CLOUD FIREWALL SERVICE

Configuration Brief For Plus and Premium

Integra™

Technology you trust. People you know.

1. Introduction

This document helps Integra's Cloud Firewall Service (CFS) customers get started. It describes the available configuration choices so that you can gather the information your Sales Engineer will need to help you set up your Cloud Firewall Service. Integra uses this information to complete the CFS Configuration Questionnaire, initially provisioning CFS according to your requirements. As you gain experience with CFS, you can use the CFS Portal to change your reports and policies after initial provisioning. Additionally, Integra's staff can make changes at your request.

2. Email Reports

You have the option of selecting daily and/or weekly reports. The layout and format of these reports is subject to change at Integra's discretion. Daily reports are run at approximately 2:00AM on the data collected over the previous calendar day. It is not possible to change the time of day that the reports run or to run an ad-hoc report. Weekly reports run on Sunday morning on the previous calendar week of data recorded.

The CFS service level and reporting frequency determines which reports you will receive. The table below illustrates the differences.

Frequency	Plus	Premium	Report
Daily	X	X	24 Hour Application Report
Daily	X	X	24 Hour Threat Report
Weekly	X	X	7 Day Application Report
Weekly	X	X	7 Day Threat Report
Weekly	X	X	7 Day URL Report
Weekly	X	X	7 Day Application Statistics Report
Weekly		X	7 Day File Filtering Report

You may want to select both daily and weekly reports.

The Daily and Weekly Application Reports are the same, with the only exception being the time span of data contained within the report. The same holds true for the Daily/Weekly Threat Reports.

The URL Report, Application Statistics Report and the File Filtering Reports are only run once per week due to the overhead placed on the firewall to run these reports.

3. Policies

Integra has developed three levels of policy profiles: Moderate, Recommended, and High. These policy profiles are used to configure Application Visibility, Application Control, URL Filtering, and Antivirus/Anti-Spyware. Using the CFS Configuration Questionnaire, your Sales Engineer will select the profile of your choice for initial CFS provisioning. Keep in mind that High is not always better because it may block traffic required by your users. Integra suggests that your CFS initially be configured with Moderate or Recommend policies and then modified later, if needed.

3.1. Application Visibility

Application visibility shows the traffic allowed on your network in terms of specific applications. The CFS Portal's Application Visibility reports show which applications are being used in your organization and their associated risk rating. Application Visibility will inform your policy customization decisions. For example, you may find that a high risk application such as *baofeng* is consuming an inordinate amount of bandwidth. If so, you can use the CFS Portal to edit an Application Control policy to block it, or you can enlist the help of the Integra Network Operations Center.

Integra's Cloud Firewall Service is built on a network of firewalls from Palo Alto Networks. Palo Alto Networks maintains an online database of applications in their Applipedia application: http://apps.paloaltonetworks.com/applipedia/. You can reference Applipedia to understand an application's security risk. Applipedia includes categories, risks assessments, and descriptions for over 1,400 applications, and the list is continually updated.

Note: Integra's CFS products will be updated at least once a week with new application information from Palo Alto Networks. Some of the descriptions below assume knowledge of Applipedia categories and risk levels. The screen shot below displays the Applipedia information about the *baofeng* application.

3.2. Application Control

Application Control uses policies that allow you to control what application traffic is allowed on your network. This is achieved by processing Internet traffic through a series of rules. The rules filter and block unwanted and harmful traffic. Integra has defined three different levels of Application Control Policies that you can choose when your Sales Engineer initially configures your service, as detailed below. The controls that are described below are only a part of the overall rule structure in the policies, but are designed to give you control over the most commonly tailored configuration issues. If you need to change more specific things or see the rest of the rules in your policy, you can do so via the CFS Portal or integraCare.

Table 1 is an overview of the Moderate, Recommended, and High Application Policies.

Table 1. Application Control Profiles

Application Attribute	Moderate	Recommended	High
Risk Rating 5 and used by malware (with exceptions)	Block	Block	Block
Risk Rating 4 and used by malware (with exceptions)	Allow	Block	Block
Risk Rating 4 or 5 and has “vulnerabilities” characteristic (with exceptions)	Allow	Allow	Block

3.2.1. Moderate Application Control Policy Profile

The Moderate policy profile blocks applications that have an overall risk rating of 5 and have the characteristic “Used by Malware”, with the exceptions listed in Appendix A. If you need to block or unblock additional applications after initial provisioning, you can do so via the CFS Portal or integraCare.

3.2.2. Recommended Application Control Policy Profile

The Recommended policy profile is more restrictive and blocks applications that have an overall risk rating of 4 or 5 and that have the characteristic “Used by Malware”, with the following exceptions listed in Appendix A. If you need to block or unblock additional applications after initial provisioning, you can do so via the CFS Portal or integraCare.

3.2.3. High Application Control Policy Profile

The High policy profile is the most restrictive and blocks applications that have an overall risk rating of 4 or 5 and that have the characteristic “Used by Malware” or the characteristic “Vulnerabilities”, with the following exceptions listed in Appendix A. If you need to block or unblock additional applications after initial provisioning, you can do so via the CFS Portal or integraCare.

3.3. URL Filtering

CFS groups URLs into categories to efficiently control access to similar URLs, for example social-networking, pornography or online gambling. URL filtering restricts a user's access to a web site based on its category. Restrictions include the following actions:

- **Allow**: No action is taken to restrict or log access.
- **Alert**: Allows the user to access the web site, but adds an alert to the URL Filtering log.
- **Continue**: Allows the user to access the blocked page by clicking the "Continue" button on the blocked page. An alert is added to the URL Filtering log.
- **Block**: Blocks access to the page and adds an alert to the URL Filtering log.

The following table shows how the three different profile levels apply URL filtering.

Table 2. URL Filtering Profiles

URL Category	Moderate	Recommended	High
Abused Drugs	Alert	Continue	Block
Adult and Pornography	Alert	Continue	Block
Bot-nets	Block	Block	Block
Confirmed spam sources	Alert	Continue	Block
Hacking	Alert	Continue	Block
Keyloggers and Monitoring	Block	Block	Block
Malware sites	Block	Block	Block
Nudity	Alert	Continue	Block
Online gambling	Alert	Continue	Block
Phishing and other frauds	Block	Block	Block
Proxy and Anonymizers	Block	Block	Block
Spam URL	Block	Block	Block
Spyware and adware	Block	Block	Block

3.4. Antivirus

Antivirus profiles inspect protocol decoders like FTP or HTTP and alert or deny traffic as described below.

- **Alert**: Allows the traffic, but adds an alert to the Threat log.
- **Block**: Blocks the traffic and adds an alert to the Threat log.

- **Default**: Takes the default action specified by Palo Alto for the type of threat. These actions are customized for each threat, so the action taken may vary, but is designed to prevent that particular virus from infecting your systems.

Many organizations will deploy Integra's Cloud Firewall Service as part of a defense-in-depth strategy that includes end-point antivirus/anti-spyware, email antivirus/anti-spyware, or both. In this case, the CFS antivirus profiles should complement those controls, and you should understand how the CFS' antivirus capability blocks traffic containing viruses. The CFS can block traffic containing viruses before the traffic enters your network. If the CFS blocks mail containing a virus, it may look to your email program like a failure to complete the transfer of mail. This could cause your email program to request the transfer again, resulting in multiple retries until a timeout occurs. If your organization has other AV controls, you may want to select the Moderate or Recommended policy to prevent conflict.

The following table shows how the three different profiles react when a virus is detected, depending on the protocol.

Table 3. Antivirus Policy Profiles

Protocol	Moderate	Recommended	High
FTP	Default	Default	Default
HTTP	Default	Default	Default
IMAP	Default	Default	Block
POP3	Default	Default	Block
SMB	Alert	Default	Default
SMTP	Default	Default	Block

3.5. Anti-Spyware

Suspected spyware traffic is categorized according to severity as Critical, High, Medium, Low, or Informational. The CFS Anti-Spyware profiles allow, alert, or block spyware threats according to severity, as shown in the table below. The Default action is Palo Alto's assigned action based on their specific knowledge of individual spyware threats. This means that CFS may take a different action for two different spyware threats, even though they have the same severity level.

Table 4. Anti-Spyware Policy Profiles

Severity	Moderate	Recommended	High
Critical	Block	Default	Block
High	Alert	Default	Block
Medium	Alert	Default	Block
Low	Allow	Default	Alert
Informational	Allow	Default	Alert

3.6. File Filtering

Controls the flow of a wide range of file types by looking deep within the payload to identify the file types (as opposed to looking only at the file extension) to determine if the transfer of the file is allowed by policy. File blocking by type can be implemented on a per application basis which can, for example, allow an organization to enable the use of specific webmail applications like Gmail and allow attachments, but block the transfer of specific file types.

Integra has implemented a tiered approach to our file-blocking feature set. The following table indicates which files are blocked/alerted by service level.

Table 5. File Blocks and Alerts by Service Level

	Moderate	Recommended	High
Alert:	All File Types	All File Types	All File Types
Block Executable:	None	Bat, cmd, exe	Bat, cmd, exe
Block Common Files			Doc, docx, dwg Encrypted-doc Encrypted-docx Encrypted-office2007 Encrypted-ppt Encrypted-rar Encrypted-xls Encrypted-xlsx Encrypted-zip Msoffice Ppt, pptx Xls, xlsx Zip

3.7. Vulnerability

A rich set of intrusion prevention features blocks known and unknown network and application-layer vulnerability exploits from compromising and damaging enterprise information resources. Vulnerability exploits, buffer overflows, and port scans are detected using proven threat detection (IDS) and prevention (IPS) mechanisms.

- Protocol decoder-based analysis statefully decodes the protocol and then intelligently applies signatures to detect vulnerability exploits.

- Protocol anomaly-based protection detects non-RFC compliant protocol usage such as the use of overlong URI or overlong FTP login.
- Stateful pattern matching detects attacks across more than one packet, taking into account elements such as the arrival order and sequence.
- Statistical anomaly detection prevents rate-based DoS flooding attacks.
- Heuristic-based analysis detects anomalous packet and traffic patterns such as port scans and host sweeps.
- Other attack protection capabilities such as blocking invalid or malformed packets, IP defragmentation and TCP reassembly are utilized for protection against evasion and obfuscation methods employed by attackers.
- Custom vulnerability or spyware phone home signatures that can be used in either the anti-spyware or vulnerability profiles.

Integra has implemented a tiered approach to our IDS/IPS feature set. The following table indicates which threat levels are blocked/alerted by service level.

Table 6. Threat Level Blocks and Alerts by Service Level

	IDS Only	IDS-IPS Moderate	IDS-IPS High
Alert (IDS):	All Threat Levels	All Threat Levels	All Threat Levels
Action (IPS):	N/A	Default All Threat Levels	Block on Medium, High and Critical Threat Levels. Default on Informational and Low Threat Levels.

4. Network Addresses Translation

Integra will automatically assign the appropriate-sized block of IP addresses to you, up to a /28, and you can use outbound Network Address Translation (NAT) with it, if needed. If you need an IP address for inbound NAT, please complete the section “Inbound Network Address Translation Requirements” on the questionnaire. Integra will allocate and assign one or more public IP addresses for you to NAT inbound traffic to your organization’s Internet-facing services. Each IP address can be NATed at the port level, which allows a single IP address to be assigned to multiple services, if needed. If you require more than a /28 of IP addresses, you must request them using Integra’s IP Justification Form. Additional fees apply.

Integra registers with the American Registry for Internet Numbers (ARIN) to obtain IP addresses. ARIN assigns and allocates IP addresses to end users and Internet Service Providers (ISPs) located in North America. ARIN requires all end users and ISPs to document their use of IP addresses.

To adequately provide this information to ARIN, Integra requires all customers to complete the IP justification form for the use of additional IP addresses. Integra abides by ARIN's policies to promote conservation and efficient use of IP address space.

Please note: You must contact Integra Customer Care to obtain an order number prior to completing the IP Address Justification Form. You will be prompted to enter your order number when completing the form. The IP Address Justification Form is located at http://www.integratelecom.com/care/ispsupport/ip_just.php.

5. Syslog Configuration

CFS can forward syslog messages to your syslog server. If you want to enable this capability, please provide your Sales Engineer with the syslog configuration information for your syslog server.

