Interested in learning more about security?

SANS Institute InfoSec Reading Room

Using Secure Sockets Layer bridging and content filtering mechanisms to provide defense in-depth when publishing SSL encrypted web hosts.

In this paper we discuss the benefits of Secure Sockets Layer (SSL) bridging, also known as SSL initiation, a practice that allows Internet security professionals to successfully proxy encrypted traffic, thus enabling intrusion detection and/or prevention, virus detection, and content filtering of encrypted communications. Until recently it was very difficult to perform these functions cost effectively. Now that SSL bridging technologies are becoming a readily available resource, we will compare these new technologies ...

Using Secure Sockets Layer bridging and content filtering mechanisms to provide defense in-depth when publishing SSL encrypted web hosts.

GSEC practical Assignment v1.4c

By: Jonathan Hallberg.

1/21/05
Revision 1.1

Table of Contents:

Using Secure Sockets Layer bridging and content filtering mechanisms to provide defense in-depth when publishing SSL encrypted web hosts.

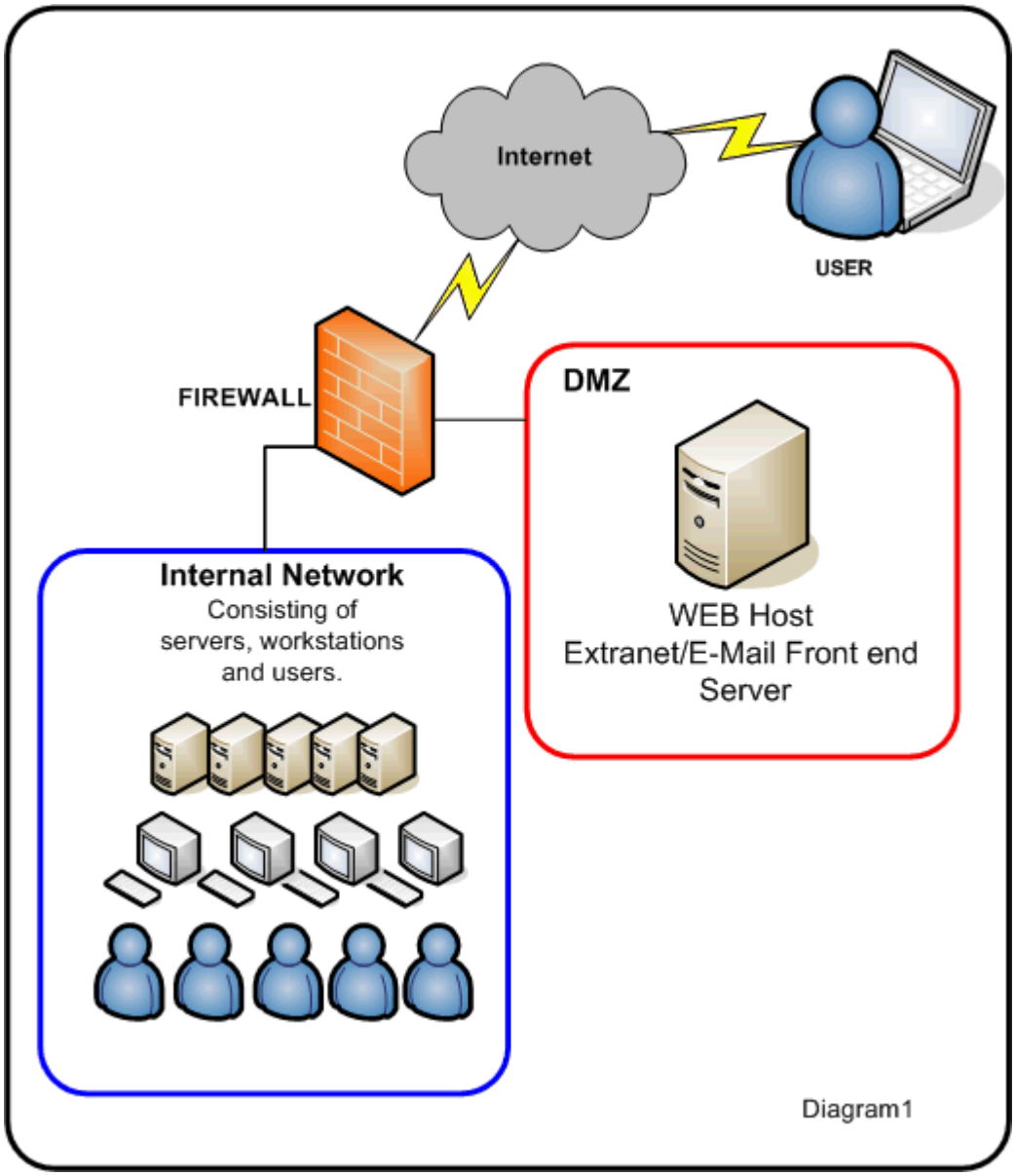
Abstract:
In this paper we discuss the benefits of Secure Sockets Layer (SSL) bridging, also known as SSL initiation, a practice that allows Internet security professionals to successfully proxy encrypted traffic, thus enabling intrusion detection and/or prevention, virus detection, and content filtering of encrypted communications. Until recently it was very difficult to perform these functions cost effectively. Now that SSL bridging technologies are becoming a readily available resource, we will compare these new technologies to previous web deployment best practices. The fictitious "Widgets Company" is used to demonstrate how the addition of SSL bridging technologies can enhance current security tools to better protect their network.

