DMZ Evaluation

Follow-up Assessment and Recommendations

November 30, 2001

Prepared By:
Jim Hudson
http://www.hudson-family.com/jim-tech/

Prepared For:

Table of Contents

Executive Summary

[COMPANY] requested a follow-up analysis of their On-Line Banking, DMZ network infrastructure. The goal of this analysis is to validate recent performance enhancements implemented by [COMPANY] and to recommend additional enhancements to further improve performance. The On-Line Banking, DMZ network infrastructure includes Internet access through an Internet Service Provider (Sprint), a DMZ (De-Militarized Zone) including Web servers, plus a backend network with database servers, translation servers, and mainframe gateways. This network infrastructure is located in the [COMPANY] building in Raleigh, N.C.

A variety of information-gathering approaches in conjunction with several network analysis tools (i.e. Sniffer, Concord Network Health) were utilized to facilitate this effort. Included in the analysis were operating statistics, component loading, and load balancing. Data network traffic samples were taken from key points in the network for analysis.

This follow-up review provides a very brief "snapshot" of the DMZ, including operational statistics as well as recommendations for performance improvements. The following factors were considered while doing the analysis:

- LAN Infrastructure
- LAN Performance statistics
- Application data flow
- Application load balancing
- Network design best practices
- Network performance best practices

Findings and recommendations from the review of each component are presented. Graphs and charts are presented to highlight network utilization, and other statistics.

1.1 Environment Overview

The fundamental DMZ architecture has not changed since the original analysis in September. Online Banking Internet access is provided via four T-1 circuits to the ISP (Sprint). Three of the circuits are point-to-point T-1 circuits, the fourth is a Frame Relay circuit. These four circuits are connected in pairs to two Cisco model 2514 routers. The routers are connected to two firewalls, which operate in an active and standby arrangement, with only one firewall operating at any given time. The firewalls use Checkpoint Firewall-1 software running on Sun workstations. The firewalls are configured in a three-legged design, with an ISP leg, a DMZ leg and an internal-network leg. In the DMZ two Alteon load balancers distribute Web connections to two sets of four IIS servers. These two sets of servers provide Web connections for various .com services *(service names removed for privacy reasons)*. The Alteon load balancers operate in an active / standby arrangement. The DMZ also contains On-Line Banking login, security and test servers.

Connections to the DMZ servers by outside users initiates additional connections to internal network servers. These connections flow from the DMZ servers, back through the firewall, through a pair of Cisco Local Director

load balancers, and to the internal network servers. The Local Directors also operate in an active /standby arrangement.

1.2 Key Observations and Recommendations

Following are the key observations and recommendations:

- Based of total packet count and Alteon connection statistics, Web traffic to/from the IIS servers was evenly distributed.
- Circuit utilization and router interface statistics indicate that the overall utilization on the primary router and the outbound T1 circuits on that router are above acceptable limits. The Cisco 2514 ISP routers should be replaced with a model utilizing a faster processor and capable of supporting full duplex 100Mb Ethernet, BGP routing and optional support for one high speed serial interface.
- Convert ISP router Ethernet connection to 100Mb, Full Duplex.
- Implement outbound load balancing between routers (RAL-ISP1 and RAL-ISP-2).
- If load balancing across routers cannot be achieved, Increase available ISP bandwidth (by at least double).
- Remove all test and development servers and user workstations from the production DMZ and internal (back-end processing) network. Maintain router interconnectivity and separate firewall between development and production networks.
- Convert the Frame-Relay circuit to a standard T-1 circuit to match the other three circuits.
- Implement monitoring and management tools to provide real-time assessment of network performance and to facilitate remote support and maintenance.

2.0 Performance Observations, Issues, and Recommendations

The operational performance and usage statistics were recorded and reviewed for data network objects in the DMZ and for the ISP circuits. The factors reviewed as part of this project were:

1. ISP Circuits
2. Routers (RAL-ISP-1 and RAL-ISP-2)
3. DMZ Subnet
4. Load Balancers
5. Firewalls
6. Active performance monitoring

The observations and recommendations for each of these are presented in the following sections.

