SANS Technology Institute
Group Discussion/Written Project

The Rapid Implementation of IPv6 at GIAC Enterprises

12/9/2010

Stacy Jordan
Beth Binde
Glen Roberts

Table of Contents

Executive Summary

GIAC Enterprises is the largest supplier of fortune cookie sayings in the world. Many of the fortunes are authored in China where the company has a presence. The company's customer base is global including a large Chinese contingent.

Connectivity with one of GIAC Enterprises plants in China was recently interrupted due to an agreement with the ISP to return part of the IPv4 allocation and employ IPv6. The team worked with the ISP to reverse the change temporarily for short-term containment, however, the ISP will be taking the IPv4 addresses back within days. As a result, GIAC Enterprises needs to complete a rapid implementation of IPv6. The implementation of an IPv6 solution will benefit all plants as the company makes the inevitable migration to IPv6 in response to the shrinking availability of the IPv4 address space.

This paper will cover the following:

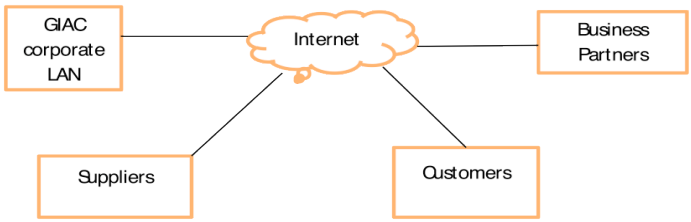
- Background and survey of existing assets which confirms that **we are able to implement an IPv6 solution** with some structural changes.
- IPv6 "bridge" and **interoperability options considered** for our environment.
- An XML schema review that confirms **our XML schema will remain functional.**
- Conclusion which outlines the **recommended solution: using tunneling.**

In addition, a high-level project plan is provided for consideration which can be executed within four days with appropriate approvals.

Background

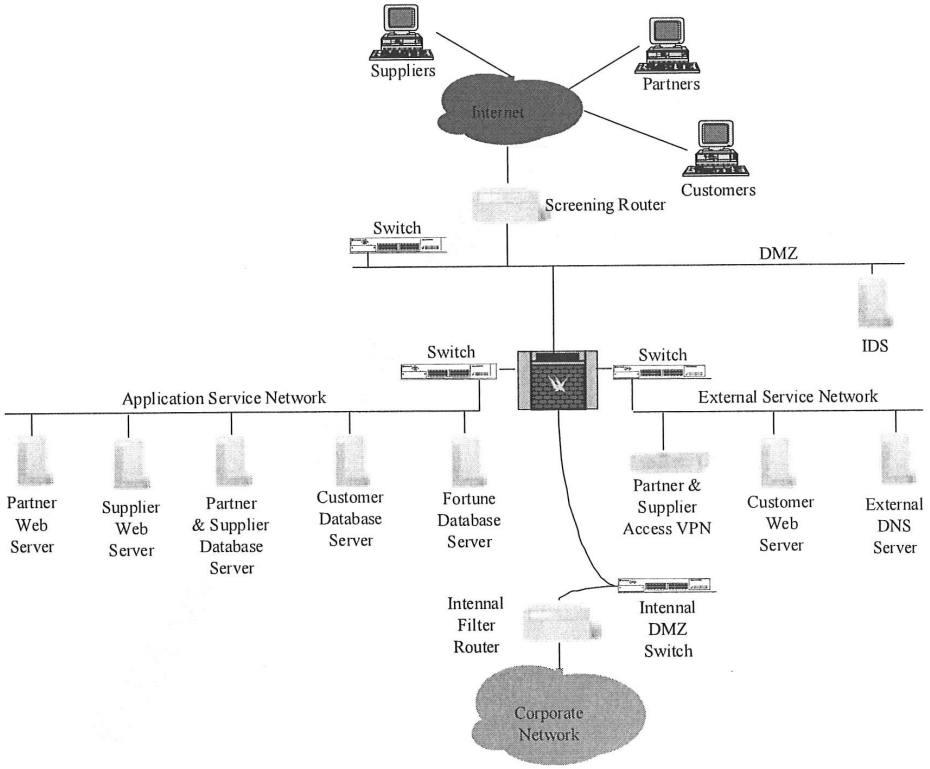
Since the founding of GIAC Enterprises in 1999, the network infrastructure has grown from a small office/home office network to one that supports business-to-business (B2B) transaction processing over the Internet. In the initial GIAC network, VPN access was granted to various entities to provide a basic level of security.