Introduction:
The Widgets Company needs to allow web-based access to corporate data and e-mail so employees can effectively communicate while away from the office. Their IT department has been instructed to deploy the necessary technology to accomplish this.

There are many ways organizations can allow access to their corporate network data via the Internet. There is no single or best way to do this. Every organization's business model differs based on the technology available to them and acceptable risk. However, most of today's industry accepted means rely on the elements of identification, authentication, authorization and a secure method of data transport. For example, sending user or password information in plain text across an unsecured network would not be an acceptable solution.

The use of SSL is the most common cryptographic methodology used to secure sensitive Internet based communications. Invented by Netscape Corporation [1] in 1994, the SSL protocol was designed to provide privacy over an unsecured network (i.e. the Internet). [2] Now in version 3, which provides up to 128-bit encryption, SSL is still the standard for online shopping, web-based e-mail, and many personal finance transactions. Once an SSL encrypted session is established from the user to the host it is safe to send identity, authentication, and data.

Common Web Infrastructure Deployment:
Diagram 1 is the configuration chosen by Widgets. It's typical of small to medium sized organization's web deployment infrastructures utilizing a firewall, an SSL enabled Web server and a Demilitarized Zone (DMZ).



In Diagram1 we can see the Widgets Company's internal network is protected by a firewall. Outside or adjacent to the firewall is a secondary network or DMZ (demilitarized zone).

The firewall is configured as follows:

1:The firewall blocks all outside traffic from entering the internal network. (External→Internal=Denied)

2:The firewall forwards traffic from the outside network to the DMZ based on a set of rules. (HTTPS→WebHost=Allowed)

3:Packets originating from within the DMZ are allowed to pass internally based on firewall rules or policies.
(HTTPS → Internal Host=Allowed)
(HTTPS→ External=Allowed)

4:Packets originating from inside the network are allowed outbound based on a set of rules:
(HTTP→Any =Allowed)
(HTTPS→Any =Allowed)

In their DMZ, the Widgets Company used a commercial SSL enabled web server to publish the extranet/e-mail gateway services. They verified they were running the latest code and applied all necessary service packs. They followed today's acceptable best practices and successfully allowed their remote workers to perform needed functions. Using this configuration, the web based extranet/e-mail gateway server within the DMZ allows authorized users to view web based information from anywhere in the world. Additionally, it enables them to send and receive e-mail as if they were sitting in the Widgets office. The firewall also provides the internal network security from the rest of the Internet. Authorized users can now connect to their corporate data without the need for a formal virtual private network (VPN) connection to the internal or "trusted" network.