2.1 ISP Circuits

Of the four ISP circuits, two are connected to each of the routers RAL-ISP-1 and RAL-ISP-2. One of the four circuits (on router RAL-ISP-1 port Serial0) is frame relay from the Rocky Mount Sprint POP (Point of Presence), the other three are point-to-point and go to Sprint's Wake Forest POP. Circuit usage statistics are based on the Sprint provided Concord eHealth reports.

2.1.1 Observations

Over the three day period from 11/26/2001 to 11/28/2001, inbound traffic (to [COMPANY]) was evenly distributed across the three T1s from the Wake Forest POP. Virtually no inbound traffic was observed on the Rocky Mount, frame relay circuit. This was expected per design.

Sustained inbound peak utilization of approximately 15% was observed on each of the three circuits used for inbound traffic.

Outbound traffic (from [COMPANY] to the Internet) was evenly distributed across the two circuits on router RAL-ISP-1. Virtually no outbound traffic was observed from router RAL-ISP-2. This was expected as these routers are configured in a non load balancing, Primary / Standby redundancy method.

Sustained outbound peak utilization of over 80% was reported daily from about 8:30am until 12:00pm on the two circuits on the primary router (RAL_ISP-1). Sustained outbound utilization did not drop below 40% until after 5:00pm, daily.

2.1.2 Issues

All outbound traffic is going across two of the four circuits. The other two circuits are under utilized for outbound traffic.

Sustained utilization of over 80% on the two primary router circuits is too high. Sustained peak utilization above 60% can cause traffic congestion and dropped data packets. Due to the nature of TCP/IP flow control, circuit utilization (for Web traffic) has a realistic limit of approximately 80%.

2.1.3 Recommendations

Additional bandwidth is required to bring the average sustained peak outbound utilization to below 60%. An aggregate circuit capacity of 6 Mbps is recommended immediately. The goal of this recommendation is to reduce the number of dropped data packets, and improve response time.

Sustained circuit utilization at or over 80% indicates that additional transmission demands are being buffered (and potentially dropped). As circuit capacity is increased the pent-up outbound traffic demands previously buffered or dropped will be able to use the new capacity. In addition to this, improved response times will cause transaction requests to increase causing still higher demands on the entire DMZ infrastructure until either the transaction volume is satisfied or some other limiting factor is reached. It is difficult to determine how much pent-up demand will be released by simply doubling the available bandwidth. Proactive reporting of circuit utilization, DMZ subnet utilization, response time statistics, router performance statistics, and DMZ server performance should be used to quickly identify or anticipate these limits.

2.2 Routers

Two routers connect the DMZ to the Internet. These routers are both Cisco model 2514 each with two Ethernet (10Mb) and two Serial (T1) ports. The DMZ is attached via 10Mb, half duplex, Ethernet connections running Hot Standby Router Protocol between the routers. RAL-ISP-1 is Primary (active). RAL-ISP-2 is standby. Inbound traffic (from the Internet) is balanced across three T1 circuits (two on router 1, one on router 2). All outbound traffic uses only the active router (usually router 1).

2.2.1 Observations

Based on circuit utilization, LAN utilization and router interface statistics, the overall utilization on the primary router (RAL-ISP-1) is above acceptable limits. Reference the following:

Router RAL-ISP-1

Interface E0	..47.121	no buffer (input)	outbound collisions	outbound deferred
	11/28/01	172	3,418,840	1,904,010
	11/29/01	197	4,041,122	2,239,568
	24 hour Delta	25	622,282	335,558

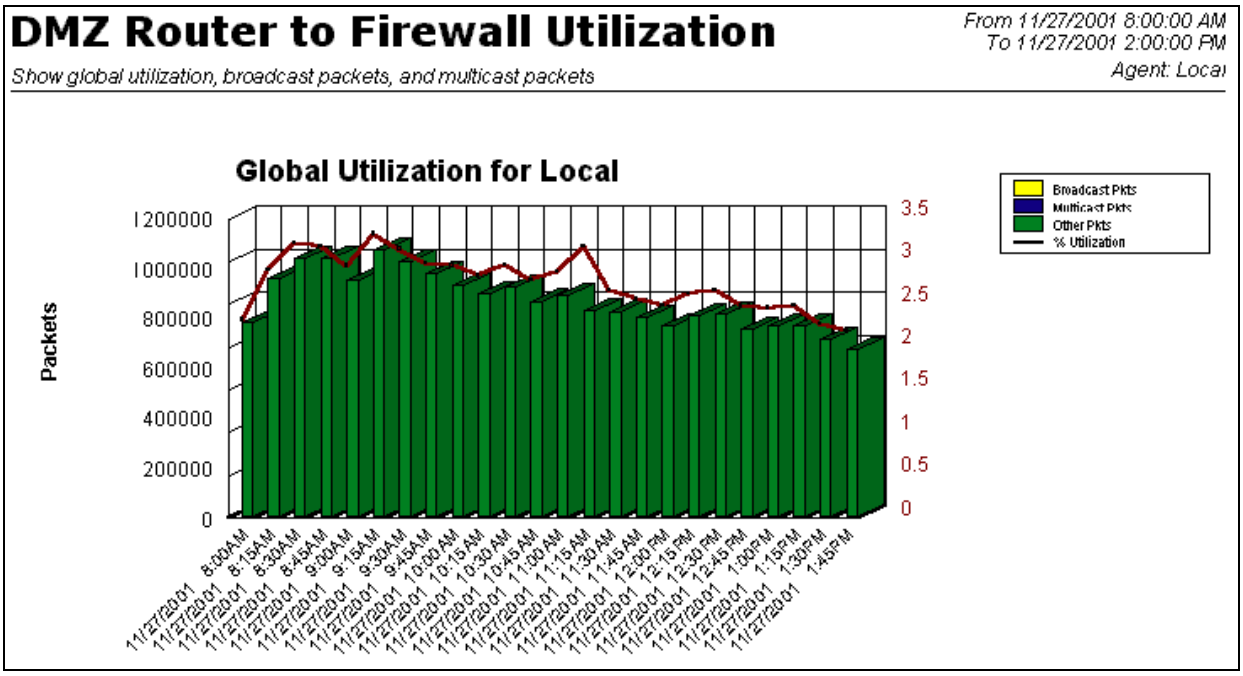
Interface S0	..113.114	no buffer (input)	Input Queue Drops	Output Queue Drops
	11/28/01	-	-	4,924
	11/29/01	-	-	5,885
	24 hour Delta	-	-	961

Interface S1	..160.242	no buffer (input)	Input Queue Drops	Output Queue Drops
	11/28/01	153	213	5,623
	11/29/01	186	253	6,643
	24 hour Delta	33	40	1,020

As shown in the above chart, the router Ethernet interface (E0) has a high number of collisions and deferred packets. This is primarily due to the Ethernet interface only supporting half duplex transmissions, however, this is complicated by high traffic volume.

As indicated in the next chart, the 100Mb subnet between the DMZ Firewall and the Internet router, utilization of 2% to 3% was recorded. This equates to 20% to 30% utilization on the 10Mb Ethernet router interface. The packet rates shown by the green bars on the graph directly correlate to the packets

per second processing requirements on the router. 1,000,000 packets per 15 minutes equals an average of 1,111 packets per second.



2.2.2 Issues

Based on the following:

- Two T1s running in excess of 80% outbound utilization,
- Round-robin load balancing on the outbound traffic,
- 15% inbound utilization on one T1,
- Average of 1000 packets per second processing load,
- 30% utilization on the DMZ Ethernet interface

The 2514 routers are at the limit of their processing capacity.

2.2.3 Recommendations

At a minimum - implement outbound load balancing between the existing routers RAL-ISP1 and RAL-ISP-2 to reduce the processing load on the individual routers.

Replace the existing model 2514 routers with model 3600 routers which support 100Mb, full duplex Ethernet and high speed serial interface connections.

The minimum recommended bandwidth is 6Mbps.

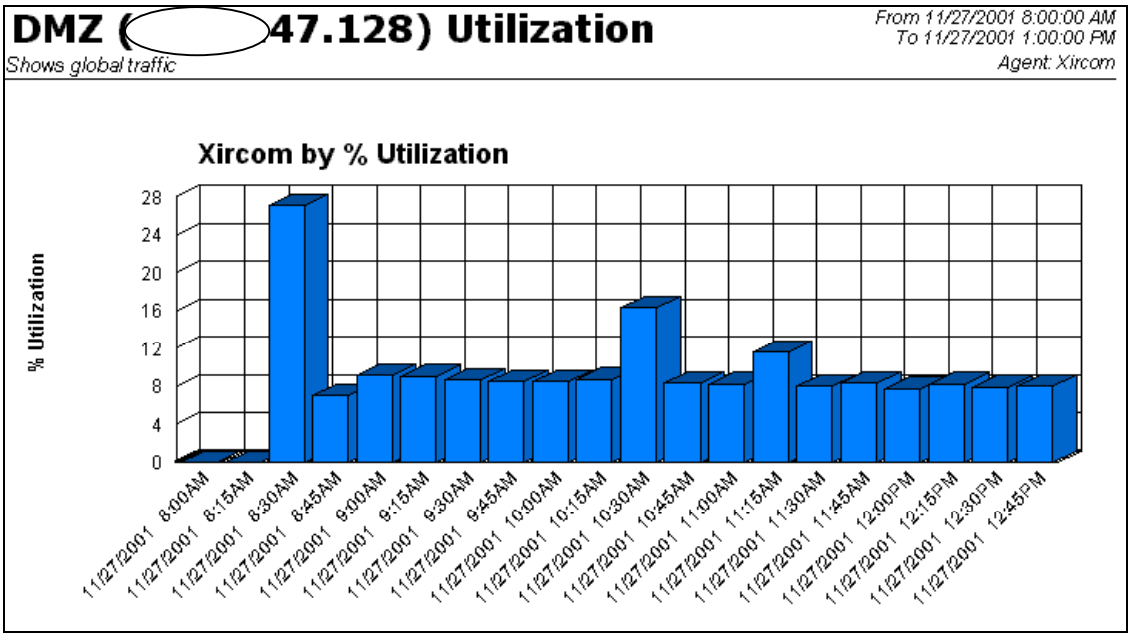
Provide HSRP serial circuit tracking on routers, with weighting to allow for single and dual circuit failures.

2.3 DMZ Subnet

Two Nortel model 450 switches provide connectivity on the DMZ subnet (..47.128). Half of the DMZ servers and load balancers are connected to one switch, half to the other. Subnet utilization was measured via port mirroring on a hub sharing connectivity with the Intrusion Detection Server (IDS). All Web traffic to and from the Internet as well as between the IIS servers and the back-end processes (i.e. SQL database, Mainframe gateways, and Translation servers) must transverse the DMZ.

2.3.1 Observations

As the following chart shows, DMZ traffic averaged about 8% utilization during the peak traffic period of 8am to 12pm.



2.3.2 Issues

There were no issues with the performance on the DMZ subnet.

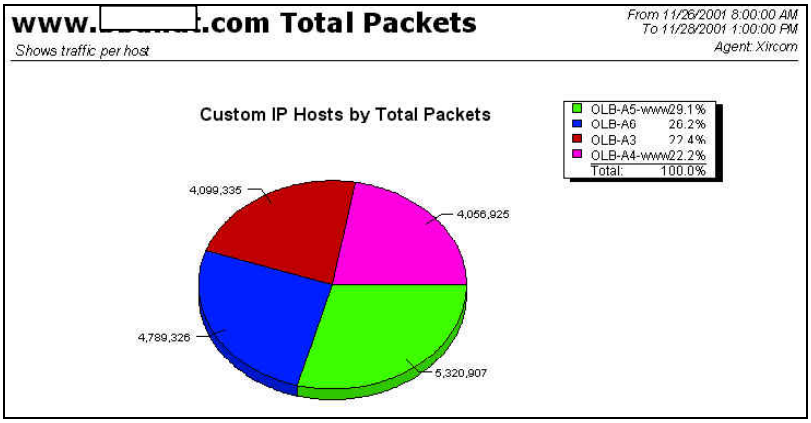
2.3.3 Recommendations

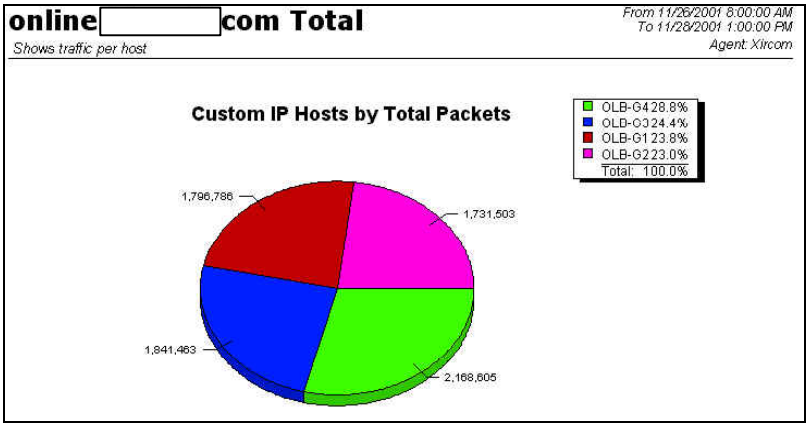
Active monitoring of DMZ utilization and performance should be implemented to report performance statistics and identify potential performance issues.

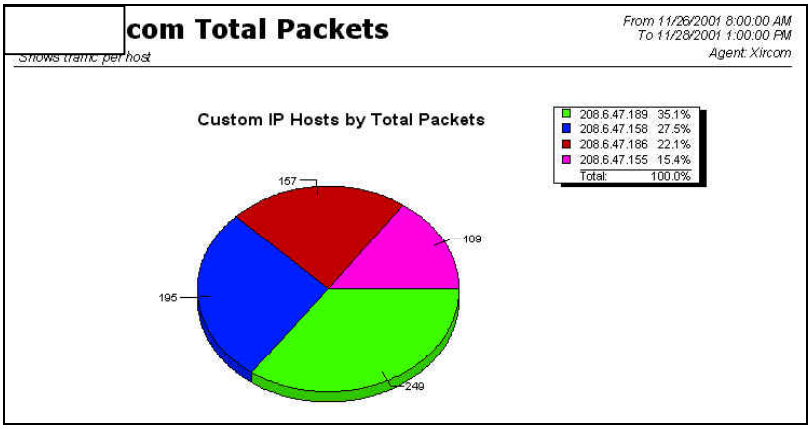
2.4 Load Balancers

2.4.1 Observations

The following charts demonstrate the even session distribution on the IIS servers.







2.4.2 Issues

During data collection, on 11/27, slow response times were observed between the Web server OLBIISA3 (A3) and the SQL cluster OLBSQLA. [IT staff] identified that the MDAC module on server A3 was older than that on the other IIS-A servers (2.0 verses 2.5 on the other three servers). After updating and rebooting the A3 server, SQL response times fell in line with the other three servers.

2.4.3 Recommendations

No recommendations.

2.5 Firewalls

2.5.1 Observations

Through discussions with firewall staff and response time measurements, no significant issues were identified with firewall performance, load, or capacity.

2.5.2 Issues

No issues were identified with performance on the firewalls. This was reinforced by the transaction response times from the "inside" and "DMZ" based ActiveWatch clients (IP Addresses 10.5.20.211 and ..47.134). Both firewall devices indicated only a moderate transaction time increase during the peak period of 8am to 12pm.

2.5.3 Recommendations

The firewall configuration allows for only one default gateway – the active ISP router. Through a combination of router and Unix configuration changes on the firewall, it is possible to force the firewall to load balance across the two ISP routers. This should be tested extensively prior to production.

2.6 Additional Recommendations

- Remove all test, development, staging and QA servers from the production DMZ and back-end networks. (Provide routed network interconnectivity, as required.)
- Remove all user PC's and workstations from the production DMZ network – except for performance monitoring systems. (Provide routed network interconnectivity, as required for maintenance and monitoring.)
- Install Y-cables in serial circuits for future Sniffer use.
- Provide active management, performance monitoring and automated reporting of network equipment and circuits.
- Monitor the Sprint Concord Network Health reports daily to confirm circuit utilization, load balancing and performance characteristics.
- Install distributed Sniffers (or other remote packet capture and analysis devices) for remote monitoring and diagnosis of ethernet LAN's and serial circuits.