Figure 1: Initial GIAC Enterprises network diagram



As business grew internationally for GIAC Enterprises, the network infrastructure expanded as well. This resulted in the infrastructure design in place today which is separated into three networks: application services network, corporate network and external services network. The application and external networks communicate to each other through a centralized firewall that sends traffic to a switch that separates each network segment. The corporate network is a completely separate environment that obtains access to the Internet through the internal DMZ switch.

Figure 2: Present day GIAC Enterprises network diagram



Survey of Existing Assets

A major task in migrating to IPv6 is to verify components that could be re-used as part of the long-term plan to migrate to IPv6. Because we entered into an agreement with our Chinese ISP that limits the use of IPv4 IP allocation, GIAC Enterprises will need to begin the transition process to IPv6 quickly and with a sense of urgency.

The following access is provided in the current GIAC Enterprise network implementation:

- Customer access via web server to purchase fortunes.
- Partner access via VPN. Once connected via VPN, partners may access an application web server to obtain fortunes for translation, and upload translated fortunes.
- Supplier access via VPN. Once connected via VPN, suppliers may access an application web server to upload fortunes.

- Employee access from the corporate network to perform ongoing maintenance and support on the infrastructure components (Wanner, 2001).

The scope of our project covers the implementation of IPv6 for GIAC Enterprises including the components required to do business with customers, partners and suppliers and the corresponding maintenance activities that must occur to support this infrastructure. It is assumed that employee-related services such as Internet access, email, web access and employee remote access are provided through a different network implementation. The only employee access that will be considered will be the access requirements for supporting and maintaining the E-commerce architecture.

This implementation was designed with the intent to compartmentalize the network into functions based on the nature of the traffic. The DMZ is used as a cushion from the Internet. None of the application services are being offered on the DMZ. This means that there are at least two lines of filtering between the Internet and any servers. The external service network is where all of the Internet-facing services are offered. For example, the web server which customers access to buy fortunes is on this network.

The application services network provides the support services for Internet-facing services. For example, this is where you will find the database servers that contain the fortunes and customer data used by the web servers.

The internal DMZ is used to keep unnecessary and unwanted noise from our corporate network from getting to our external networks. It has been our experience that enough noise is generated on our corporate network (especially from NetBIOS traffic), that it can have an impact on the performance of the firewall. The internal filter router is used to filter this noise (Wanner, 2001).

Infrastructure Suitable for IPv6 Migration:

- Desktops and Laptops - GIAC enterprises has standardized its desktop and laptop operating environment by utilizing Windows Vista Professional. MS Vista Professional natively supports IPv6 and 32-bit operating system environment so older applications can run without a problem.

