Information and Network Security
6G6Z1012

Joshua Michael Ephraim Bridge
joshua.m.bridge@stu.mmu.ac.uk
14032908

March 21, 2018

Abstract

In this report a solution is proposed for ensuring a much more robust network within a financial company, which is much more defended from both internal and external attack vectors. The technologies proposed are re-used for greater cost-effectiveness (such as IPSec tunnel) without compromising on security. Multiple vulnerabilities & attacks are highlighted with the current network layout and solutions for each of these are clearly defined. Finally, every additional requirement from the company is met with a cost-effective solution, again through re-use of technologies.

Keywords— IPSec tunnel (VPN), Application-level Gateway, IDS (Network), SFTP

1 System Analysis (Vulnerabilities & Attacks)

1.1 Insecure IP packets

At the moment, the branches communicate to the headquarters over the internet in an insecure way. As the packets being sent over the internet are not protected, anyone could read the contents of these messages and potentially use them to attack the system. Any router or system that lies in the network path between each branch and the headquarters could intercept any message sent between them and possibly modify, remove or replay that message.

Replay Attack The current network is very suceptible to a replay attack with its user/password system. As there is no underyling security protocol to protect messages over the internet, a packet sniffer could be used to listen for a valid sign-in message and then that message could be re-sent by an attacker to gain access to the system (OWASP n.d.).

1.2 Internal Access Control

A major issue with the current network layout is that all devices in each location are grouped together within the same LAN, so any computer/server can access every other computer/server. There is no access control which could prevent resources being accessed by users who should not be able to.

Internal Malicious Access Either an employee with internal network access or an outside attacker who has gained access to the network is able to access all of the resources within any location. This allows the possibility of a whole host of attacks such as offline dictionary attacks & DNS cache poisoning.

1.3 User/Password Authentication

A user/password system is unsuitable for secure authentication when connecting over the internet. Usernames and passwords for users are often very simple for the sake of being able to remember them, therefore this makes them much more suceptible to being guessed by an attacker.

Offline Dictionary Attack If an attacker manages to get into the database containing all company usernames and passwords and there is no encryption on the passwords, then they can easily make a copy of all of these records and then could use them to hijack any system on the network without effort (CAPEC n.d.).

1.4 Insecure FTP Server

The current FTP server is serving with unprotected traffic, which is easily exploitable and a very critical vulnerability when the company is dealing with financial information.

Packet sniffing Attackers can scan network traffic to easily pick up FTP login passwords sent in plain text, furthermore they can see the files being transferred and make a copy of any file. This can be done with free software such as Wireshark (`https://www.wireshark.org`).

1.5 Unprotected DNS

The DNS server at the headquarters is currently located within the same LAN as the public facing servers and the office workstations. Therefore if any of these devices were to be compromised then the DNS server is very suceptible to being attacked.

DNS cache poisoning Due to the current network design, once an attacker has gained entry to an employee computer via either a Replay or Dictionary attack it is possible to then reach the DNS server via the LAN and poison its cache (Son & Shmatikov 2010). It would therefore be possible to redirect any authentication traffic to an attacker-controlled server and collect the passwords of every user that tried to log in while the cache is poisoned.

2 Secure Network Design Proposal

2.1 Attack Prevention

In order to protect against the attacks I have identified, I suggest that the following technologies be implemented. In **bold** are the vulnerabilities/attacks which are being prevented.

2.1.1 IPsec-ESP (VPN)

In order to protect against **Replay attacks**, an IPsec tunnel is an ideal solution for maintaining message authenticity (NCSC 2016). When deployed in ESP mode, all devices connecting remotely to the main network has a secure connection which can not be interfered with by attackers and using network sniffing tools would only show encrypted packets with an IP destination. Therefore, re-sending the same packet would not work due to the contents of the TTL header. This method is suitable due to the fact that the organisation already has DNS infrastructure required for setting up a VPN, it would only require possible replacement of the office boundary routers from the ones supplied by the ISP in order to handle the VPN traffic.

2.1.2 Application-level Gateway

An application-level Gateway would be an ideal solution for protecting against **Internal Malicious Access** and therefore also protecting against **DNS Cache Poisoning** & **Offline Dictionary Attacks**. This is due to the fact that if an attacker can not gain access the internal network then it is not possible for them to even begin more specific attacks such as the two mentioned previously. The networks within the headquarters should be split up into DMZs seperated by firewalls, where only certain users are permitted to cross these zones for certain application uses (This can be seen in fig. 1). For example if an outside attacker has managed to gain access to an employee account within the network, they still will not be able to access the DNS server due to not having the correct authentication to access the server.

