{REDACTED} Security Assessment Checklist Appendix B – Network Configuration Report

Prepared for {CLIENT} {CLIENT} by Sean Cooper for {REDACTED}

Table of Contents

TABLE OF CONTENTS 2

REVISION CONTROL LOG 3

INTRODUCTION 4

SCOPE 4
LIMITATIONS 4

GENERAL NETWORK TOPOLOGY 5

ROUTER / FIREWALL ASSESSMENT 5

SERVICE CONFIGURATION 5

SCAN RESULTS 5
PING SCAN 5
TCP SCAN 5
UDP SCAN 5
INTERPRETATION 6

USERNAMES / ACCOUNTS / PASSWORDS 6

NETWORK ENCRYPTION 6

STORAGE ENCRYPTION 6

INTERNET SERVICE PROVIDER (ISP) INFORMATION 7

RECOMMENDED NETWORK CHANGES 7

INFRASTRUCTURE 7
FIREWALL 8
WORKSTATION 8

SIGNATORY PAGE 10

Revision Control Log

Date	Old Version #	New Version #	Revised By:	Description
2014-09-24	0.0	0.1	Sean Cooper	Initial Document Composition
2014-09-25	0.1	1.0	Sean Cooper	Initial Document Delivery

Introduction

{REDACTED} (SPTP) was retained by {CLIENT} {CLIENT} to perform a network security audit after a third-party vendor (TPV) indicated that {CLIENT} {CLIENT} may have had a security incident that resulted in the disclosure of customer data to an unknown party. As part of the remedy for this security incident, SPTP performed a network scan and audit of the {CLIENT} {CLIENT} network. This artifact contains those results along with an interpretation and recommendation section.

Scope

The scope of this network configuration audit is such that the following systems were analyzed:

- Network devices such as routers, firewalls and wireless networking
- Network connectivity analysis
- Unnecessary service analysis
- User Account security practices
- Data in-transit encryption standards
- Data storage encryption standards
- ISP Information

This analysis also includes an interpretation section as well as a recommendations section, to better align the {CLIENT} {CLIENT} network with modern security best-practices.

Limitations

This analysis does not include specific implementation instructions, as it is up to the client to decide if the TCO of suggested vulnerability mitigations outweighs the risk of the potential security threats to the {CLIENT} {CLIENT} network. Should {CLIENT} {CLIENT} wish to engage SPTP in an engagement extension to develop specific implementation instructions, those implementation instructions will be provided under separate cover.

This analysis is limited to network systems and configurations, as directed by the {REDACTED} Security Checklist instructions. This analysis does not include significant guidance on desktop security or server security issues that may or may not exist.

General Network Topology

The general network topology is a hub and spoke network configuration, with the Dell SonicWALL appliance providing router and firewall services to the internal network. The network has two upstream providers, both connected to the Dell SonicWALL device, providing fail-over from one Internet link to the other.

Router / Firewall Assessment

All local routing and firewall services are provided by a single Dell SonicWALL network appliance. While this single Dell SonicWALL device does present a single point of failure (SPoF), it is an accepted risk by the IT engineers at {CLIENT} {CLIENT}.

The routing is done by standard IP-network style routing, with the default gateway for the network being assigned to the .1 IP address of the LAN segment. The IP addressing scheme on the internal zone of the firewall is a non-routable network address space.

Firewall functionality is provided by network address translation (NAT) and a rule-based firewall policy engine that restricts traffic based on the rules input by the appliance administrator. This particular rule engine is configured to allow certain types of traffic, and then deny others with a typical ALLOW/DENY configuration.

The Dell SonicWALL is using an updated version of its firmware.

Service Configuration

Scan Results

PING Scan

```
Scanning {CLIENT} [7 ports]
Completed Ping Scan at 10:09, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:09
Completed Parallel DNS resolution of 1 host. at 10:09, 0.00s elapsed
```

TCP Scan

```
Scanning {CLIENT} ({CLIENT}) [1000 ports]
Discovered open port 554/tcp on {CLIENT}
Discovered open port 80/tcp on {CLIENT}
Discovered open port 22/tcp on {CLIENT}
Discovered open port 443/tcp on {CLIENT}
Discovered open port 21/tcp on {CLIENT}
Discovered open port 7070/tcp on {CLIENT}
Completed SYN Stealth Scan at 10:10, 32.63s elapsed (1000 total ports)
```

UDP Scan

```
Scanning {CLIENT} ({CLIENT}) [1000 ports]
Discovered open port 500/udp on {CLIENT}
Completed UDP Scan at 10:28, 1102.83s elapsed (1000 total ports)
```

Interpretation

Port filtering is implemented on the Dell SonicWALL appliance, which lies on the network perimeter, just inside the ISP router.

There are several services that are accessible from the external interface of the firewall, including:

- FTP
- SSH
- HTTP
- HTTPS
- RTSP
- RealAudio Client
- ISAKMP

Usernames / Accounts / Passwords

Username and password requirements were moderate, with all usernames having at least an 8 character password.

The password policy clearly indicates that users are responsible for changing their passwords on a regular basis, and that the passwords are not to be shared between users.

Default usernames and passwords on firewalls and routers have been changed to a non-default value.

Users did not have Administrator / “root” access to machines to install software or make modification changes. No unauthorized software packages were found on the inspected workstations.

Network Encryption

{CLIENT} {CLIENT} uses SSL/TLS to connect to all third-party vendors (TPV) such as {REDACTED}, {REDACTED}, {REDACTED}.

Username and password data is encrypted between workstations and servers using the default Windows Server 2008 and Windows 7 mechanisms (NTLM).

Occasional unencrypted data transfer happens on a one-way basis through a telnet service that {CLIENT} utilizes as-needed.

