

Cloud Firewall Service User Guide

April 2019



Copyright

Under copyright laws, this publication may not be reproduced in any form in whole or in part, without the prior written consent of Allstream Business, Inc. The information contained in this publication is proprietary and confidential and is subject to change without notification. Users should contact Allstream Business, Inc. to ensure that they have the most up to date version.

© 2019 Allstream Business, Inc. All rights reserved.

Contents

- Introduction** _____ **1**
- System User Accounts _____ 1
- CFS Features _____ 1
- Accessing the CFS Portal _____ 2
- Passwords _____ 2
- Web Access Security Messages _____ 2
- Navigating the CFS Portal _____ 2
- Timestamps and Time Zones _____ 3
- Using the Dashboard _____ 3
- Understanding Security Policies and Rules** _____ **3**
- Rule Order and Data Flow _____ 4
- Default Rule Set _____ 4
- MyCompany Denied Apps Rule _____ 4
- MyCompany Allowed Apps Rule _____ 4
- Web Browsing Applications _____ 5
- Risk 5 Exceptions _____ 5
- Risk 5 Block _____ 5
- General Internet L4 _____ 5
- Network Vulnerabilities _____ 5
- Best Practices – Configuring Rules _____ 5
- Managing Security Rules _____ 6
- Working with Network Address Translation (NAT) Rules _____ 6
- 1:1 NAT Model _____ 7
- Managing NAT Rules _____ 7
- Working with Profiles** _____ **8**
- Default Profiles _____ 8
- Anti-Spyware Profile _____ 8
- Antivirus Profile _____ 9
- URL Filtering Profiles _____ 9
- Changing the Default Profiles _____ 10
- Managing URL Filtering Profiles _____ 10
- Managing File Blocking Profiles _____ 11
- Applying a File Blocking Profile to a Security Rule _____ 13

| | |
|---|-----------|
| Managing Vulnerability Protection (IDS/IPS) Profiles _____ | 13 |
| Protection Levels _____ | 13 |
| Applying IDS/IPS Profiles _____ | 13 |
| Working with Objects and Groups _____ | 14 |
| Managing Service Objects _____ | 14 |
| Managing Addresses for Objects _____ | 14 |
| Managing Address Groups _____ | 15 |
| Managing Application Groups _____ | 16 |
| Committing Changes _____ | 17 |
| Monitoring Settings _____ | 17 |
| Resetting IPSec Tunnel Connections _____ | 17 |
| Monitoring User ID Agents _____ | 18 |
| Monitoring GlobalProtect Users _____ | 18 |
| Viewing Users _____ | 18 |
| Disconnecting Remote Users _____ | 18 |
| Appendix A: Risk Calculations _____ | 19 |
| Understanding Application Risks _____ | 19 |
| Researching Risk Levels for a Single Application or Web Site _____ | 19 |
| Researching Risk Levels for a Group of Applications or Web Sites _____ | 20 |
| App-ID Metadata _____ | 20 |
| Risk Calculation _____ | 21 |
| Appendix B: Obtaining Base DN and Bind DN for Active Directory Servers _____ | 22 |
| Base DN _____ | 22 |
| Bind DN _____ | 22 |
| Appendix C: Application Policy Exceptions _____ | 23 |
| Moderate Application Control Policy Exceptions _____ | 23 |
| Recommended Application Control Policy Exceptions _____ | 23 |
| High Application Control Policy Exceptions _____ | 23 |

Introduction

As an outsourced security solution, Allstream's Cloud Firewall Service (CFS) delivers the protection your business requires without demanding a capital expenditure or a staff of internet security experts. The elements that make up the CFS deliver a highly-secure perimeter around your business internet access. With a single point of control that monitors and protects your business from the harm of dangerous internet incidents, CFS includes:

- An application-aware firewall
- Web site filtering
- Antivirus and anti-spyware
- Customizable policies
- A Virtual Private Network (VPN) client for remote users

You can rely on Allstream to thoroughly oversee and update your services and defend your network from internet threats. If you need help with the CFS portal, user logins, or changes to your default firewall settings, contact Allstream's Customer Support.

System User Accounts

To access the CFS, you must first have a portal user account. If you do not already have an account, contact your System Administrator for assistance. If you are a System Administrator and need to set up user accounts, contact Customer Support for more information.

CFS Features

The CFS provides the following features:

| Feature | Description |
|------------------------|---|
| Security Policies | Application control policies specify whether the CFS blocks or allows individual applications and/or files. The behavior depends on the Palo Alto Networks® application risk rating and the policy profile you selected when you ordered CFS. For assistance customizing control policies, contact Customer Care. |
| URL Filters | URL filtering allows or restricts access to web sites based on the URL category, such as social networking or online gambling. Depending on the policy profile you selected, a web site is allowed, allowed with an alert logged, allowed when a user clicks Continue, or completely blocked. If you need to block a URL category or a particular URL, contact Customer Care. |
| Antivirus Protection | Antivirus protection either blocks traffic or records an alert if a virus is detected. The action taken depends on both the protocol (such as FTP or HTTP) and the policy profile you selected on the CFS Configuration Questionnaire. If you need to change the action for a protocol, contact Customer Care. |
| Anti-Spyware Detection | Anti-spyware detection blocks traffic, records an alert, or allows traffic if spyware is detected. The action taken depends on the severity level Palo Alto Networks' knowledge of the particular spyware, and the policy profile you selected. To adjust the behavior or anti-spyware detection, contact Customer Care. |
| NAT Policies | Network Access Translation (NAT) is available for inbound or outbound traffic. The CFS portal supports 1:1 NAT policies only. If you require NAT policies beyond 1:1, contact Customer Care. |
| Public IP Address | By default, Allstream provides one public IP address that can be used for outbound traffic. Additional IP addresses for inbound traffic may be available depending on system performance requirements. |

Accessing the CFS Portal

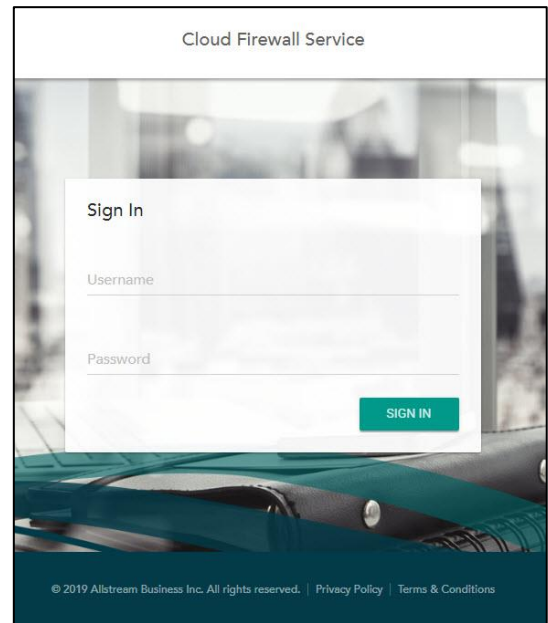
To access the CFS portal:

1. Use a web browser to visit <https://cfs.allstream.com>. The **Sign In** page displays.
2. Enter your username and password and click **SIGN IN**.