2.1.3 SFTP (Secure File Transfer Protocol)

To protect against **Insecure FTP**, a more secure file transfer protocol implementation is ideal. While internet traffic would be protected from IPSec VPN, within the network file transfers would still be insecure. SFTP is an extension of SSH (Secure Shell) which allows for secure transfer of files over any network (SSH n.d.). This is relatively simple to set up and does not interfere with any firewall, as it only requires a single port (22) to work. This makes it a much easier solution than FTPS (FTP Secure) which requires many ports which are difficult

to manage (GoAnywhere 2011). Many FTP clients will support this mode such as Filezilla (`https://filezilla-project.org`) and WinSCP (`https://winscp.net/`).

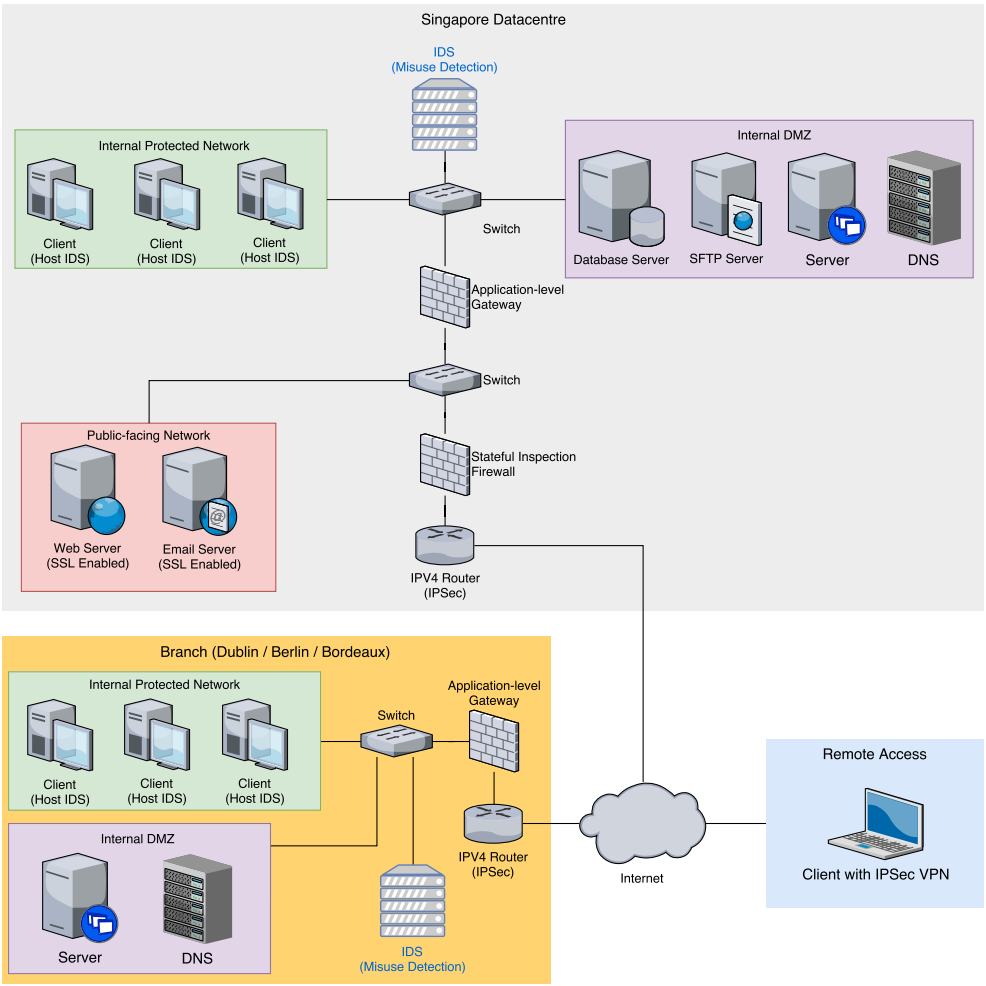

Figure 1: Network diagram

2.2 Additional Requirements

Below are the solutions I propose for each of the additional requirements of the company.

2.2.1 Authentication

For authenticating users, I would suggest that a more secure form of the user/password system be implemented such as password Hash & Salt. A salt of 64 bytes is the standard recommended size if allowed by the storage mechanism (OWASP 2018). The salt dramatically slows down **Offline Dictionary Attacks** as each attempted password crack must be recomputed with each different salt. Therefore it is suggested to use a different salt for each password and not a single re-used salt. This would not require huge amounts of work as the user system is already

there, furthermore making sure the passwords are not sent in plaintext over the network which could be picked up by an attacker using a packet sniffer.

2.2.2 Access Control

Access control could easily be managed by the application-level gateway described in section 2.1.2. The gateway is capable of understanding which users have access to which resources and can stop the packets from reaching the intended destination if the user does not have the correct permissions as specified in its policy fields (*Application level gateways* n.d.).

2.2.3 Site-to-site Connection

An IPsec VPN (as mentioned in section 2.1.1) would provide a secure connection for both site-to-site and remote access. When deployed at the site gateway, each site could connect securely to one-another by establishing a secure tunnel where data sent between sites could not be interfered with.

2.2.4 Remote Access

As mentioned in sections 2.1.1 & 2.2.3, IPSec VPN is a perfect solution for implementing secure remote connection to the company network. As the same technique will be used for connecting different sites, it is more or less trivial to set this up on other computers wishing to connect from remote locations. While it would require installation on each machine wishing to connect to the network, this could be seen as a positive as it enures only trusted devices will be capable of connecting.

2.2.5 Secure Web & Email Access

In order to secure the connection between users and the Web & Email servers, installing the SSL/TLS protocol on each server would be the best way of securing those connections (NCSC 2017). Those protocols are designed specifically for the purpose of securing connections to online resources, and they provide protection for both confidentiality and message integrity. All it requires is the purchase of some SSL certificates, which does not require much upkeep as once it is in place it should work for at least a year until the certificate needs to be renewed.

2.2.6 Attack Detection / Mitigation

When trying to detect and mitigate attacks within a network, a network-based IDS with signature-based detection is the most ideal solution. While it is not 100% effective and can produce false-negatives, therefore still requiring some monitoring, it is a lot more efficient then hiring a human being to constantly sit and monitor many different systems for signs of an intrusion. Host-based IDS' (Avast Free) are currently installed on client machines, so there is no reason to remove this software. This software however will not protect any of the application servers from being attacked, therefore an additional network-based IDS is recommended for optimal security.

2.2.7 DDoS Attacks

In order to protect against DDoS attacks, a cloud-based DDoS protection service would be ideal for filtering out requests from users which aren't trying to create a genuine session, but just to

overload the servers. Services such as Kona Site Defender (Akamai n.d.) offer this protection by forwarding any genuine request to the web server, and ignoring any request which it deems to be invalid. With a solution like this it would greatly reduce the server load on the outbound router & web server and stop the DDoS from having a big effect on service quality. This is because the cloud servers would be more equipped to deal with high load without much overhead, whereas on the web server it would have to dedicate much more resources to each request/packet.

3 Conclusion

The network design proposed in this report I believe is an effective and cost-effectve suggestion for increasing the security within this organisation. While it may require a lot of initial set-up/configuration, I feel that the solutions I have suggested are used in an efficient way due to their re-use against multiple attack vectors. For example the Application-level Gateway (section 2.1.2) protects against 3 of the identified security vulnerabilities due to their cascasding nature.

Some flaws in my proposal include that it does not make use of SSO (Single Sign-On) which could be implemented using Kerebos however I felt that adding this to my solution would not be cost-effective. Furthermore it does not include an explicit access control matrix which could prevent users from acessing specific files - it only includes access control for requests made over the network.

I believe this solution is much more advanced than the original network, as it protects against intrusions from both within and outside the LAN of any branch - without involving a complex set of security solutions.

References

Akamai (n.d.), 'Ddos mitigation', https://www.akamai.com/us/en/resources/ddos-mitigation.jsp.

Application level gateways (n.d.), http://www.open.edu/openlearn/science-maths-technology/computing-and-ict/systems-computer/network-security/content-section-9.5.

CAPEC (n.d.), 'Capec-16: Dictionary-based password attack', https://capec.mitre.org/data/definitions/16.html.

GoAnywhere (2011), 'Sftp vs ftps', https://www.goanywhere.com/blog/2011/10/20/sftp-ftps-secure-ftp-transfers.

NCSC (2016), 'Using ipsec to protect data', https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data.

NCSC (2017), 'Using tls to protect data', https://www.ncsc.gov.uk/guidance/tls-external-facing-services.

OWASP (2018), 'Password storage cheat sheet', https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet#Use_a_cryptographically_strong_credential-specific_salt.

OWASP (n.d.), 'Testing for ws replay (owasp-ws-007)', https://www.owasp.org/index.php/Testing_for_WS_Replay_(OWASP-WS-007).

Son, S. & Shmatikov, V. (2010), The hitchhiker's guide to dns cache poisoning, *in* 'International Conference on Security and Privacy in Communication Systems', Springer, pp. 466–483.

SSH (n.d.), 'Sftp – ssh secure file transfer protocol', https://www.ssh.com/ssh/sftp/.