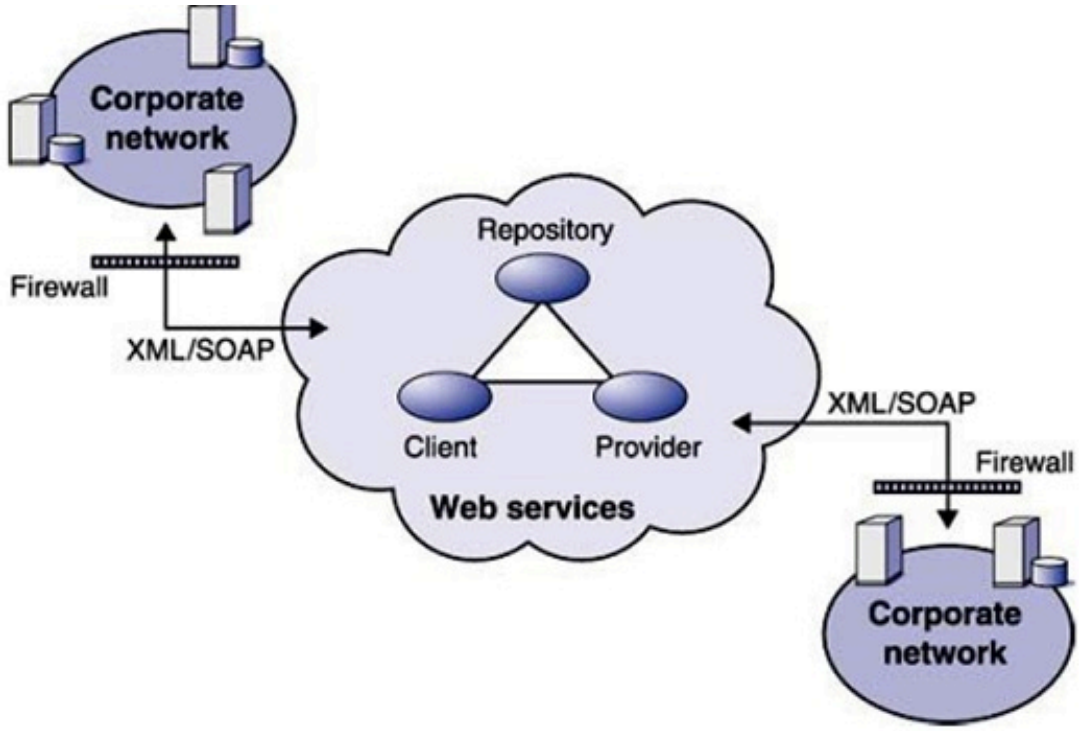
- Routers and Switches - GIAC Enterprises have moved from using Bay Networks to Cisco Systems for their routers and switches. With this migration, all network routers and switches are IPv6 compatible as Cisco IOS has been supporting IPv6 when it released Cisco IOS 12.0. Our screening router is a Cisco 3845 ISR which allows for GIAC Enterprises to add new modules as needed. For the internal filter router, Cisco 3825 ISR has been deployed to handle the workload for our employees. In terms of switches, Cisco Catalyst 6500 series is connected to the screening router while Cisco Catalyst 3500XL series is deployed as end-points to the firewall.

- Firewall - Because GIAC Enterprises has expanded its reach globally, an upgrade to a medium-size Cisco Firewall was in order. Our enterprise has employed another 6500 with a firewall service module (FWSM) that will handle all traffic.

- Web server - All our web servers are running Apache version 2.0 or higher. These versions are compatible with BIND 9 which supports IPv6.
- External DNS server - Our DNS server is built as an HP 6500 workstation running HP-UX 11.23 and BIND version 9.0.
- Intrusion Detection System (IDS) - Our IDS product is ISS (IBM) Realsecure Network Sensor version 7.0 running on a Solaris-7 32-bit server.
- VPN - VPN access is maintained through our Cisco 3500 XL switches that contain VPN modules.
- Database servers - Our database servers are running Microsoft 2003 Enterprise Edition and Oracle version 11 as the database application.

IPv6 and the XML Schema

GIAC Enterprises uses an Enterprise Resource Planning (ERP) system globally to obtain accurate production data from the fortune authors and to feed orders for the right configurations requested by its stores. The ERP system uses SOAP over HTTPS for communication. XML schemas are employed for fortunes and cookies requests and responses.



Internal standards for XML/SOAP at GIAC Enterprises require the use of a Uniform Resource Identifier (URI) rather than hardcoded IP addresses for access to Internet resources. Our code is written in accordance with best practices including W3C markup validation (W3.org, 2010). This is audited within the code approval and change control processes at GIAC Enterprises so there is a high degree of certainty of its standardization (Coyle, 2002).

IPv6 "Bridge" and Interoperability Options

DNS is required to map domain names to network addresses and vice versa. Resolvers query DNS servers for IP addresses. In addition, DNS servers implement a resolver to send DNS queries to other DNS servers. The resolvers on a mixed network must be able to handle both the A record type for IPv4 and the AAAA ("quad A") record type for IPv6. BIND implements IPv6 DNS in versions of BIND 8.4 and higher. GIAC Enterprises' external DNS server is currently running BIND 9.0.

The web servers are configured so that if there is no response for an IPv6 query, it falls back to an IPv4 lookup. Fortunately, Apache already supports this feature. We need a DNS server that can be accessed over IPv4. Windows Vista supports does resolving DNS names over IPv6 (Hagen, 2006). DNS (BIND 9) is configurable to respond appropriately for IPv4 queries vs. IPv6 queries. "Quad A" records will be inserted for local IPv6 hosts (Liu and Albitz, 2006).

