RESPONSIBILITIES GUIDE

SECURITY CONSULTING SERVICES

November 2013

RESPONSIBILITIES GUIDE

SECURITY CONSULTING SERVICES

RESPONSIBILITIES GUIDE

SECURITY CONSULTING SERVICES

1. ABOUT THIS GUIDE

There are a number of terms, conditions, requirements, roles and responsibilities associated with the purchase and use of Telstra's Security Consulting Services (**Services**).

The guide outlines both your and our roles and responsibilities regarding the Services.

This guide is divided according to the broad product offerings, Translation, Design and Optimisation and Optional Services. It is a companion document to the Security Consulting Services section of Our Customer Terms, and your Application Form.

Your requirements

You are expected to manage and use your Services according to the requirements outlined in this guide.

If you choose not to follow these requirements, we will not be responsible for any loss or inconvenience experienced if your Service is disrupted, and we may charge you additional fees in order to fix your Service.

You are required to provide us with all applicable information, data, consents, authorisations, decisions and approvals in order to activate service requests. You have to provide these things in the formats we specify (if any).

You are also required to identify when you need assistance from your assigned Telstra account executive and submit the appropriate requests.

Our requirements

We will provide your Service according to the requirements outlined in this guide.

We will provide service support and notify you of any service changes and let you know when a service request has been completed.

We will endeavour to answer questions you raise regarding the solution within agreed timeframes.

REQUIREMENT	RESPONSIBILITY	
	Telstra	You
Specify the format to collect the information for the Security Consulting service to be purchased	✓	
Provide the necessary information for the Security Consulting service in the format specified by Telstra		✓
Provide timely access to suitable personnel to clarify or confirm information as required		✓
Specify the available formats for the outputs from the Security Consultancy Service	✓	

RESPONSIBILITIES GUIDE

SECURITY CONSULTING SERVICES

Keeping your contact details up to date

From time-to-time we will need to get in contact with you regarding your Service, so it's important that you keep your organisation's details up-to-date.

You need to ensure that the following contact details are correct and kept up-to-date:

- **Commercial contact**: the authorised staff member who acts on your business's behalf regarding all commercial matters associated with your service. Your Telstra account executive may call these contacts the 'primary contact' when carrying out functions on your behalf.
- **Technical contact:** the authorised person who answers any technical questions associated with your service on your behalf.

2. POLICY TRANSLATION SERVICES

The devices we will translate from

We will translate the policies on your existing devices into a format you select. The appliances we will support are set out in the table below:

Supported Existing Devices (translate from)		
Firewall		
Vendor	Model(s)	Comments
Cisco	PIX	version 6.x to 8.4
	ASA	Versions 6.x to 8.4
	FWSM	
	iOS Routers	Version 12.0 to 12.14, excluding X* series
Juniper	Netscreen	
	SSG	
	ISG	
Checkpoint	SmartCenter NG/NGX	
	Secure Platform	
IPS		
Cisco	4200	
Juniper	All models	

RESPONSIBILITIES GUIDE

SECURITY CONSULTING SERVICES

Checkpoint	All models	
Content Security		
Firstwave	All models	Internet Protection Web and Internet Protection Mail

What we need from you

In order to carry out the translation services, we need the following inputs from you. You have to provide them in the time we specify, or if no time is specified, a reasonable time. We may not be able to perform the translation services until you provide us with the requested details.

Firewall	IPS	Content Security
Accurate extract of existing Firewall policy	Accurate extract of existing IPS policy	Accurate extract of existing Content Security appliance policy
Configuration or policy supplied in the format we specify	Configuration or policy supplied in the format we specify	Configuration or policy supplied in the format specified by us
Existing Firewall vendor and type	Existing IPS vendor and type	Existing Content Security appliance vendor and type
Proposed Firewall vendor and type if applicable	Proposed IPS vendor and type if applicable	Proposed Content Security appliance vendor and type if applicable
Ready access to your personnel to clarify or confirm information	Ready access to your personnel to clarify or confirm information	Ready access to your personnel to clarify or confirm information

How to extract files from devices

Some of the information we request from you can be extracted from your devices. Appendix 1 includes technical directions to assist you with this process to ensure the information is made available in a usable format.