Was the deployment a success? Perhaps, but If the Widgets Company sells gizmos to the defense industry, the Widgets' executives want to make sure they are not risking losing sensitive information. Even if the web server containing the extranet/e-mail gateway software has not been compromised and all connections in and out are secure, monitoring traffic during these secure sessions can become a difficult and daunting task for the Widgets' network administrators. Until recently, many network administrators thought it didn't really matter, as the time an attacker would take trying to decrypt SSL data streams was too immense. Additionally, internal mechanisms were already in place to provide an acceptable level of security in-house. These countermeasures could include virus scanning, the use of content filtering firewalls, intrusion detection and/or intrusion prevention systems etc. The countermeasures could be deployed inside the network or within the DMZ to minimize risk.

Today, hackers are equipped with the latest technology and tend to share their

knowledge and resources with many others across the web. Many of today's hackers are not a threat to society. Some have the common goal of pointing out security issues in software code. Some want to speak up against social injustices. Some just want a bit of a challenge. However, there are also many hackers who want to cause damage to a company's reputation or gain access to private information for fraudulent use.

Consider the following scenario. In a routine check of the system logs a network administrator at Widgets combines the firewall, the web server and the internal authentication servers logs. This experienced administrator sees the following events clearly:

A: At 10:00PM Saturday evening, a request on TCP/IP port 443 was made to the firewall's external address. The firewall forwarded the TCP/IP port 443 traffic to the extranet server.

B: An SSL tunnel was established between the extranet server and a remote system with an IP address of 123.123.123.123

C: The Extranet web host received an authentication request from user JSmith. The request was forwarded to the internal network for validation.

D: At 10:01PM the internal server validated the authentication request as JSmith. (Jim from accounting)

E: The extranet server gave Jim access to the extranet web site and mail gateway services.

F: Jim's system disconnected at 1:30AM the following morning.

What the logs can't show us is this: Jim was fast asleep by 9:00 Saturday evening in preparation for a fishing trip early Sunday morning. The user who logged in with Jim's credentials was actually half way across the globe poking away at the corporate network hoping to gain additional information that would help mount a further attack. Jim's login credentials were harvested from his laptop a few days earlier by an Internet worm and were now published in an online newsgroup for the world to see.