802.11b/g wireless access is secured by WPA2 encryption provided by the WAP.

Storage Encryption

Very little customer data is stored on individual workstations or servers, it is processed or hosted on a third-party platform. The user workstations function mainly as access terminals. As such, the need for on-site disk encryption is low.

Internet Service Provider (ISP) Information

{CLIENT} {CLIENT} utilizes the Optimum Online for internet connectivity as their primary ISP.

They also use Verizon as a backup ISP, with the Dell SonicWALL appliance managing the failover between the two links.

Recommended Network Changes

Infrastructure

1. Due to pending EOL, Windows Server 2003 should be upgraded to Windows Server 2008, at minimum and Windows Server 2012 if possible.

2. Windows "Administrator" username should be changed to something non-obvious to lessen the chance of compromise of that account.

3. There were no physical controls observed to prevent tampering with infrastructure equipment. It is recommended that a physical access control, such as a keyed or RFID lock, be installed on the door to prevent tapering with equipment. This door should be shut at all times.

4. An IDS/IPS solution would strengthen the ability to detect and react to network intrusions in real-time. It should be installed in-line, behind the firewall and before the user-access switch.

5. DHCP should be configured to use a whitelist of MAC addresses to provide network IP addresses. If a machine doesn't have a whitelisted MAC address and a valid IP address from DHCP, no traffic should be allowed to or from the device.

6. All network services should be configured to only provide access to a whitelisted IP address and MAC address, if possible. This includes the firewall and gateway devices.

7. No network access control was observed. This should be implemented by either whitelisting MAC addresses on certain switch ports, or preferably through an interactive client such as Cisco NAC that ties into the Active Directory authentication subsystem and uses those credentials to open a network port.

8. No DLP software or appliances were observed. A DLP system can prevent the loss of customer or company data through deep content inspection of network packets, when properly configured and maintained.

9. Zoning or VLANing of network segments should be implemented to better manage broadcast traffic, as well as to provide segregation of network components from other network components. This is currently done with the WLAN, but should be extended into the server zone, the workstation zone, the utility zone (printers/copiers/faxes), etc. This provides the ability to monitor and restrict traffic traveling from one subset of machines to another.

10. Wireless network access should be controlled by 802.1x credentialing (either username and password, or certificate-based), if it is to allow access into the internal network segment.

Firewall

1. The firewall appliance is using a non-default username, but the username is obviously an “admin” username. It is suggested that this be changed to something less-obvious.

2. Firewall password complexity and length requirements are not being enforced. It is recommended that the password complexity be enabled, and that the password length requirement be set to 12 characters.

3. The firewall appliance has a web-based configuration and management utility that is externally facing, which is a security risk. This should be either disabled completely, or, configured to use an IP whitelist provided by the upstream (ISP) router. The non-SSL port (port 80) should also be disabled.

4. The inbound firewall appliance FTP username and password are set as default “admin/password” combination. This should be updated to non-default username/password combinations.

5. Inbound FTP connections should not be allowed, as they allow unencrypted infiltration and exfiltration of user credentials and company data.

6. All IPv6 accessibility should be disabled unless IPv6 is actively being used by the enterprise and the upstream ISP.

7. The business need for Inbound RTSP and RealAudio connections could not be substantiated, so it is suggested that they be disabled on the Dell SonicWALL firewall appliance.

8. The Dell SonicWALL appliance has entered “active retirement mode”, which indicates that the support and security updates for the platform will terminate. It is suggested that a replacement platform be identified in CY 2015.

Workstation

1. The use of 8 character passwords provides moderate security; it is suggested that a formal password policy be instated and that the default complexity requirements GPO be activated on the Active Directory domain controller used for logins on the network. This would increase password length to 12 characters and provide a password complexity requirement for the use of 2 capital letters, 2 number, 2 special characters.

2. For the computers directly accessing {REDACTED} data, it is recommended that these computers undergo whole-disk encryption (WDE) with an approved WDE product.

3. To greatly enhance the security profile of the user workstation, it is suggested that more stringent user controls be implemented, in line with the DISA STIGs for Windows 7 workstations.

4. Properly installed and configured anti-virus, anti-malware, anti-spyware, and firewall software was found on all workstations that were audited.
5. All workstations were patched and up-to-date using either vendor update mechanisms or third-party patch management tools.

6. Users should not provide username/password combinations to management, this lessens the auditability of network sign-in and resource access, as the user can successfully refute activity by the presence of this list. A better SOP would be for an administrative reset of the password in the event that a manager needs access to the workers files.

7. To prevent account compromise, users should not write usernames or passwords down or store them where anyone else has access to them, as was observed. This should be integrated into the yearly information security training.

8. The following machines have anomalous traffic and virus / comprise counters. The computers should be intensely scanned and the users of those machines should be given enhanced security training.

IP Address	Blocked	Virus	Intrusion
{CLIENT}21	11	0	39458
{CLIENT}237	9	2	23630
{CLIENT}78	16	0	1
{CLIENT}253	16	0	5
{CLIENT}242	15	0	1
{CLIENT}200	13	0	3
{CLIENT}28	16	0	1
{CLIENT}240	11	0	2
{CLIENT}238	15	0	1
{CLIENT}88	14	0	1
{CLIENT}27	9	0	1
{CLIENT}99	9	0	1
{CLIENT}26	16	1	0
{CLIENT}74	9	0	1
{CLIENT}247	6	3	0

--- END OF REPORT, SIGNATURE PAGE FOLLOWS ---

Signatory Page

I attest that I conducted the network configuration review as indicated in this report, and that any and all gathered data relevant to the assessment has been included in this report.

Any and all statements made are true to the limits of my knowledge.

So sworn this 25th day of September, 2014.

_____

//S// Sean C. Cooper, CISSP