RESPONSIBILITIES GUIDE

SECURITY CONSULTING SERVICES

The devices we will translate to

We will translate the policies on your existing devices onto a defined range of devices. The devices we will support are set out in the table below:

Supported Existing Devices (translate from)		
Firewall		
Vendor	**Model(s)**	**Comments**
Cisco	PIX	version 6.x to 8.4
	ASA	Versions 6.x to 8.4
	FWSM	
	iOS Routers	Version 12.0 to 12.14, excluding X* series
Juniper	Netscreen	
	SSG	
	ISG	
Checkpoint	SmartCenter NG/NGX	
	Secure Platform	
IPS		
Cisco	4200	
Juniper	All models	
Checkpoint	All models	
Content Security		
Firstwave	All models	Internet Protection Web and Internet Protection Mail

The export formats we support

We can provide translation details in specified formats. The formats we currently support are set out below:

1. Example IPOT (Telstra IP Ordering Tool). IPVAS, MDN, IPWAN
2. Example MSS Detailing Workbook (Telstra)

RESPONSIBILITIES GUIDE

SECURITY CONSULTING SERVICES

3. Standard formats (Non Telstra)
   a. CSV
   b. TXT
   c. XML

Limits on service scope

Policy translation is usually offered on similar devices for similar environment that have similar traffic requirements. No change in requirements in traffic flow, routing or other relevant change is included.

Policy translation is completed by our Professional Services Consultants and passed to the SSF team for implementation. We can provide a copy of the translated policy upon request. Should you require any change to the policy, this can be addressed via SSF standard change request process.

The second limit relates to unusual requests beyond the usual scope of translation work. We will advise you if a request is outside what we include in our standard service offering.

If you ask us to exceed these limits, additional charges may apply.

3. POLICY DESIGN SERVICES

The devices we will design for

We will design policies for certain devices. The devices we will support are set out in the table below:

Supported Devices
Firewall
Cisco Security Appliances: PIX ASA FWSM ASA 8.3 **Firstwave**
Cisco IOS routers: Version 12.0 to 12.14, excluding X* series
Juniper firewalls: Netscreen, SSG, ISG
Check Point: SmartCenter NG/NGX, Security Management R70 to R75 running on any platform, including: SecurePlatform Check Point IPSO (formerly Nokia) Crossbeam Linux Solaris Windows
Intrusion Prevention System
Cisco IPS Appliances: Cisco IPS 4200 Series Juniper
Content Security
Firstwave Cisco Palo Alto

RESPONSIBILITIES GUIDE

SECURITY CONSULTING SERVICES

What we need from you

In order to carry out the policy design services, we need the following inputs from you. You have to provide them in the timeframe we specify, or if no time is specified, a reasonable time. We may not be able to perform the policy design services until you provide us with the requested details.

Firewall	IPS	Other	Content Security
Accurate extract of existing Firewall policy	Accurate extract of existing IPS policy	Your Regulatory Requirements (eg PCI, ISO27001, ISM, etc)	Accurate extract of existing Content Security appliance policy
Configuration or policy supplied in the format we specify	Configuration or policy supplied in the format we specify	Your Business Requirements	Configuration or policy supplied in the format specified by us
Existing Firewall vendor and type	Existing IPS vendor and type	Your Traffic flow requirements	Existing Content Security appliance vendor and type
Proposed Firewall vendor and type if applicable	Proposed IPS vendor and type if applicable	Your Network architecture diagrams	Proposed Content Security appliance vendor and type if applicable
Ready access to your personnel to clarify or confirm information	Ready access to your personnel to clarify or confirm information	Any other relevant information	Ready access to your personnel to clarify or confirm information

The export formats we support

We can provide policy design details in specified formats. The formats we currently support are set out below:

4. Example IPOT (Telstra IP Ordering Tool). IPVAS, MDN, IPWAN
5. Example MSS Detailing Workbook (Telstra)
6. Standard formats (Non Telstra)
    d. CSV
    e. TXT
    f. XML

RESPONSIBILITIES GUIDE

SECURITY CONSULTING SERVICES

Limits on service scope

It is not possible to anticipate every service architecture and device setting. Accordingly, our service is subject to reasonable limits.