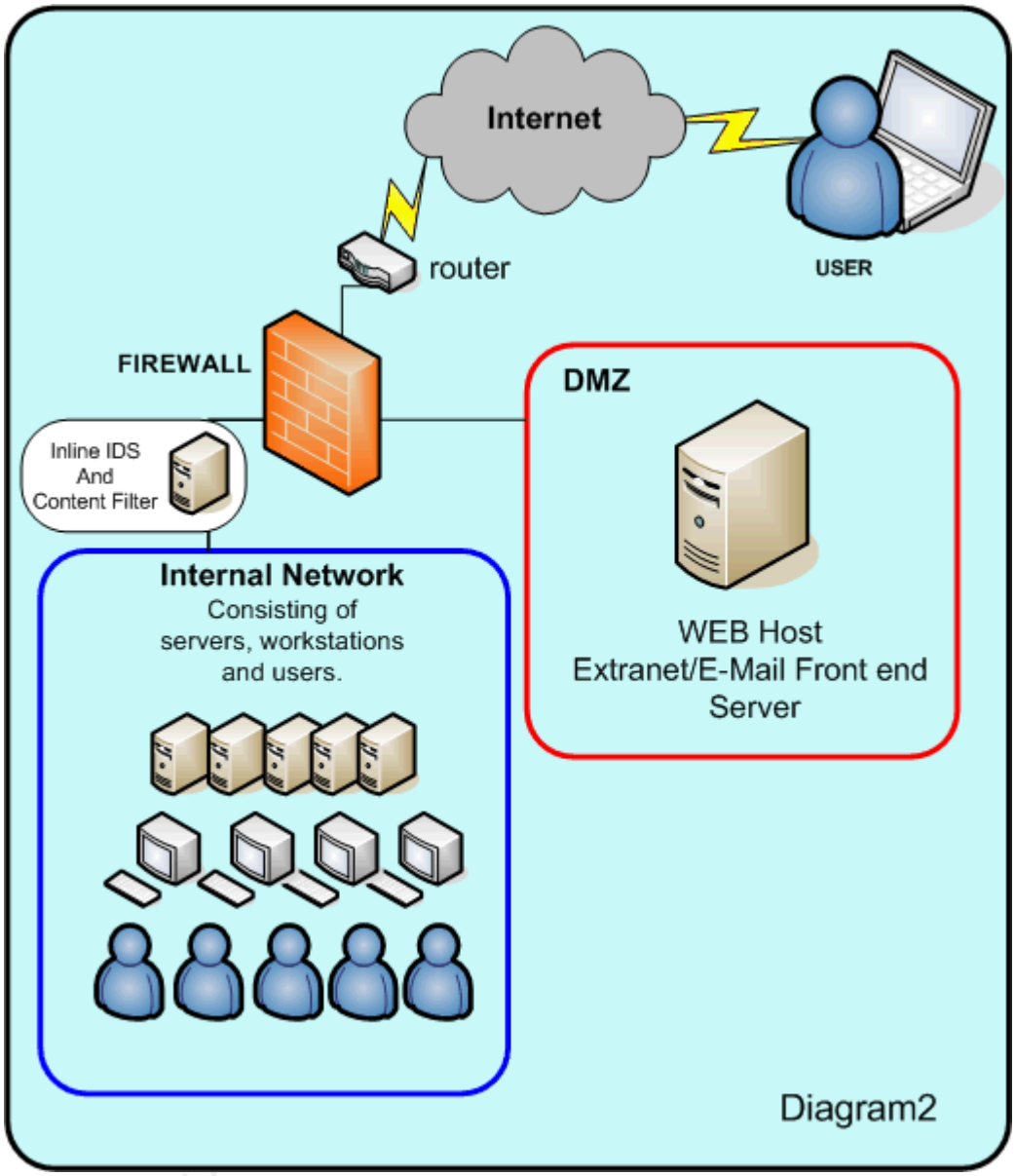
Since the intruder originally queried the firewall on TCP/IP port 443 (SSL) the firewall did not inspect the traffic. Per the firewall policy, all HTTPS traffic was forwarded to the web server. Thus, the first line of defense is the physical server the intruder was connecting to. Although measures were in place on the server to identify and authenticate users, in this case the Widgets company required identification of the user to be verified with the use of a username and password, which had been compromised. After receiving the logon credentials,

the web server queried the inside network, and as the intruder had Jim's password they had the ability to log in as Jim. Now connected, the intruder quickly reads Jim's e-mail and attempts to send additional traffic toward port 443 that is designed to fingerprint [3] the operating system of the web server. By sending invalid traffic and monitoring the server's responses, the intruder is hoping to find out what version of code Widgets web server is running and if it may be vulnerable to more attacks. If any vulnerability were present on the web server there would be a potential for the intruder to take over the box and attempt to execute code. If the system was well maintained and all security patches and fixes were up to date, the intruder could still attempt a denial of service attack on the box. All the while the web server does not see this as an attack. It's just Jim from accounting. Additionally, since a secure tunnel was established between the intruder and the web server itself, any malicious payload would be invisible to any upstream device, including the firewall.

With this configuration, additional proactive measures could be placed upstream to help identify users before they get to the server. These could include limiting connections at the firewall based on IP or hostname via access control lists instead of simply forwarding all HTTPS traffic to the DMZ. Two-phase authentication using third party authentication devices could be used to make the login process more robust. RSA security tokens are just one example. Additionally, administrators could use internally generated "private" SSL certificates versus a public SSL certificate. In this case administrators could require end users to present an assigned certificate for authentication [4]. To enable this two-phase authentication process, a list of certificates must be generated and maintained on the web server. Each user would either need to carry a special USB key-fob, Smart Card or would have to manually import a certificate into each computer that would be used to connect to the extranet site. However, if the intent were to allow users to connect from any Internet connected web browser such as at a hotel or airport kiosk, private certificates would not be an ideal option as the certificates could be compromised. A trusted third party certifying body such as Verisign or GeoTrust would need to be used to generate a "public" certificate to facilitate basic SSL. This would not authenticate the end user, just validate the identity of the host to the end user and provide the necessary building blocks for encryption. Thus, adding a two-phase authentication system that facilitates rotating or changing keys (i.e. RSA security tokens) would be more secure compared to "static" private certificates or keys.