Interoperability
Given the extremely tight deadline, we considered the two most viable approaches for implementing IPv6 compatibility within an IPv4 infrastructure: dual stack and tunneling.

Dual stack techniques allow IPv4 and IPv6 to coexist in the same devices and networks. An IPv6/IPv4 node requires at least one network address for each protocol version; this would require extensive DNS and host updates. In a dual-stack network, both IPv4 and IPv6 forwarding is enabled on routers. A full network software upgrade would be needed to run both protocol stacks. All tables (for example, routing tables) would have to be kept for both protocols at the same time; this impacts router performance (Hagen, 2006).

Tunneling techniques allow the transport of IPv6 traffic over the existing IPv4 infrastructure. The advantage of tunneling techniques (also known as encapsulation) is that they can be used to deploy an IPv6 forwarding infrastructure while keeping IPv4 infrastructure in place. IPv6 traffic can be carried over the IPv4 routing infrastructure. Tunneling can be implemented quickly and transparently over the network infrastructure currently in place. Current router hardware and software are capable of supporting the tunneling solution with router configuration changes at the Internet handoff. It permits us to transport IPv6 packets over the IPv4 infrastructure and connect to our remote locations, including China, without upgrading the network backbone first. There is some

additional load on the router (tunnel entry and exit points) as packets are encapsulated to send and decapsulated at the other end of the wire. Of greater concern is the introduction of single points of failure (Hagen, 2006). Hot spare routers on hand would help mitigate this risk.

Conclusion

Tunneling is the recommended solution to meet the given time constraint and avert the immediate crisis with the ISP in China. It is supportable within the current network and software infrastructure. When the IT roadmap permits, we recommend a planned migration to IPv6 across all divisions and geographical locations for a long-term solution. This will be a multiyear project requiring significant resources.

References

Cisco IOS IPv6 configuration guide, release 12.4. (2010). Retrieved December, 2010, 2010, from http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4/ipv6_12_4_book.pdf

Coyle, F. P. (2002). XML, web services, and the data revolution Addison-Wesley, Professional.

DNS, BIND, DHCP, LDAP and directory services. (2010). Retrieved December, 2010, 2010, from http://bind9.net

Liu, C., & Albitz, P. (2006). DNS and BIND, fifth edition (Fifth Edition ed.) O'Reilly Media, Inc.

Apache HTTP server . (2010). Retrieved December, 2010, 2010, from http://projects.apache.org/projects/http_server.html

W3C markup validation service. Retrieved December, 2010, 2010, from http://validator.w3.org/

Wanner, R. (2001). Firewalls, perimeter protection and VPNs. Retrieved December, 2010, 2010, from http://giac.org/certified_professionals/practicals/gcfw/135.php

Hagen, S. (2006). IPv6 essentials, second edition O'Reilly Media, Inc.

Taylor, M. (2009). Securing the enterprise service bus: Protecting business critical web-services. Retrieved December, 2010, 2010, from http://www.sans.org/reading_room/whitepapers/firewalls/securing-enterprise-service-bus-protecting-business-critical-web-services_33084

Appendix - High-Level Project Plan

The following high-level project plan for implementing the proposed solution can be carried out within four days and can also be customized as needed to support business priorities to ensure the least amount of customer impact. System and network change windows will need to be negotiated with the business units in accordance with standard change management procedures including emergency rollbacks.

Day 1:
- Negotiate change window with business units (IT Business Relationship Manager).
- Execute communication plan (IT Business Relationship Manager).
- Verify survey of assets (Network/Systems Engineer).
- Submit Request for Change (Network/Systems Engineer). [MILESTONE]

Day 2:
- Build out test environment for testing the proposed change (Network/Systems Engineer). [MILESTONE]

Day 3:
- Successfully test proposed change in test environment (Network/Systems Engineer). [MILESTONE]

Day 4:
- Implement tunneling solution changes in production environment (Network/Systems Engineer).
- Systems testing (Network/Systems Engineer).
- Successful business validation testing (Business Analyst). [MILESTONE]