You will be limited to two changes within the scope of the initial engagement. However if any changes result in any or all of the requirements falling outside the initial scope Telstra reserves the right to review the fixed rate charge or convert the engagement into a customised solution.

The second limit on this solution relates to unusual requests beyond the usual scope of policy design work. We will advise you if a request is outside what we include in our standard service offering.

If you ask us to exceed these limits, additional charges may apply.

4. POLICY AUDIT & OPTIMISATION SERVICES

The devices we support

We will optimise the policies on your existing devices into a format suitable for management by SSF. The devices we will support are set out in the table below:

Supported Devices
Firewall
Cisco Security Appliances: PIX - ASA version 6.X to 8.4 Cisco FWSM Firstwave Checkpoint Security Gateway
Cisco IOS routers: Version 12.0 to 12.14, excluding X series
Juniper firewalls: Netscreen, SSG, ISG
Check Point: SmartCenter NG/NGX, Security Management R70 to R75 running on any platform, including: SecurePlatform Check Point IPSO (formerly Nokia) Crossbeam Linux Solaris Windows
Intrusion Prevention System
Cisco IPS Appliances: Cisco IPS 4200 Series
Content Security
Firstwave (Internet Protection Web and Internet Protection Mail)

RESPONSIBILITIES GUIDE

SECURITY CONSULTING SERVICES

Palo Alto

What we need from you

In order to carry out the optimisation services, we need the following inputs from you. You have to provide them in the time we specify, or if no time is specified, a reasonable time. We may not be able to perform the optimisation services until you provide us with the requested details.

Firewall	IPS	Content Security	Other
Accurate extract of existing Firewall policy	Accurate extract of existing IPS policy	Accurate extract of existing Content Security appliance policy	Your regulatory requirements (PCI, ISO27001, ISM, etc.)
Configuration or policy supplied in the format we specify	Configuration or policy supplied in the format we specify	Configuration or policy supplied in the format we specify	Your business requirements
Existing Firewall vendor and type	Existing IPS vendor and type	Existing Content Security appliance vendor and type	Your traffic flow requirements
Proposed Firewall vendor and type if applicable	Proposed IPS vendor and type if applicable	Proposed Content Security appliance vendor and type if applicable	Your network architecture diagrams
Ready access to your personnel to clarify or confirm information	Ready access to your personnel to clarify or confirm information	Ready access to your personnel to clarify or confirm information	Any other relevant information

How to extract files from devices

Some of the information we request from you can be extracted from your devices. The table in Appendix 1 sets out the instructions for common data-extraction tasks.

The export formats we support

We can provide policy optimisation details in specified formats. The formats we currently support are set out below:

7. Example IPOT (Telstra IP Ordering Tool). IPVAS, MDN, IPWAN
8. Example MSS Detailing Workbook (Telstra)
9. Standard formats (Non Telstra)
    g. CSV
    h. TXT
    i. XML

Limits on service scope

RESPONSIBILITIES GUIDE

SECURITY CONSULTING SERVICES

It is not possible to anticipate every service architecture and device setting. Accordingly, our service is subject to reasonable limits.

You will be limited to two changes within the scope of the initial engagement. However if any changes result in any or all of the requirements falling outside the initial scope Telstra reserves the right to review the fixed rate charge or convert the engagement into a customised solution.

The second limit on this solution relates to unusual requests beyond the usual scope of policy design work. We will advise you if a request is outside what we include in our standard service offering.

If you ask us to exceed these limits, additional charges may apply.

RESPONSIBILITIES GUIDE

SECURITY CONSULTING SERVICES

5. OPTIONAL SERVICES (INCLUDING SERVICE REQUEST CONSULTANCY)

The services we provide

You can ask us to provide services outside the scope of our standard security consulting service packages. For instance, we will review and where necessary optimise any requests you submit for professional services covered under the Optional Services. Once this process has been completed we will submit and manage the completion of these requests on your behalf.

What we need from you

In order to carry out the Optional Services, we need the following inputs from you. You have to provide them and any additional information we request in the time we specify, or if no time is specified, a reasonable time. We may not be able to perform the service request service until you provide us with the requested information.