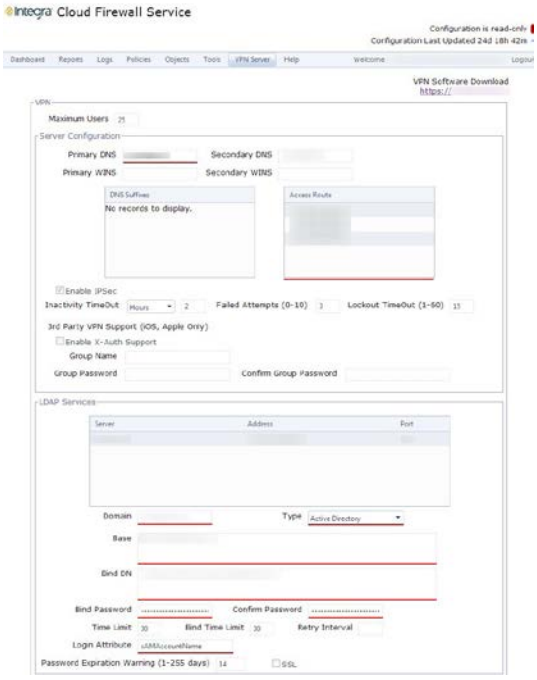
6. Remote Access VPN Client Configuration

Remote Access VPN is an optional add-on service available to both CFS Plus and CFS Premium customers and is sold on a per simultaneous user connection basis. Remote Access VPN is supported via the GlobalProtect client software on the following Operating Systems: Microsoft Windows XP, Microsoft Windows Vista, Microsoft Windows 7, Apple Mac OS X (Snow Leopard, Lion) and Apple iOS (users built-in IPSec client).

If you have purchased the optional VPN Client, you will need to tell us whether you are using the LDAP/Active Directory or RADIUS. When Remote Access VPN Client users initiate a connection, they will be authenticated using your company's LDAP/Active Directory or RADIUS directory service. Additionally, you will need to provide any network routes that Remote Access VPN Client users will need to use to access your network resources; e.g. 192.168.125.0/24. Note, it is recommended that your network not include network routes, such as 192.168.1.1, that are likely to be used by the remote user's local network.

6.1. Customer's Configuration Responsibilities for VPN Client

After logging into the CFS Portal you will need to configure CFS to work with your specific directory service. The following screen shot shows you the information you will need to enter to configure CFS to authenticate remote users against your LDAP/AD directory service. It is recommended that you have this information on-hand when configuring the capability. The fields underlined in red are required. These requirements are also mentioned in the CFS Portal User Guide.



7. Site-to-Site VPN IPSEC Tunnel Configuration

Virtual Private Networks (VPNs) allow systems to connect securely over a public network as if they were connecting over a local area network (LAN). The IP Security (IPSec) set of protocols is used to set up a secure tunnel for the VPN traffic, and the private information in the TCP/IP packets is encrypted when sent through the IP Sec tunnel.

8. PTR/MX Record Creation

If you host your own mail server and your public IP address changes, you will need to create a new PTR/MX Record to facilitate reliable email delivery. Creating the PTR/MX Record needs to coincide with the IP address change during the cutover. If you use a DNS hosting service, such as GoDaddy.com, you may want them to make the change on your behalf.

For immediate PTR/MX Record creation, please contact ISP support 2 hrs. prior to turn-up at: 866-871-1114.

Alternatively, you may submit a request form at: http://www.integratelecom.com/care/ispsupport/reverse_dns.php. If you elect to submit a request via web link, you should allow 24-48 hrs. turn-around for DNS (MX/PTR) to propagate and resolve. You will need to provide the host name and IP address for your mail server.

Appendix A. Application Exceptions

Note: Application exceptions may change at Integra's discretion, at any time.

Moderate Application Control Policy Exceptions

ftp, google-docs, http-audio, http-video, nntp, rss, skype, smtp, yahoo-im, and youtube

Recommended Application Control Policy Exceptions

Blackberry, DNS, Facebook, Flash, FTP, Gmail, Google-docs, Google-talk, h.323, Hotmail, http-audio, http-video, icmp, imap, ms-exchange, msn, myspace, nntp, outlook-web, pop3, pptp, rss, sip, skype, smtp, ssh, ssl, tftp, twitter, web-browsing, yahoo-im, and youtube

High Application Control Policy Exceptions

Adobe-connect, Blackberry, DNS, Facebook, Flash, FTP, Gmail, Google-docs, Google-talk, h.323, Hotmail, http-audio, http-video, icmp, imap, ms-exchange, msn, myspace, nntp, outlook-web, pop3, pptp, rss, sip, skype, smtp, ssh, ssl, tftp, twitter, web-browsing, yahoo-im, and youtube