Reactionary countermeasures could also be placed downstream in the connection. By placing an IDS sensor at the outside edge of the internal network, administrators would now be able to monitor and compare known intrusion signatures to traffic coming in and out of the network. By adding a content filter to the firewall or IDS, administrators could watch for invalid content types or filter packets containing proprietary information from passing in and out of the network.

(See diagram 2.)



In the Widgets Company scenario, the extranet server contained an e-mail “front end” server such as “MS Outlook Web Access [5] or Lotus Domino Web Access [6]”. Thus, the web server in the DMZ would need to communicate with the inside network in order to provide not only user authentication against the internal servers, but also e-mail functionality. Depending on the e-mail “front end” the administrator would need to open up additional ports on the firewall to allow traffic from the web server in the DMZ to pass inbound for these features to work properly. Widget’s administrators would be opening the internal network up to a much wider range of attacks if the web server were compromised, as the

web/front end server has access to the internal network via multiple ports.

SSL Bridging:
Could SSL bridging be beneficial to the Widgets Company? Does it provide additional defense in depth to their configuration?

With the number of computer security related incidents reported rising yearly and the use of automated attack tools becoming commonplace, [7] depending solely on reactionary technologies to defend your network has shortcomings. Providing a multi-layered approach to security that enables as many defenses as possible is the best way to protect valuable resources. Inspecting all traffic before it enters the network guards against known or potential external threats. Additionally, inspecting outbound traffic prevents employee misuse and unwanted traffic from leaving the network, i.e. company secrets and viruses.

According to the Sans Institute, "Using a defense in-depth strategy does not make it impossible to get to your core resources…However, a well-thought-out defense in-depth strategy, utilizing the strongest protections feasibly possible at each layer, presents a formidable defense against would-be attackers." [8]

Let's review the web deployment infrastructure the Widgets organization chose in detail and then introduce SSL bridging into the environment. Adding SSL bridging provides several advantages.

NOTE: There are a few vendors that make SSL bridging server software or even pre-configured "network appliances" that provide this functionality. However, for this example we will be using Microsoft ISA Server 2004 (Internet Security and Acceleration Server). ISA server provides a robust feature set and allows administrators familiar with the MS Windows platform a fairly straightforward set of configuration, monitoring, and reporting tools. Microsoft claims [9] that ISA server 2004 is an all in one IDS, SSL to SSL Bridge and Firewall. However, as our scenario is to provide defense in depth, the firewall and IDS features of ISA server will be used to compliment our network design and not to replace existing firewalls and IDS sensors. However, if deployed correctly, ISA server can take the place of some or all of these systems, depending on the risk tolerance allowed.