Note: If this is your first time signing in to the portal, you are prompted to change your password.

Passwords

Your initial username and password were provided to you in a welcome email. When you sign in to the portal for the first time, you are prompted to change your password. Passwords must be at least six (6) characters long. After changing your password, you must sign in again using the new password. If you need assistance with additional user accounts or forgotten passwords, contact Customer Care.

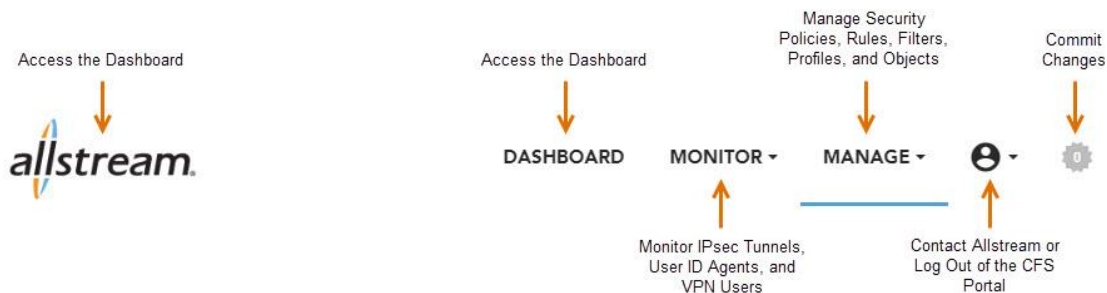


Web Access Security Messages

CFS provides various levels of web site access controls used to block some web sites that are considered to have inappropriate content (for example, online gambling or adult entertainment) or sites that are untrusted due to potential risks for malware, spyware, or viruses.

Depending on your security profile, CFS returns to its default setting and redisplay the warning if users signed in to the CFS continue to access a blocked web site.

Navigating the CFS Portal



The CFS portal provides a navigation bar for quick access to application features and tasks:

- **DASHBOARD**—the default home page where you can view and manage security rules, filters, and objects
- **MONITOR**—used by System Administrators to reset IPsec Tunnels, view User ID agents, and sign out VPN (GlobalProtect) users
- **MANAGE**—used by System Administrators to manage security rules and display information regarding object addresses and application groups
- **User Profile**—contact Allstream or log out of the portal
- **Commit Changes**—click to commit any policy, rule, filter, profile, and object changes to the CFS (this icon is inactive if no changes to commit exist)

Timestamps and Time Zones

The CFS portal displays all dates and timestamps in the time zone where the physical CFS Firewall is located. If you are not sure of the firewall's location, contact Customer Care. The **Commit Queue** is an exception and always displays dates in Pacific Standard Time (PST).

Using the Dashboard

The **Dashboard** is the default home page where you can quickly view and manage rules and profiles within the CFS. You can use the **Search** and **Add** icons at the top of each section to locate and create new rules and profiles, or you can click a specific rule or profile to make changes or remove them from the CFS.

Once changes to the CFS are made, the **Dashboard** displays the affected rules or policies in *Italics* until those changes have been committed. For more information about committing changes, see [Committing Changes, page 17](#).

Understanding Security Policies and Rules

Security policies determine whether to block or allow network traffic through the firewall into your internal network and intranet (trusted zone) or from your intranet to the internet (untrusted zone). Security zones are used to group interfaces according to the relative risk of the traffic they carry. For example, an interface connected to the internet is in an “untrusted” zone, while an interface connected to the internal network is in a “trusted” zone. Using firewall security policies, you can control which web sites and URLs are accessible, which applications are acceptable to use, and which source and destination security zones, addresses, and application services (such as HTTP) are accessible and pose a minimal security threat. Traffic between trusted and untrusted security zones is blocked until at least one rule is added to allow traffic between the two zones.

A rule is a set of specific instructions used within security policies to provide information on what web sites, applications, and services to block. There are several components defined in the rule that define the types of incoming and outgoing traffic that is allowed or denied, specify known applications, or are of high-risk of spyware and viruses.

Each rule contains the following information:

- **Name**—describes the rule for ease of organization
- **Source**—defines where the traffic is coming from, such as an IP address range or zone
- **Users**—specifies the user or users to which the rule applies
- **Destination**—defines where the traffic is headed, such as an IP address range or zone
- **Application**—determines the applications to filter (individual or group)
- **Service**—determines the service to filter (for example, block the https side of an application while allowing http for the same application)
- **Action**—the action to take (allow or deny) on traffic that matches the rules
- **Profile**—the levels, if any, of antivirus, anti-spyware, or URL filtering to perform on the rule

These components, when combined into a rule, and with those rules placed in the correct order, will filter your internet traffic and provide protection from virus infection and attack.

Rule Order and Data Flow

Security policies can be as general or specific as needed. The policy rules are compared against incoming and/or outgoing traffic in sequence, and because the first rule that matches the traffic is applied, the more specific rules must precede a rule for all applications if all other traffic-related settings are the same. If the traffic does not match any of the rules, the traffic is blocked.

When data from an untrusted zone is received by your company network, it is matched against a set of rules in the firewall to determine if the data is allowed to pass through. The rules are checked in the order that they are listed. When a rule is matched, the data stops being examined and is either sent to the trusted zone or denied by the firewall.

Default Rule Set

Within the CFS firewalls, there are a few rules not displayed on the portal, and they cannot be changed by you. These can change at Allstream's discretion and are to always ensure access to the firewall, even if you inadvertently block access through a rule. The first policy is a pre-rule that is applied to all traffic before your company's custom rules. It allows access to the Allstream Domain Name Server (DNS) and CFS portal that you, as a customer, are using.

The second policy is a post-rule that is applied to all traffic after your custom rules and allows a few networking utilities and VPN services (such as Citrix or GoToMyPC) to aid in troubleshooting.

