify network resources such as network access shares, printers, users and groups, and running applications. (net use, sid2user, nbtstat, nbtscan, enum, etc.)

19



WEB CYBER Threat Breakdown

- ◆ **Network Attacks**
 - ◆ Denial of Service-DDOS: A high-volume of invalid IP packets that force your systems to respond preventing legitimate traffic from getting through. In extreme cases IP stack failure may allow other hacking tools entry into the network.
 - ◆ Dial-In/VPN system intrusion.: Exploiting a back-door into your local network by identifying and compromising trusted user information.
 - ◆ Router and switch programming: Exploit network device configuration by hacking the security of LAN devices to either take over the device or fool the device into treating the traffic as trusted.
- ◆ **Operating System Attacks:** Gain authority over network servers by compromising server/network login accounts.
 - ◆ Anonymous Log-In attempts
 - ◆ Password cracking utilities
 - ◆ Specific protocol attacks
- ◆ **Software Attacks:** Compromise software running on the network.
 - ◆ Web server software
 - ◆ Data base server software
 - ◆ Email software

20



Intrusion Detection System Management

- ◆ *Signature Files:* Keep IDS signature files updated weekly. Hackers quickly adopt new techniques.
- ◆ *Evaluate each Production server (6-9 Months):* Regularly perform detailed server configuration analysis to confirm patch level, review port configurations, and comb for past hack attempts.
- ◆ *Internal Analysis:* Annually review application work flow and port communications to analyze application security and vulnerability.
- ◆ *Filtering:* Use filtering to reduce false positives.
- ◆ *Blocking:* Maintain listing of all blocked sources and share with enterprise security teams.
- ◆ Review Platform Vulnerabilities
 - ◆ Printers
 - ◆ IIS
 - ◆ SQL Server
- ◆ Reverse Lookup
 - ◆ URL ARINS.NET

21



FIREWALL Intrusion Detection System Button Up Techniques

- ◆ Suspending access
- ◆ Blocking access
- ◆ Filtering to minimize false positives
- ◆ Virus scanning
- ◆ Reverse Footprinting

22



KDOR Internet Security Contacts

- ◆ Tim Blevins, CIO: trb@kdor.state.ks.us
- ◆ Glen Yancey, Technical Architect: gggy@kdor.state.ks.us
- ◆ Stan Black, Applications Manager: stanley_black@kdor.state.ks.us
- ◆ Sean Buffum, Network Manager: sean_buffum@kdor.state.ks.us
- ◆ Stan Weichart, IT Security Officer: stan_weichart@kdor.state.ks.us