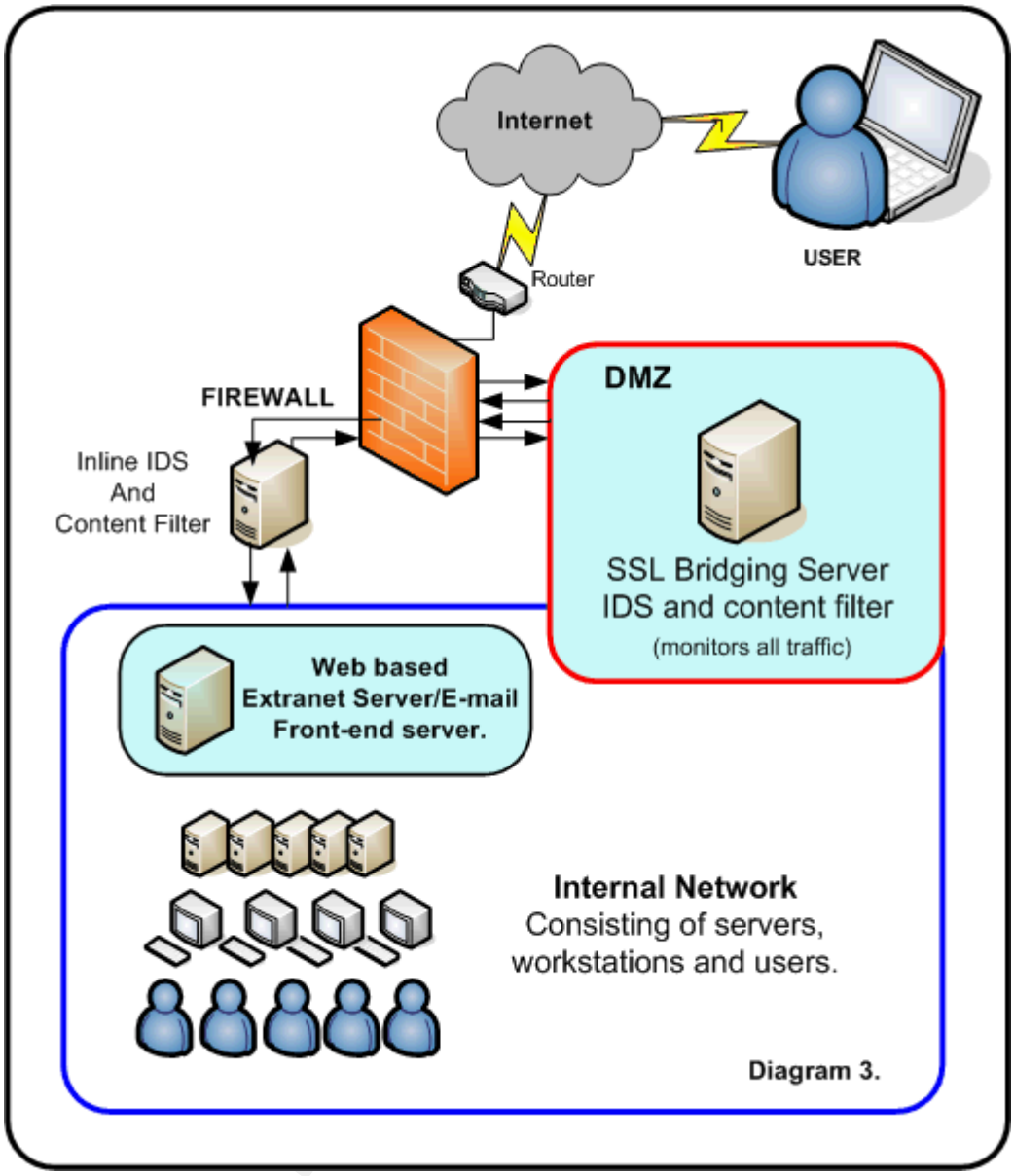


Diagram 3 is a design similar to that already discussed. Here we have placed the extranet/e-mail gateway internally. Placing the web server inside the network would normally be a poor security practice, but in this scenario, it is acceptable because the user never actually connects with the web server at any time. Instead, the user connects to an SSL bridge server functioning as a proxy. All communication between the user and the proxy is secured. The commands or requests the user initiates to the proxy are automatically screened, and if valid and allowed they are forwarded to the real host.

How is SSL bridging different from a simple proxy?

SSL bridging works by allowing the bridge server to mimic the internal hosts much like a proxy. However, due to the nature of the SSL handshake, [10] the bridging server also contains a customized certificate server. This certificate

server allows the administrator to easily install copies of the certificates from internal hosts locally. This allows the "proxy" to mimic the identity of the real host and connect securely to the user via SSL. As far as the user and third party certifying body of the SSL certificate are concerned, the bridging server is the internal host. Additionally, the bridging server is capable of connecting to internal hosts via SSL, minimizing the need for multiple ports to be open at the firewall interface connected to the internal network. One major benefit of this type of configuration is that the bridging server can be used to inspect the traffic in a non-encrypted form before re-encrypting the traffic that goes out to the end user or to the inside network. Whether the bridging server is in the DMZ or directly exposed to the web, the authentication process and data streams remain secure. The bridging server is now a centralized point to monitor traffic, create reports and allow for virus scanning, content filtering, and intrusion detection.