Each of the following rules is protected by the level of antivirus, anti-spyware, and URL filtering you selected on your questionnaire. While some of the applications allowed through the firewall are labeled as vulnerable or contain high-risk levels, they are not all bad and should not be blocked. Some of the applications are required for many business functions to continue working properly, therefore, these applications are allowed through the firewall with somewhat restricted access and are monitored by the security profiles. To research risk levels for applications or URLs, visit Palo Alto Networks' Appliedia site at <https://appliedia.paloaltonetworks.com>.

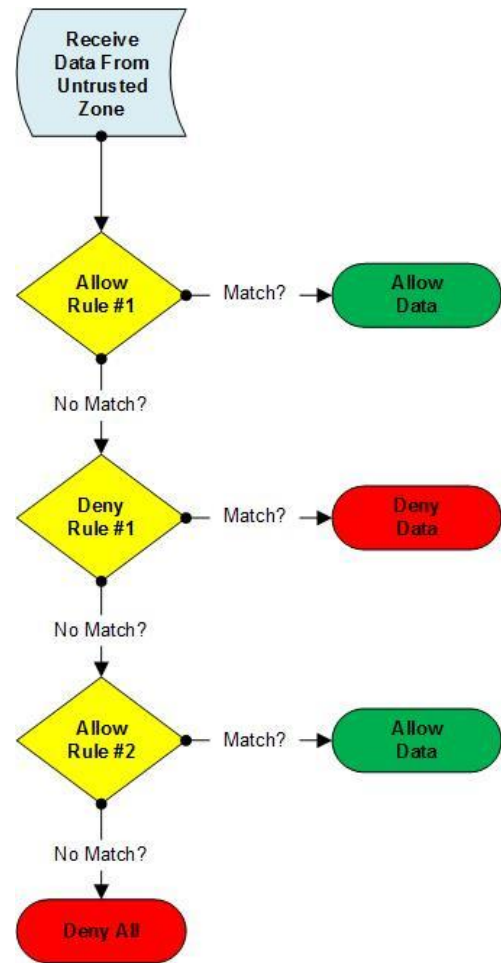
In most cases, it is best practice not to edit the default rules. Allstream has provided an extra allow and deny rule with associated customizable groups that allow you to add the applications you want to allow or block. These rules are described below.

MyCompany Denied Apps Rule

This rule acts as a container for any applications you want to block. It refers to the predefined *MyCompany Denied Apps Grp* application group. You can add applications to this group to prevent their use on your network. It is listed at the top of the rule set so that the applications you block are not inadvertently allowed by another rule.

MyCompany Allowed Apps Rule

This rule acts as a container for any applications you want to allow. It refers to the predefined *MyCompany Allowed Apps Grp* application group. You can add applications to this group to allow them on your network. It is listed before the other default rules. Be careful when allowing applications this way, especially if using a filter, as you may inadvertently bypass the rules that protect your network.



Web Browsing Applications

This rule allows traffic generated by Flash, SSL, and web-browsing from the trusted zone to flow to the outside.

Risk 5 Exceptions

This rule allows traffic generated by the Real-Time Messaging Protocol (RTMP) and the applications within the *Risk 5 Vulnerabilities* filter from any source zone/user to flow to any destination zone/user running any service. The *Risk 5 Vulnerabilities* filter contains all the applications that are risk level 5 and are characterized by being vulnerable but should still be allowed.

Risk 5 Block

This rule blocks traffic generated by the applications within the *Risk 5 Used by Malware* filter from any source zone/user to flow to any destination zone/user running any service.

General Internet L4

This rule allows traffic from any source zone/user to flow to any destination zone/user running HTTP or HTTPS.

Network Vulnerabilities

This rule allows traffic generated by Jabber, vnc-base, and the applications in the *Networking Risk 1-3* filter from any source zone/user to flow to any destination zone/user running any service. The *Networking Risk 1-3* filter contains all of the applications that are risk levels 1 through 3 and fall into the networking category.

Best Practices – Configuring Rules

The following are several examples of common rule actions you may need to make. If you are not sure which applications may need to be allowed or blocked in your network, you can research various application and URL threat levels on Palo Alto Networks' Applopedia site at <https://applopedia.paloaltonetworks.com>.

When creating rules, consider the following best practices:

- Order the “allow” policies from most to least specific and the “deny” policies from least to most specific.

For example, to deny peer-to-peer file sharing but allow the Azureus application through the firewall, your policies must have an “allow” rule for Azureus before the broader rule that blocks all peer-to-peer file sharing.







Note: It is important to list allow and deny rules in the correct order to avoid errors. In most cases, when a problem exists with a program being unable to access either untrusted or trusted zones, it is because the order in which the rules are applied is blocking the program from passing through the firewall. Always check rule order first for unexpected allow/deny behavior.

- Use explicit “allow” rules for applications that are needed to prevent any firewall-related errors with user programs and applications.
- When a rule is matched by either “allow” or “deny”, no further rules are examined. Be careful putting broad “allow” rules near the top as they may permit too much traffic and cause any deny rules below them to go unused.




Managing Security Rules

To manage security rules, from the **MANAGE** drop-down list in the navigation bar, select **Security Rules**. The **Security Rules** page displays a list of existing security rules.

The **Security Rules** page allows you to perform the following rule management tasks:

- Click a rule in the list to display the **Create/Edit Security Rule** page. This page allows you to modify or remove the rule.
- Click the **Search** icon  to search for a specific rule in the list.
- Click the **Add** icon  to create a new rule.
- Check the box next to a rule in the list and click the **Up** or **Down** icons   to reprioritize the rule.
- Check the box next to a rule in the list and click the **Enable** icon  to enable the rule or the **Disable** icon  to disable the rule.

Security rule properties include the following:

| Attribute | Description |
|------------------------------------|--|
| Name (required) | A descriptive name for the rule. Names can contain up to 31 alphanumeric characters and may include symbols and spaces. |
| Description | A short description of the rule. Descriptions can contain up to 255 alphanumeric characters and may include symbols and spaces. |
| Source | Zone: Select a zone from the drop-down list that identifies where traffic comes from. Address: Select an address from the drop-down list that identifies where traffic comes from. To add a new address, click the plus sign  . Negate: Check this box to nullify the source. |
| Users | Select a user from the drop-down list or search for a user to which the rule applies. |
| Destination | Zone: Select a zone from the drop-down list that identifies where the traffic flow ends. Address: Select an address from the drop-down list that identifies where the traffic flow ends. To add a new address, click the plus sign  . Negate: Check this box to nullify the destination. |
| Applications & Services | The applications and services you want to control. Select one or more applications and services from the drop-down lists or search for those to which the rule applies. To add a new service, click the plus sign  . |
| Action | Specify whether the rule is to Allow or Deny traffic based on the criteria defined in the rule. When the rule is set to Allow , additional protection from threats, vulnerabilities and data leaks is provided by selecting security profiles from the appropriate drop-down lists. |

Important: After creating or modifying a rule, you must commit your changes for them to take effect. For more information, see [Committing Changes, page 17](#).

Working with Network Address Translation (NAT) Rules

Each computer and device within an IP network is assigned a unique IP address that identifies the host. Using NAT, you can enhance your network security by limiting the direct connectivity that is possible between internal network hosts and the outside, making it more difficult for outside hackers to “map” your internal network.

1:1 NAT Model

CFS uses a 1:1 NAT model to create a fixed translation of a routable IP address to a private IP address. Because the mapped address is the same for each consecutive connection, 1:1 NAT allows unidirectional connection initiation to the host for a single IP address (if an access rule exists that allows it).

Note: The CFS portal supports 1:1 NAT policies only. If you require other NAT policies, contact Customer Support.







Managing NAT Rules

NAT rules are used to specify which untrusted IP addresses can pass through the firewall with an assigned translated IP address used at the receiving port. CFS used service objects that define the receiving port address (trusted site); NAT rules define which untrusted port is directed to which trusted internal port.


The following information describes how to manage a NAT rule to be used with a service object. For information about service objects, see [Working with Objects and Groups, page 14](#).

To manage NAT rules, from the **MANAGE** drop-down list in the navigation bar, select **NAT Rules**. The NAT Rules page displays a list of existing NAT rules.

The NAT Rules page allows you to perform the following rule management tasks:

- Click a rule in the list to display the **Create/Edit NAT Rule** page. This page allows you to modify or remove the rule.
- Click the **Search** icon  to search for a specific rule in the list.
- Click the **Add** icon  to create a new rule.
- Check the box next to a rule in the list and click the **Up** or **Down** icons   to reprioritize the rule.
- Check the box next to a rule in the list and click the **Enable** icon  to enable the rule or the **Disable** icon  to disable the rule.

NAT rule properties include the following:

| Attribute | Description |
|--|--|
| Name (required) | A descriptive name for the rule. Names can contain up to 31 alphanumeric characters and may include symbols and spaces. |
| Description | A short description of the rule. Descriptions can contain up to 255 alphanumeric characters and may include symbols and spaces. |
| External/WAN IP Address (required) | The external IP address to which you want to apply NAT policies. The external or WAP IP address is limited to one address. |
| Service (required) | Select the name of the service object you want to use for the rule from the drop-down list. To apply the rule to all traffic for the IP address entered for the Original Packet Destination Address, select Any . To add a new service, click the plus sign  . |
| Internal Translated IP Address (required) | Select the IP address used as the (final) translated destination IP address from the drop-down list. The internal translated IP address is limited to one address. |

Important: After creating or modifying a rule, you must commit your changes for them to take effect. For more information, see [Committing Changes, page 17](#).

Working with Profiles

A *policy* refers to the combined sets of rules, filters, and groups that create the overall instructions that govern what traffic is allowed or blocked by the firewall. Each rule is a specific instruction that tells the firewall to block an application, service, or combination thereof. Each rule is assigned a *profile*. The profile refers to the specific settings of *Moderate*, *Recommended*, or *High* for the antivirus, anti-spyware, and URL filtering actions that are applied to a rule.

The **MANAGE** drop-down list of the CFS portal is used to display and edit the rules and filters that define what CFS blocks, allows, and monitors for your firewall. From the **MANAGE** drop-down list, you can view the existing set of rules and add, delete, disable, or change the order of the rules in the list. Extra care must be taken when manipulating the rules in this panel. Improper rules or rules that are incorrectly sequenced can potentially leave your network vulnerable to attacks or block necessary traffic.

Note: Changing the rules options for a policy directly alters access to the Internet. Please read the following sections carefully before making any changes. If you are unsure of what may result from changes you want to make, contact Customer Support.

Before you create or edit rules and filters, refer to [Understanding Application Risks, page 19](#) for information about how risk levels are assigned to applications and web sites.

Default Profiles

The anti-spyware, antivirus, and URL filtering profiles attached to rules are assigned at the time your default rules are set up and are based on the information provided in the CFS Configuration Questionnaire. Each profile has three settings: *Moderate*, *Recommended*, and *High*. They are built into the default rule set based on your choices, but you may find it necessary to change them at a later time or add them to future rules you create.

Note: The default actions for profiles are customized to mitigate each threat in a way specific to that threat. Some threats may be blocked, some threats may send a rest to the server involved, or some threats may require a variety of similar actions to occur.

Anti-Spyware Profile

The Anti-Spyware security profile blocks spyware from accessing your network in a variety of ways depending on the severity threshold you define for your security zone. For example, you may want to have a lower threshold when going from the trusted zone (your network) to the untrusted zone (the Internet) to speed up traffic flow. The actions taken for each level of spyware threat are shown below, sorted by the level of protection selected:

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

Spyware severity thresholds include:

- **Moderate:** Least restrictive
- **Recommended:** Default defined actions are taken on all levels of spyware
- **High:** Most restrictive

Actions taken on known spyware include:

- **Allow:** Permits the application through the firewall
- **Alert:** Creates a notification in the threat log
- **Block:** Denies access to the network and drops the packet
- **Default:** Takes the default action that is specified internally

Antivirus Profile

The Antivirus security profile is used to identify which applications are inspected for viruses and what action is taken when a virus is detected. The profile inspects all of the listed protocol decoders and signatures for viruses and blocks or generates an alert depending on which profile is used. The difference between each security policy, based on the protocol used to transfer data, is shown below:

| Severity | 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 |

Antivirus severity thresholds include:

- **Moderate:** Least restrictive
- **Recommended:** Maintains a balanced approach to antivirus protection
- **High:** Most restrictive

Actions taken on known spyware include:

- **Allow:** Permits the application through the firewall
- **Alert:** Creates a notification in the threat log
- **Block:** Denies access to the network and drops the packet
- **Default:** Takes the default action that is specified internally

URL Filtering Profiles

CFS groups URLs into categories to efficiently control access to similar URLs (for example, social networking or pornography). URL filtering restricts a user from gaining access to a web site based on its category. Restrictions work as follows:

| 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 |

URL filtering severity thresholds include:

- **Moderate:** Least restrictive
- **Recommended:** Maintains a balanced approach to URL filtering protection
- **High:** Most restrictive

Actions taken on known spyware include:

- **Alert:** Creates a notification in the threat log
- **Block:** Denies access to the URL
- **Continue:** Warns the user about the site and gives the option to continue while access is logged

Changing the Default Profiles

While altering the default rules is not encouraged, you may want to change the level of protection offered by the anti-spyware, antivirus, or URL filtering profiles.

To change the protection level for a rule:



1. From **MANAGE** drop-down list in the navigation bar, select **Security Rules** to display a list of rules.
2. Click the default rule you want to modify.
3. When the rule is set to **Allow**, additional protection from threats, vulnerabilities and data leaks is provided by selecting security profiles from the appropriate drop-down lists.
4. Click **OK**.
5. Commit the changes. For more information, see [Committing Changes, page 17](#).

Managing URL Filtering Profiles

Custom URL filtering profiles allow you to add filtering controls to selected sites. When a URL filtering profile is applied to a security rule, CFS filters the site according to the profile settings, either allowing or restricting site access. Once a URL filtering profile is created, it may be applied to a security rule. For more information, see [Understanding Security Policies and Rules, page 3](#).



To manage URL filtering profiles, from the **MANAGE** drop-down list in the navigation bar, select **URL Filtering**. The **URL Filtering** page displays a list of existing filters.

The **URL Filtering** page allows you to perform the following filter management tasks:

- Click a filter in the list to display the **Create/Edit URL Filtering Profile** page. This page allows you to modify or remove the profile.
- Click the **Search** icon  to search for a specific profile in the list.
- Click the **Add** icon  to create a new profile.

URL filtering profile properties include the following:

| Attribute | Description |
|------------------------|---|
| Name (required) | A descriptive name for the profile. Names can contain up to 31 alphanumeric characters and may include underscores, hyphens, spaces, and periods. Symbols cannot be used. |
| Description | A short description of the profile. Descriptions can contain up to 255 alphanumeric characters and may include symbols and spaces. |

| Attribute | Description |
|-----------------|--|
| Domain | <p>URL: The URL of the web site you want to filter.</p> <p>Action: Select Allow or Block from the drop-down list to determine the action to take for the URL.</p> <p>Click ADD to add the domain and associated action to the profile. You may add any number of domains to the profile.</p> <p>Added Domains: Displays a list of all domains added to the profile. To remove a domain, check the box next to the domain you want to remove and click the Delete icon .</p> |
| Category | <p>Categories: Select a category for the profile from the drop-down list.</p> <p>Action: Select Block, Allow, Alert, or Continue from the drop-down list to determine the action to take for the category.</p> <p>Click ADD to add the category and associated action to the filter. You may add any number of categories to the profile.</p> <p>Added Categories: Displays a list of all categories added to the profile. To remove a category, check the box next to the category you want to remove and click the Delete icon .</p> |

Important: After creating or modifying a profile, you must commit your changes for them to take effect. For more information, see [Committing Changes, page 17](#).

Managing File Blocking Profiles

Note: File blocking profiles are available only in CFS Premium subscriptions.



If you subscribe to CFS Premium, you can include File blocking profiles in your security rules that alert the user or block the transfer of selected file types (as opposed to looking at file extensions only) when those file types are uploaded, downloaded, or otherwise detected. File blocking by type is implemented on a per-application basis. This allows organizations to use specific webmail applications such as Gmail and allow attachments but block the transfer of specific file types.

The CFS file blocking feature has three predefined file blocking profiles as indicated in the table below. You may use these predefined profiles or create your own if you need more customization.


| Action | 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 | None | None | 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 |

To manage file blocking profiles, from the **MANAGE** drop-down list in the navigation bar, select **File Blocking**. The **File Blocking** page displays a list of existing file blocking profiles. Once a profile is created, it may be applied to your security rules. For more information, see [Applying a File Blocking Profile to a Security Rule, page 13](#).

The **File Blocking** page allows you to perform the following profile management tasks:

- Click a profile in the list to display the **Create/Edit Security Rule** page. This page allows you to modify or remove the profile.
- Click the **Search** icon  to search for a specific profile in the list.
- Click the **Add** icon  to create a new profile.

File blocking profile properties include the following:

| Attribute | Description |
|------------------------|---|
| Name (required) | A descriptive name for the profile. Names can contain up to 31 alphanumeric characters and may include symbols and spaces. Profile names display in the list of file blocking profiles available when defining security rules. |
| Description | A short description of the rule. Descriptions can contain up to 255 alphanumeric characters and may include symbols and spaces. |
| Rules | <p>Rule: A descriptive name for the rule you want to apply to the profile.</p> <p>Applications: Select one or more applications from the drop-down list to apply to the rule.</p> <p>Note: CFS defaults to <i>Any</i>. This default setting essentially blocks all applications from passing through the firewall. To create an effective file blocking profile, you must choose which applications to block and which to allow through the firewall.</p> <p>File Types: Select one or more file types from the drop-down list to apply to the rule. To block all Windows Portable Executable files, select PE from the drop-down list.</p> <p>Note: CFS defaults to <i>Any</i>. This default setting essentially blocks all files from passing through the firewall. To create an effective file blocking profile, you must choose which file types to block and which to allow through the firewall.</p> <p>Direction: Select the file type direction to which the rule action applies. For example, to apply an action to selected file type downloads while allowing uploads, select Download from the drop-down list.</p> <p>Action: Select the action that applies when the associated file types are moving in the direction selected from the Direction drop-down list.</p> <p>Click ADD to add the rule to the profile. You may add any number of rules to the profile.</p> <p>Added Rules: Displays a list of all rules added to the profile. To remove a rule, check the box next to the rule you want to remove and click the Delete icon .</p> |

Important: After creating or modifying a profile, you must commit your changes for them to take effect. For more information, see [Committing Changes, page 17](#).

Applying a File Blocking Profile to a Security Rule

To apply a file blocking profile to a security rule:

1. From the **MANAGE** drop-down list, select **Security Rules**.
The **Security Rules** page displays.
2. Click the security rule to which you want to add the profile.
3. From the **Actions** section, click **File Blocking** and select the desired profile or preconfigured levels for the rule.
4. Click **OK**.
5. Commit the changes. For more information, see [Committing Changes, page 17](#).

Managing Vulnerability Protection (IDS/IPS) Profiles

Note: IDS/IPS profiles are available only in CFS Premium subscriptions.

If you subscribe to Premium CFS services, you can apply IDS/IPS profiles that detect potential vulnerabilities to your network, such as buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. CFS provides a default profile that protects clients and servers from all known critical, high, and medium severity threats.

You can use the default profile provided or add additional profiles to minimize vulnerability checking for traffic between trusted security zones, and to maximize protection for traffic received from untrusted zones, such as the internet, as well as the traffic sent to highly sensitive destinations, such as server farms.

Protection Levels

CFS supports a tiered approach to IDS/IPS protection. The following table indicates which threat levels are alerted (IDS) or blocked (IPS) by service level.

| Protection Type | Moderate | Recommended | High |
|---------------------|-------------------|---------------------|---|
| Alert (IDS) | All Threat Levels | All Threat Levels | All Threat Levels |
| Action (IPS) | N/A | Default All Threats | <ul style="list-style-type: none">• Blocks Medium, High, and Critical Threat Levels• Default Informational and Low Threat Levels |

Applying IDS/IPS Profiles

To apply IDS/IPS profiles:

1. From the **MANAGE** drop-down list, select **Security Rules**.
The **Security Rules** page displays.
2. Click the security rule to which you want to add the profile.
3. From the **Actions** section, click **IDS-IPS** and select the vulnerability protection level for the rule.

Note: The **IDS-IPS** drop-down list includes the settings “default” and “strict.” These settings are available only to Allstream’s Network Operations Team and cannot be selected for your IPS-IDS vulnerability protection level.

4. Click **OK**.
5. Commit the changes. For more information, see [Committing Changes, page 17](#).

Working with Objects and Groups

One of the more common tasks when setting up CFS is to create service objects that have defined ports and protocols. A service object can then be referenced from other areas of CFS, such as with NAT rules or firewall security policies, for example.

There are several methods you can use to define security policies for specific source or destination addresses. You can assign an IP address (or a range of IP addresses) to a defined rule. However, if you have multiple IP addresses that require the same security settings, rather than assigning each IP address to a rule, you can combine the IP addresses into an address object, then assign the object to a security policy. This method of grouping objects based on security policy requirements can simplify policy creation.

Managing Service Objects



To manage service objects, from the **MANAGE** drop-down list in the navigation bar, select **Services**.

The **Service** page displays a list of existing service objects. Once a service object is created, it may be applied to your security rules.

The **Service** page allows you to perform the following service object management tasks:

- Click a service object in the list to display the **Create/Edit Service** page. This page allows you to modify or remove the object.

Note: Some default objects are protected and may not be modified or removed.

- Click the **Search** icon  to search for a specific object in the list.
- Click the **Add** icon  to create a new object.

Service object properties include the following:

| Attribute | Description |
|------------------------------------|--|
| Name (required) | A descriptive name for the service. Service names may contain up to 63 alphanumeric characters and may include dashes, underscores, and periods. |
| Description | A descriptive, identifiable, and brief explanation of the service. Descriptions may contain up to 255 alphanumeric characters and may include dashes, underscores, and periods. |
| Protocol (required) | Select the protocol you are using from the drop-down list: TCP or UDP . |
| Destination Port (required) | The port number for the destination IP address. Numbers can be between 0 and 65535 or a range of port numbers (port1-port2). Multiple ports or ranges must be separated by commas. |

Important: After creating or modifying a service object, you must commit your changes for them to take effect. For more information, see [Committing Changes, page 17](#).



Managing Addresses for Objects

To manage an address for an object used for a security rule and policy, from the **MANAGE** drop-down list, select **Addresses**. The **Addresses** page displays a list of existing addresses. Once an address is created, it may be applied to your security rules.

The **Addresses** page allows you to perform the following address management tasks:

- Click an address in the list to display the **Create/Edit Address** page. This page allows you to modify or remove the address.

Note: Some default addresses are protected and may not be modified or removed.

- Click the **Search** icon  to search for a specific address in the list.
- Click the **Add** icon  to create a new address.

Address properties include the following:



| Attribute | Description |
|--------------------------------|---|
| Name (required) | A descriptive name for the address. Address names may contain up to 63 alphanumeric characters and may include dashes, underscores, and periods. |
| Type (required) | Select the address type from the drop-down list: <ul style="list-style-type: none">• Fqdn (fully qualified domain name)• IP Range (two IPv4 or IPv6 addresses denoting the start and end range separated by a hyphen)• IP Netmask (in CIDR notation) |
| Description | A descriptive, identifiable, and brief explanation of the address. Descriptions may contain up to 255 alphanumeric characters and may include dashes, underscores, and periods. |
| IP/URL/Range (required) | Enter the IP address, URL, or IP address range. |

Important: After creating or modifying an address, you must commit your changes for them to take effect. For more information, see [Committing Changes, page 17](#).

Managing Address Groups

An address group allows you to group multiple address objects into a single group that may be used for security rules and policies. To manage an address group, from the **MANAGE** drop-down list, select **Address Groups**. The **Address Groups** page displays a list of existing address groups. Once an address group is created, it may be applied to your security rules.

The **Address Groups** page allows you to perform the following address group management tasks:

- Click an address group in the list to display the **Create/Edit Address Group** page. This page allows you to modify or remove the address group.
- Click the **Search** icon  to search for a specific address group in the list.
- Click the **Add** icon  to create a new address group.

Address group properties include the following:

| Attribute | Description |
|------------------------|---|
| Name (required) | A descriptive name for the address group. Address group names may contain up to 63 alphanumeric characters and may include dashes, underscores, and periods. |
| Description | A descriptive, identifiable, and brief explanation of the address group. Descriptions may contain up to 255 alphanumeric characters and may include dashes, underscores, and periods. |
| Address | Select one or more address objects to include in the group. |
| Address Groups | To include multiple address groups under the single address group, select one or more address groups from the drop-down list. |



Important: After creating or modifying an address group, you must commit your changes for them to take effect. For more information, see [Committing Changes, page 17](#).

Managing Application Groups

Application groups are objects that contains applications that you want to treat similarly within a security rule. Application groups are useful for enabling access to applications that you explicitly sanction for use within your organization. If you want to explicitly allow or deny specific objects, create a set of applications that may or may not be related and group them together. You can then use them as a single object in a rule. You can simplify the creation and maintenance of security rules by grouping applications together that require the same security rules.

To manage an application group, from the **MANAGE** drop-down list, select **Application Groups**. The **Application Groups** page displays a list of existing application groups. Once a group is created, it may be applied to your security rules.

The **Application Groups** page allows you to perform the following group management tasks:

- Click a group in the list to display the **Create/Edit Application Group** page. This page allows you to modify or remove the group.
- Click the **Search** icon  to search for a specific group in the list.
- Click the **Add** icon  to create a new group.