- All device related information supplied in the agreed format
- Clear instructions regarding the work required
- Any specific requirements regarding timeframes or access requirements
- Access to your personnel or authorised representatives to clarify or confirm any of the supplied information

Limits on service scope

For all Optional Services we will agree a service scope with you. Any work outside that agreed scope will incur additional charges.

IT'S HOW WE CONNECT

RESPONSIBILITIES GUIDE

SECURITY CONSULTING SERVICES

RESPONSIBILITIES GUIDE

SECURITY CONSULTING SERVICES

1. Appendix 1

The following table sets out suggested ways of extracting relevant information from your devices. You are responsible for all activities you undertake with your devices and we exclude all liability for steps you take in reliance on this information.

Firewalls
Cisco PIX/ASA Firewalls
1. Connect to the device using SSH or telnet. 2. Enter the command *enable* and provide the enable password. 3. ***If you are connecting to a PIX firewall running version 6.x,*** enter the command *no pager*. 4. ***If you are connecting to an ASA firewall or a PIX firewall running 7.x or higher,*** enter the command *terminal pager 0*. 5. Enter the command *show run* and capture the output to a file called *config.txt*. 6. Enter the command *show route* and capture the output to a file called *route.txt*. 7. Send the above files (*config.txt and route.txt*) as an encrypted zip file to your Telstra Security Consultant.
Cisco IOS Routers
1. Connect to the IOS device using SSH or telnet. 2. Enter the command *enable* and provide the enable password. 3. Enter the command *terminal length 0*. 4. Enter the command *show run* and capture the output to a file called *config.txt*. 5. Enter the command *terminal ip netmask-format bit-count*. 6. Enter the command *show ip route* and capture the output to a file called *route.txt*. 7. Enter the command *show ip route* vrf [*vrfName*], where [*vrfName*] is the name of the router's VPN routing/forwarding instance. 8. Capture the output to a file called *vrf-routes.txt*. 9. Send the above files (*config.txt, route.txt and vrf-routes.txt*) as an encrypted zip file to your Telstra Security Consultant.
Cisco PIX/ASA Security Context
There are two options when connecting to security contexts on PIX/ASA devices: connecting as a device administrator, and connecting as a context administrator. If you connect as a context administrator, you will not be able to access system space or administrator contexts. We recommend connecting as a device administrator when possible.
To connect as the device administrator: 3. Connect to the device using SSH or telnet. 4. Enter the command *enable* and provide the enable password. 5. Enter the command *changeto context* [*contextName*], where [*contextName*] is the name of the security context. 6. Enter the command *terminal pager 0*. 7. Enter the command *show run* and capture the output to a file called *config.txt*. 8. Enter the command *show route* and capture the output to a file called *route.txt*. 9. Send the above files (*config.txt and route.txt*) as an encrypted zip file to your Telstra Security Consultant.
To connect as the context administrator:

1. Connect to the security context on the PIX/ASA device using SSH or telnet.
2. Enter the command *enable* and provide the enable password.
3. Enter the command *terminal length 0*.
4. Enter the command *show run* and capture the output to a file called *config.txt*.
5. Enter the command *show route* and capture the output to a file called *route.txt*.
6. Send the above files (*config.txt and route.txt*) as an encrypted zip file to your Telstra Security Consultant.

Cisco FWSM

The procedure to get configs from FWSM on Cisco devices differs depending on what OS the device is running.

To get configs from FWSM on Cisco devices running IOS:

1. Connect to the supervisor modules of the device using ssh or telnet.
2. Enter the command *enable* and provide the enable password.
3. Enter the command *session slot [moduleNumber] processor [processorNumber]*, where [*moduleNumber]* is the slot number for the FWSM module, and [*processorNumber]* is its processor number.
   Note: If you do not know the module number, run the supervisor command show modules to find it. The value for *processorNumber* is **1** in most cases, but can range from **0** to **9**.
4. Enter the password to start the FWSM session.
5. Enter the command *enable* and provide the enable password.
6. ***If you are connecting to a device running an FWSM version below 3.1.x,*** enter the command *no pager*.
7. ***If you are connecting to a device running FWSM version 3.1.x or higher,*** enter the command *terminal pager 0*.
8. Enter the command *show run* and capture the output to a file called *config.txt*.
9. Enter the command *show route* and capture the output to a file called *route.txt*.
10. Send the above files (*config.txt and route.txt*) as an encrypted zip file to your Telstra Security Consultant.

To get configs from FWSM on Cisco devices running CatOS:

1. Connect to the supervisor modules of the device using ssh or telnet.
2. Enter the command *enable* and provide the enable password.
3. Enter the command *session [moduleNumber]*, where [*moduleNumber]* is the slot number for the FWSM module.
   Note: If you do not know the module number, run the supervisor command show modules to find it.
4. Enter the password to start the FWSM session.
5. Enter the command *enable* and provide the enable password.
6. ***If you are connecting to a device running an FWSM version below 3.1.x,*** enter the command *no pager*.
7. ***If you are connecting to a device running FWSM version 3.1.x or higher,*** enter the command *terminal pager 0*.
8. Enter the command *show run* and capture the output to a file called *config.txt*.
9. Enter the command *show route* and capture the output to a file called *route.txt*.
10. Send the above files (*config.txt and route.txt*) as an encrypted zip file to your Telstra Security Consultant.

Juniper NetScreen Firewall

There are two options when connecting to Juniper NetScreen devices: connecting to a physical device, and connecting to a virtual system.

To get configs from a physical Juniper NetScreen firewall device:

1. Connect to the NetScreen device using SSH or telnet.
2. Enter the command *set console page 0*.
3. Enter the command *get config* and capture the output to a file called *config.txt*.
4. Enter the command *get route* and capture the output to a file called *route.txt*.
5. Enter the command *get service* and capture the output to a file called *service.txt*.

6. Send the above files (*config.txt, route.txt and service.txt*) as an encrypted zip file to your Telstra Security Consultant.

To get configs from a virtual Juniper NetScreen firewall system:

1. Connect to virtual system:
    a. Use the system management IP address to connect over SSH or Telnet, or in the HyperTerminal command-line interface.
    b. Enter the user name for the administrative user.
    c. Enter the password for the administrative user.
2. Enter the command *set console page 0*.
3. Enter the command *get config* and capture the output to a file called *config.txt*.
4. Enter the command *get route* and capture the output to a file called *route.txt*.
5. Enter the command *get service* and capture the output to a file called *service.txt*.
6. Send the above files (*config.txt, route.txt and service.txt*) as an encrypted zip file to your Telstra Security Consultant.

Check Point Firewalls

1. Enter **Expert Mode.**
2. Copy the configuration files from the remote Check Point management server to the local FSM server:
    a. Connect to the Check Point SmartCenter server using SSH or Telnet.
    Note: This is not the Smart Dashboard client GUI. Connect to the server directly.
    b. Find the directory on the server where the Check Point management server software is installed. This may be defined by the *$FWDIR* environment variable.
    c. Copy the file *$FWDIR/conf/objects_5_0.C* to your local file system.
    Note: There is also a file called *objects.C*. This is not the correct file.
    d. Copy the file *$FWDIR/conf/rulebases_5_0.fws* to your local file system.
3. Extract the routing table with the *cpstat* command:
    a. Connect to the Check Point management console.
    b. ***If you are connecting to a Provider1 system***, connect to the Customer Management Add-on (CMA) that manages the firewall.
    c. Enter *cpstat os -f routing -h [ipAddress] > route.txt*, where [*ipAddress]* is the IP address of the firewall module.
    Note: If this command is not available, use the procedure at the end of this section to manually obtain the routing table from the device.
4. Send the above files (*objects_5_0.C, rulebases_5_0.fws and route.txt*) as an encrypted zip file to your Telstra Security Consultant.

To manually obtain the routing table from a Check Point device:

1. Connect to the device using SSH or Telnet.
2. Run one of the following commands, depending on the host platform:
    - **SecurePlatform:** netstat -rn
    - **Check Point IPSO Appliance:** *show route*
    - **Nokia IPSO:** netstat -rn
    - **Linux:** netstat -rn
    - **Solaris:** netstat -rn
    - **Crossbeam UTM:** netstat -rn
3. Copy the output from the command to a text file called route.txt.