Implications of SSL bridging:

Although SSL bridging introduces the benefits discussed above, questions have been raised pertaining to the potential implications that go along with its use. The end user of the SSL connection may be under the impression that the SSL connection is "secure" from endpoint to endpoint and is unable to be opened by anyone along the way. (Refer to SSL Protocol Specification [1]) However, with SSL bridging enabled this is no longer the case. SSL Bridging enabled devices are essentially opening "secure" packets, inspecting them, and then re-encrypting them before forwarding them to the intended host. Thus, although the connection is "secure" the end user may not be aware that the bridging device is able to decrypt, read, filter or modify the traffic based on whatever criteria the bridging device's configuration allows.

This implication was originally raised with the advent of SSL off-loading, the precursor to SSL termination or bridging. In the case of SSL off-loading, added security was not the intent of the technology. SSL off-loading was originally adopted to enhance the delivery of secure data by off-loading the physical hardware resources of encrypting and decrypting packets from the host itself to another device in order to conserve CPU cycles. This allows the host to deliver more information to the web cost effectively. With SSL offloading, the connection is secured from the end user to the offloading device. But the connection is unsecured from the off-loader to the host. In this scenario, while there is a performance benefit there is also significant risk involved if the unsecured portion of the connection ever travels over an insecure network. Many critics of SSL off-loading have theorized that in the event of a compromise of data, end users may take legal recourse against the company or ISP using off-loading technologies. As the end users may have been under the impression that their data was "secure". With SSL termination/bridging technologies, the connection is secured in both directions of the bridge minimizing the risk, as data is not transported in an unsecured fashion.

The added security benefits of SSL bridging allow administrators to inspect traffic for potentially harmful characteristics. However, bridging could also be used to inspect traffic for other information the end user thought was safe inside the encrypted tunnel. Depending on the type of data involved and configuration one chooses end users may need to be aware that the connection is no longer adhering to the original SSL specifications. Thus, before implementing SSL-Bridging, administrators should make sure their usage and privacy policies properly allow for its use. Additionally, appropriate measures should be put in place to validate the configuration. A poorly configured bridge could allow an administrator to place a custom filter into the bridging device allowing it to copy every packet while in its unsecured state and redirect or forward packets to another location. If the Administrator were also allowing normal function of the bridge, the administrator would be essentially creating a “man in the middle attack”, allowing them to sniff the data for passwords and or other proprietary information, which could be used inappropriately. Thus, Administrators should fully understand the SSL bridging technology before installing and configurations should also be audited for mistakes.

Let’s see what happens with the SSL Bridging server installed.

A: At 10:00PM Saturday evening, a request on TCP/IP port 443 was made to the firewall’s external address. The firewall forwarded the TCP/IP port 443 traffic to the Bridging server.

B: An SSL tunnel was established between the bridging server and a remote system with an IP address of 123.123.123.123

C: The Bridging server attached to the extranet/e-mail gateway via an SSL session.

D: The Bridging Server received an authentication request from user JSmith. This allowed request was forwarded to the extranet server for validation

F: The two-phase authentication process/service sees the request and issues the user an additional challenge, and waits for the response. (I.e. certificate hash, pin-code etc)

G: The response to the secondary authentication request comes back as valid: This time it really is Jim from accounting.

H: The extranet server forwarded the original authentication request to the internal authentication server.

I: At 10:01PM the internal server validated the authentication request as JSmith. (I.e. Jim from accounting)

J: The extranet server gave the bridging server access to the extranet web site and mail gateway services.

K: The bridging server is now standing in as an active proxy.

L: Jim's system attempted to perform a port scan of what it thought was the web host in the DMZ. The bridging server identifies the incoming traffic as not allowed, and immediately disables the connection and places an event in the logs.

Even though a two-phase authentication process was added to our configuration, it is important to remember that dangerous attacks can originate from anyone including an authorized employee. If Jim had malicious intent and was now the attacker he still would have access to the network even with 2-phase authentication. SSL bridging with content filtering prevents even authorized users with secure sessions from attacking the network.