Application group properties include the following:

| Attribute | Description |
|------------------------|--|
| Name (required) | A descriptive and unique name for the group. Group names may contain up to 31 alphanumeric characters and may include dashes, underscores, and periods. |
| Description | A descriptive, identifiable, and brief explanation of the group. Descriptions may contain up to 255 alphanumeric characters and may include dashes, underscores, and periods. |
| Application | Select one or more applications to include in the group. It is important to note that some category 4 and category 5 applications are not necessarily bad. Some applications are labeled as category 4 or 5 because some of the programs or services can be exploited and have a high exploitation rating. If your business or organization uses specific applications that fall under category 4 or 5, you can add them to the <i>MyCompany Allowed Apps</i> rule. Some examples of common category 4 and 5 applications that may be needed despite the classification include Hotmail, Facebook, or certain YouTube functions, Google Docs, or Skype. |



| Attribute | Description |
|-------------------------------|---|
| Application Groups | To include multiple application groups under the single application group, select one or more application groups from the drop-down list. |
| Application Containers | Application containers, such as Docker, encapsulate the files, dependencies, and libraries of an application to run on an OS. To include multiple application containers under the application group, select one or more application containers from the drop-down list. |
| Application Filters | An application filter is an object that dynamically groups applications based on attributes that you define, including category, subcategory, technology, risk factor, and characteristic. These are not created in the CFS portal, but can be included in an application group by selecting one or more filters from the drop-down list. |

Important: After creating or modifying an application group, you must commit your changes for them to take effect. For more information, see [Committing Changes](#).

Committing Changes

Changes made to rules and objects take effect after committing the changes. You must commit your changes to have a direct effect on how internet traffic is scrutinized and handles at the firewall.

The **Commit** icon in the navigation bar displays in two ways:

- If no changes to commit exist, the icon is disabled and displays 0: 
- If there are changes to commit, the icon is enabled and displays the total number of changes: 

Note: If you are implementing more than one update, save the updates as you build new rules and commit all changes at the same time.

To commit changes:

1. After a rule or object is created or changed, click **OK** to save the changes.
The **Commit** icon in the navigation bar displays the total number of changes ready to commit.
2. Click the **Commit** icon.
A **Commit** page displays allowing you to review the changes.
3. Click **Commit** at the bottom of the page to submit the changes to the firewall.

Monitoring Settings

Resetting IPSec Tunnel Connections

Due to the nature of network connections over the public internet, there may be times when an Internet Protocol Security (IPSec) tunnel is dropped from one of the end points. If you experience a connection that hangs or drops, you can quickly reset the connection as described below. If your connection is not repaired after resetting the connection, contact Customer Support for assistance.

To reset an IPSec tunnel connection:

1. From the **MONITOR** drop-down list in the navigation bar, select **IPSec Tunnels**.
2. Click **Reset** to reset the desired tunnel.

Monitoring User ID Agents

User ID agents map usernames to IP addresses. This feature allows you to create security rules based upon users and groups. User ID agents are created and managed outside of the CFS portal but may be viewed and implemented within CFS security policies. The **User ID Agents** page displays all of agents being using in the CFS portal. To access the **User ID Agents** page, from the **MONITOR** drop-down list, select **User ID Agents**. This information is read-only. For help or further information, contact Customer Care.

Monitoring GlobalProtect Users

Allstream's CFS can be accessed by end users locally or remotely through Allstream's secure VPN. The **GlobalProtect Users** page displays a list of users logged in to the VPN either historically or currently and allows you to disconnect users when needed.

To access the **GlobalProtect Users** page, from the **MONITOR** drop-down list in the navigation bar, select **GlobalProtect Users**.

Viewing Users

The **GlobalProtect Users** page allows you to access a list of remote end users that are currently logged in to CFS as well as historical login and logout information. Information about each user's login origin (such as public and private IP addresses, type of VPN tunnel established, and the timestamp of their last login) is also displayed.

To view VPN users currently logged in to CFS, on the **GlobalProtect Users** page, move the toggle at the top of the page to **Current**.

To view a summary of past user login and logout activity, on the **GlobalProtect Users** page, move the toggle at the top of the page to **History**.

Disconnecting Remote Users

There may be times when a System or Network Administrator requires all remote users to disconnect their CFS session. This is typically required to perform routine maintenance and/or updates to the system.

To disconnect VPN users currently logged in to CFS, on the **GlobalProtect Users** page, click **Logout** next to the user's name you want to disconnect. The system immediately disconnects the user from the VPN session. Note that any changes the user has made while logged in to CFS that have not been saved will be lost.

Appendix A: Risk Calculations

Based on your security profile, CFS allows certain types of applications and blocks others. You can adjust either the firewall policies or the visibility of an individual application as needed. However, before you allow a blocked application through the firewall, Allstream recommends that you review the application's security risks in the Palo Alto Networks' Applopedia database available at <https://applipedia.paloaltonetworks.com>.

Understanding Application Risks

Palo Alto Networks' Applopedia has risk assessments for over 1,400 applications. Palo Alto Networks updates the database as they learn of new applications and information regarding existing applications.

The Palo Alto Networks' Applopedia database available at <https://applipedia.paloaltonetworks.com>.

Researching Risk Levels for a Single Application or Web Site

To learn about a specific application:

1. On the Applopedia site, type the application name in the **Search** field at the top of the page and press **Enter**.
A list of application names that match displays, as well as applications whose descriptions reference that application name.
2. Click the application name to see a description, an overall risk rating, and the characteristics that contribute to its security risk.

Application characteristics include the following:

- **Evasive:** Indicates whether the application attempts to evade firewall rules.
- **Excessive Bandwidth:** Indicates whether the application uses significant bandwidth, which can compromise network performance.
- **Prone to Misuse:** Indicates whether the application tends to attract misuse.
- **Capable of File Transfer:** Indicates whether the application can transfer files.
- **Tunnels Other Applications:** Indicates whether the application can carry other applications within the traffic it sends.
- **Used by Malware:** Indicates whether the application is used by malware.
- **Has Known Vulnerabilities:** Indicates whether the application has any currently known vulnerability.
- **Widely Used:** Indicates whether the application is widely used.

Researching Risk Levels for a Group of Applications or Web Sites

You can look up applications in Applipedia by category, subcategory, technology, risk, characteristic, or a combination of those filters.

To research a group of applications:

1. If you have already searched by name or filtered the list, click **Clear Filters**, located in the upper right-hand corner of the page.
2. Select one or more links in the following filters:
 - **Category:** Defines the purpose of the application, such as business systems or media.
 - **Subcategory:** Further defines the purpose of the application. Note that each subcategory is only associated with a single category.
 - **Technology:** Defines the type of connection, such as browser-based or client-server.
 - **Risk:** Defines a risk assessment based on the technology and/or characteristics. A lower number indicates lower risk.
 - **Characteristics:** Defines application characteristics that may make them dangerous.
3. To clear a particular filter, click it again.

App-ID Metadata

App-ID metadata is a group attributes of an App-ID that define its characteristics and capabilities. For instance, an application timeout or a risk value is an example of metadata for an App-ID. A metadata change is when one of these attributes is changed to improve application capabilities. App-ID metadata helps to improve virus detection and reporting capabilities.

| Technology | Description |
|------------------|--|
| network-protocol | An application that is generally used for system-to-system communication that facilitates network operation. This includes most IP protocols. |
| client-server | An application that uses a client-server model where one or more clients communicate with a server in the network. |
| peer-to-peer | An application that communicates directly with other clients to transfer information instead of relying on a central server to facilitate the communication. |
| browser-based | An application that relies on a web browser to function. |

| Characteristics | Description |
|--------------------------|---|
| Capable of File Transfer | Has the capability to transfer a file from one system to another over a network. A streaming application that has no other mechanism to transfer files other than the video or audio streaming should not be flagged as able to transfer files. |
| Used by Malware | Malware has been known to use the application for propagation, attack, or data theft, or is distributed with malware. |
| Excessive Bandwidth Use | Uses a port or protocol for something other than its originally intended purpose with the hope that it will traverse a firewall. |
| Evasive | Uses a port or protocol for something other than its originally intended purpose with the hope that it will traverse a firewall. |
| Pervasive | Likely has more than 1,000,000 users. |
| Known Vulnerabilities | Has publicly reported vulnerability. For web-based applications, it should also be set to Yes as HTTP always has vulnerabilities. |
| Prone to Misuse | Often used for nefarious purposes or is easily set up to expose more than the user intended. |
| Tunnels Other Apps | Able to transport other applications inside its protocol. |
| Fine-type-ident | Should be set if the application can upload or download a file-type over a decodable protocol (for example, HTTP). |
| Spyware-ident | Should be set if the application can upload or download an executable file for over a decodable protocol. |
| Virus-ident | Should be set if the application can upload or download an executable file for over a decodable protocol. |
| Vulnerability-ident | For web-based applications, the vulnerability-ident should always be Yes as HTTP always has vulnerabilities. |
| Deny-action | For web-based applications, deny-action should be set to drop-reset unless there are issues with the application receiving top-reset. |

Risk Calculation

The level of risk that a web site or application is assumed to have is based on the characteristics of the potential threat, and the number (factor) of characteristics of each threat. Web sites and applications are assigned a 'Risk Level' based on the characteristics and factors of the threat, as shown in the following tables:

| Threat Characteristics | Factor |
|--------------------------|-----------|
| Evasive | 3 |
| Excessive Bandwidth Use | 1 |
| Used by Malware | 4 |
| Capable of File Transfer | 3 |
| Known Vulnerabilities | 3 |
| Tunnels Other Apps | 2 |
| Prone to Misuse | 2 |
| Pervasive | 1 |
| Total | 19 |

| Risk Level Assignment | Factor Range |
|-----------------------|--------------|
| 1 | 0-3 |
| 2 | 4-6 |
| 3 | 7-9 |
| 4 | 10-13 |
| 5 | 14+ |

Appendix B: Obtaining Base DN and Bind DN for Active Directory Servers

To correctly integrate your Active Directory with CFS, LDAP Base DN and Bind DN syntax must be correct. Although understanding how the LDAP directory structure and LDAP attributes are used is beyond the scope of this User Guide, you do need to be familiar with your Active Directory (AD) structure to configure LDAP on the Cloud Firewall.

For this reason, the following sections describe how to obtain the Base DN and Bind DN for your LDAP server.

Note: You can use an LDAP browser to easily obtain the Base DN and Bind DN for your server. However, the information in the following sections assumes you must obtain this information without the use of an LDAP browser.

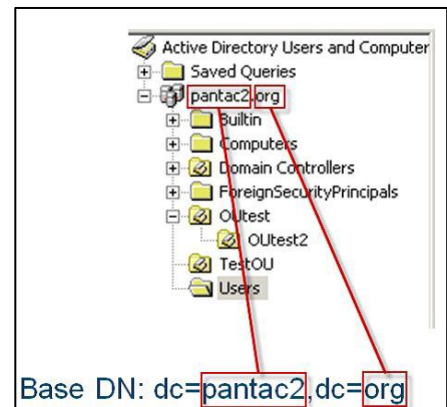
Base DN

The Base DN is where the system begins to search for users and groups and is most often your domain name. If you're using a default Active Directory setup, all user accounts and groups are located in the **Users** folder under your domain.

For example, let's say your domain is myCompany.com. In this case, the Base DN is:

dc=myCompany,dc=com

The illustration on the right shows the Base DN for pantac2.org as viewed through an LDAP browser.

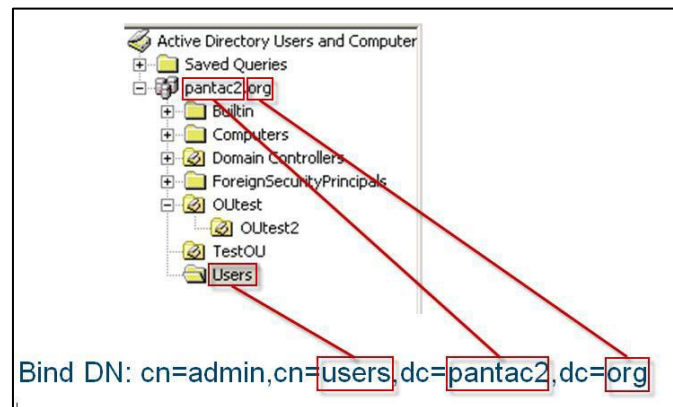


Bind DN

The Bind DN is the username on the external LDAP server that has permission to search the LDAP directory (within the defined search base) and request authentication. The role of the Bind DN is to query the directory using the LDAP query filter and search base for the distinguished name for authenticating users. The Bind DN is derived by using LDAP syntax and going up the tree starting at the user with applicable permissions.

In the example on the right, the user Admin is the user account with LDAP search permissions and is contained in the folder Users, under pantac2.org. In this case, the corresponding Bind DN is:

cn=Admin,cn=Users,dc=pantac2,dc=org



Appendix C: Application Policy Exceptions

The security policies listed below are preconfigured for new customers. They are set up in accordance with Palo Alto Networks best practices in order to provide you with a more secure baseline.

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

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, httpvideo, 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