Conclusion:

In the above scenario, the Widgets IT staffers were able to add an additional layer of security to their web hosts with the implementation of SSL bridging. With this technology in place, the Widgets IT staff can now inspect and monitor all traffic to and from their organization, minimizing the risks associated with secure connections. Whether the solution they chose was a pre-configured appliance or an enterprise level software package, the Widgets Company's investment in SSL bridging technology enhances established technologies. This allows intrusion detection, content filtering, and virus scanning technologies to perform their critical functions in a proactive manner on traffic that was up until now, invisible. By providing true defense in-depth, even when authenticated users attempt to perform unauthorized actions, the use of SSL bridging and content filtering technologies in concert thwart the attack.

References:

[1] SANS Institute Track 1-1.4 –SANS Security Essentials ”Encryption 101” p 63.

[2] Netscape Communications “SSL 2.0 Protocol Specification” http://wp.netscape.com/eng/security/SSL_2.html

[3] Chapel, Laura -Security Pro News “OS Fingerprinting With ICMP”2003-09-29. http://securitypronews.com/securitypronews-24-20030929OSFingerprintingwithICMP.html

[4] RSA Security Inc. “Cryptography in the real world”- Section 5.1.2 “What is SSL” http://www.rsasecurity.com/rsalabs/node.asp?id=2293

[5] Microsoft Corporation “Customizing Microsoft Outlook Web Access” http://www.microsoft.com/downloads/details.aspx?familyid=6532E454-073E-4974-A800-1490A7CB358F&displaylang=en

[6] IBM Corporation “Lotus Domino Web Access 6.51” ftp://ftp.lotus.com/pub/lotusweb/products/dominowebaccess/LotusDominoWebAccess651.pdf

[7] CERT “CERT/CC Statistics 1988-2004” http://www.cert.org/stats/cert_stats.html

[8] SANS Institute -Track 1-1.2 “Defense in-depth (2)” p.13

[9] Microsoft Corporation, ISA Server 2004 “Product Overview”. http://www.microsoft.com/isaserver/evaluation/overview/default.asp

[10] Ourshop.com “Straightforward Explanation of SSL and HTTPS” How Does SSL work?” page 2. http://www.ourshop.com/resources/ssl_step1.html

Additional Resources:

There are many resources available online that will describe individual SSL bridging/initiation products. This section contains links to additional sources of helpful information.

For information on the general security implications of SSL offloading/Bridging technologies:

http://www.windowsecurity.com/articles/SSL-Acceleration-Offloading-Security-Implications.html (A general article that describes SSL Bridging technologies from a different perspective than most vendor related sites. The article also raises the question about the implied end user perception of SSL technologies, a subject on which an entire paper could be written about. [Hopefully another GSEC candidate will want to tackle this topic]).

SSL Bridging, Offloading and Termination technology vendors include:

Microsoft Corporation
http://www.microsoft.com/isaserver/ (the official home of Microsoft ISA Server, check up on the latest service packs, or download a fully functioning demo of ISA Server 2004)

SonicWall
http://www.sonicwall.com/services/ssl_documentation.html (Sonic wall's SSL bridging/offloading technology page)

http://www.techworld.com/files/whitepapers/SSL_solutions.pdf (A SonicWall SSL white paper)

Cisco Systems
http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_configuration_guide_chapter09186a0080292a22.html (Cisco Systems guide to SSL technologies including SSL Initiation)

Octagate inc.
http://www.octagate.com/SSLDetails.asp (a software based HTTP load balancing product with SSL acceleration and offloading features, this may just be the tool for organizations on a budget).

Safe Enterprises/Rainbow
http://www.rainbow.com/products/igate/netswift2012.asp (an SSL accelerator appliance with authentication and SSL termination functionality, also offers authentication via with USB tokens)

Last Updated: October 23rd, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
GridEx IV 2017	Online,	Nov 15, 2017 - Nov 16, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, GB	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS San Diego 2017	OnlineCAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced