



Configuring Virtualization on the Virtual Firewall

This module describes how to configure virtualization for the VFW application.

Feature History for Configuring Network Address Translation on the VFW Application

Release	Modification
Release 3.5.0	This feature was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Contents

- [Information About Virtualization, page VFC-45](#)
- [How to Configure Virtualization, page VFC-49](#)
- [Configuration Examples for Virtualization, page VFC-59](#)

Information About Virtualization

You can operate your VFW application in a single context or in multiple contexts. Multiple contexts use the concept of virtualization to partition your VFW application into multiple virtual devices or contexts. Each context contains its own set of policies, interfaces, resources, and administrators. This feature provides you with the tools to more closely and efficiently manage the system resources and users of the VFW application and to manage the services you provide to your customers.

By default, your VFW application provides an Admin context and five user contexts. This provision allows you to use multiple contexts if you choose to configure them. To increase the number of user contexts (up to a maximum of 250), you may purchase a separate license from Cisco Systems.

This section provides an overview of the basic concepts involved with virtualization. Virtualization consists of the following functional areas:

- [Contexts, page VFC-46](#)
- [Domains, page VFC-47](#)
- [Role-Based Access Control, page VFC-48](#)
- [Resource Classes, page VFC-49](#)

Contexts

The virtualized environment is divided into objects called *contexts*. Each context behaves like an independent VFW with its own policies, interfaces, domains, and administrators. Each context also has its own management interface that you can access using Telnet or SSH.

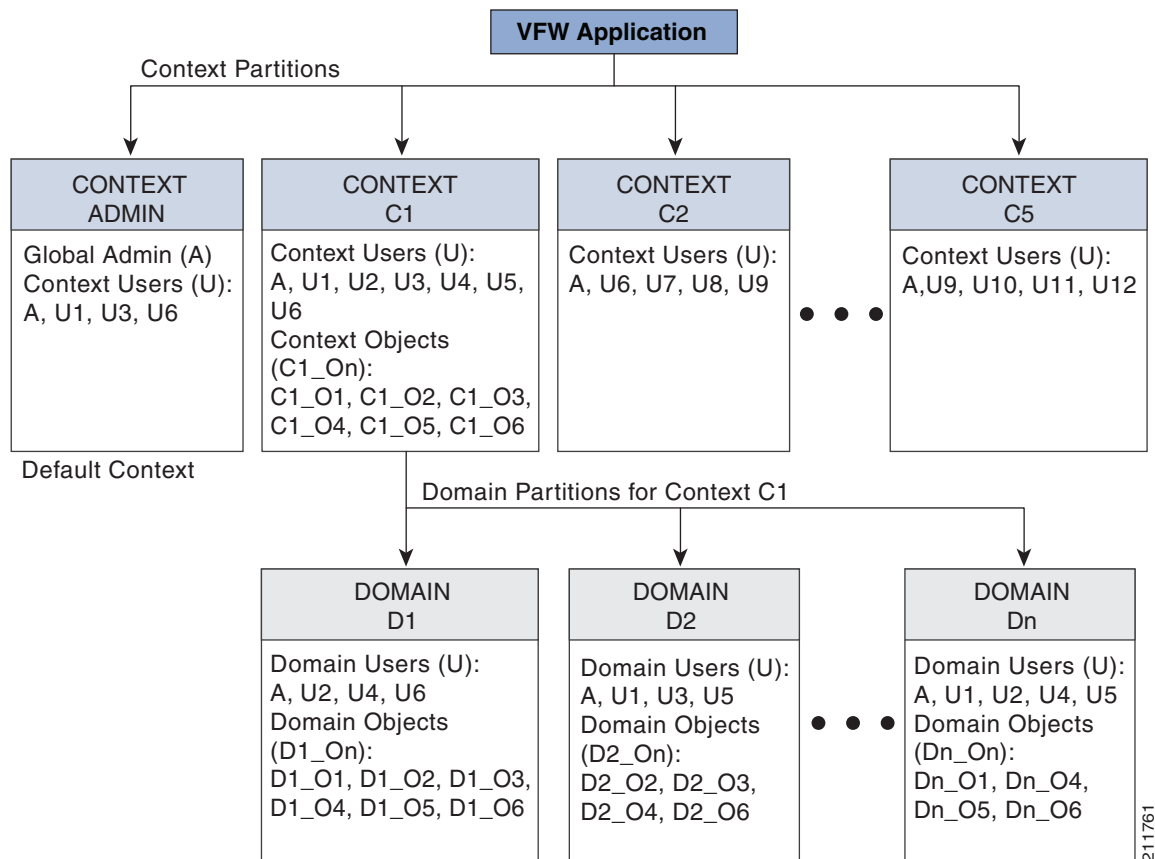
As the global administrator (Admin), you can configure and manage all contexts through the Admin context, which contains the basic settings for each virtual device or context. When the Admin logs in to the VFW application through the router processor using Telnet, the Admin is authenticated in the Admin context.

The Admin context is similar to other contexts, except that, when you log in to the Admin context (for example, using SSH), you have full system administrator access to the entire VFW application and all contexts and objects within it. The Admin context provides access to network-wide resources, for example, a syslog server or context configuration server. All global commands for the VFW application settings, contexts, resource classes, and so on are available only in the Admin context.

Each context, including the Admin context, has its own configuration file and local user database that are stored in the local disk partition on the flash disk or that can be downloaded from an FTP, TFTP, or HTTP(S) server. The startup-config for each context is stored as the startup-configuration file on the flash disk.

Figure 8 illustrates the concept of VFW application virtualization in which you create partitions that enable the VFW application to function as multiple virtual devices.

Figure 8 VFW Virtualization Chart



211761

In the Admin context, use the **changeto** command in EXEC mode or the **do changeto** command in configuration modes to move between contexts. Only users authenticated in the Admin context can use the **changeto** command.

Each context you create represents a virtual device. You can partition each context into domains for managing access to context resources. [Table 3](#) describes the various components in [Figure 8](#).

Table 3 VFW Virtualization Elements

Element	Description
Context (Cn)	You can configure a single VFW application to behave as multiple, virtual devices by creating partitions called <i>contexts</i> . Each context functions as an independent device, with its own set of users, objects, and allocated resources. By default, the VFW application comes preconfigured with an Admin context and five configurable user contexts. To upgrade to a maximum of 250 user contexts, you must purchase a separate license from Cisco Systems. For more information about contexts, see the “ Contexts ” section.
Domain (Dn)	You can divide each context into multiple partitions called <i>domains</i> , allowing you to manage user access to the objects within a context. When you create a domain, you form an association between a select group of context users and a select group of context objects. For more information about domains, see the “ Domains ” section.
User (A, Un)	The VFW application is preconfigured with a default global system administrator that provides access to all VFW application functionality and allows you to create additional users. Any user you create while in Admin context, by default, has access to all resources in the VFW application. Any user you create while in a user-defined context, has access only to the resources within that context. You assign each user a role, which determines the commands and resources that are available to that user.
Object (Cn_On, Dn_On)	Objects are user-configurable items, such as: <ul style="list-style-type: none"> • Access lists • Defined interfaces • Policy maps • Scripts <p>The objects you create are specific to the context you are in while creating the object. If the context is partitioned into multiple domains, you allocate objects within each domain.</p>

Domains

For management purposes, contexts are divided into objects called *domains*, and each domain is fully contained within a context. A domain provides a namespace in which a user operates, and each user is associated with at least one domain. The role assigned to a user determines the operations that a user can perform on the objects in a domain and the command set available to that user. When you create a context, the VFW application automatically creates a default domain for that context.

The global admin or context administrators can create additional domains. A domain name must be unique within the context with which it is associated.

You can add to a domain any object that you can create (for example, an interface) and you can add an object to multiple domains. If you add an object that has other objects associated with it to a domain, the associated objects do not automatically become part of the domain. You must add each object individually. When you create an object, the VFW application automatically adds it to your domain.

**Note**

A domain does not restrict the context configuration that you can display using the **show running-config** command. However, a domain does restrict a user's access to configurable objects in the VFW application. You can further restrict the operations a user can perform on those configurable objects by assigning a role to a user. For information about user roles, see the [“Role-Based Access Control”](#) section.

Role-Based Access Control

The VFW application provides role-based access control (RBAC), which is a mechanism that determines the commands and resources available to each user. A role defines a set of permissions for accessing the objects and resources in a context and the actions that you can perform on them. The global administrator or the context administrator assigns roles to users based on their network function and the resources to which you want them to have access.

The VFW application provides the following predefined roles that you cannot delete or modify:

- Admin—If created in the Admin context, has complete access to, and control over, all contexts, domains, roles, users, resources, and objects in the entire VFW application. If created in a user context, this role gives a user complete access to and control over all the objects in that context. A context administrator can create, configure, and modify any object in that context, including policies, roles, domains, and so on.
- Network Admin—Complete access to and control over the following features:
 - **changeto** command
 - Connection parameters
 - Copy configurations
 - Interfaces
 - Routing
 - NAT
- Network-Monitor—Access to all **show** commands and the **changeto** command only. If you do not explicitly assign a role to a user with the **username** command, this is the default role.
- Security-Admin—Complete access to and control over the following security-related features within a context:
 - AAA
 - ACLs
 - Application inspection
 - **changeto** command
 - Connection parameters
 - Copy configurations
 - Interfaces
 - NAT

Resource Classes

Resource classes are the means by which you manage context access to VFW application resources, such as concurrent connections or bandwidth rate. The VFW application is preconfigured with a default resource class that it applies to the Admin context and any user context upon creation. The default resource class is configured to allow a context to operate within a range that can vary from no resource access (0 percent) to complete resource access (100 percent). When you use the default resource class with multiple contexts, you run the risk of oversubscribing VFW application resources. This means that the VFW application permits all contexts to have full access to all resources on a first-come, first-served basis. When a resource is utilized to its maximum limit, the VFW application denies additional requests made by any context for that resource.

To avoid oversubscribing resources and to help guarantee access to a resource by any context, the VFW application allows you to create customized resource classes that you associate with one or more contexts. A context becomes a *member* of the resource class when you make the association. Creating a resource class allows you to set limits on the minimum and maximum amounts of each VFW application resource that a member context is entitled to use. You define the minimum and maximum values as a percentage of the whole.

You can limit and manage the allocation of the following VFW application resources:

- ACL memory
- Buffers for syslog messages and TCP out-of-order (OOO) segments
- Concurrent connections (through-the-VFW application traffic)
- Management connections (to-the-VFW application traffic)
- Proxy connections
- Regular expression (regexp) memory
- Set resource limit as a rate (number per second)
- Static or dynamic network address translations (Xlates)

By default, when you create a context, the VFW application associates the context with the default resource class. The default resource class provides resources of a minimum of 0 and a maximum of unlimited for all resources.

How to Configure Virtualization

- [Configuring Virtualization, page VFC-49](#)
- [Displaying Virtualization Configuration and Statistics, page VFC-57](#)

Configuring Virtualization

This task describes how to create and configure the virtualization feature for your VFW application. As the global administrator (SuperUser), you configure and manage all contexts through the Admin context, which contains the basic settings for each virtual device or context. Each context that you configure contains its own set of policies, interfaces, resources, and administrators.



Note By default, the VFW application provides an Admin context and allows you to configure five user contexts. To create the maximum of 250 user contexts, you must purchase a license from Cisco Systems.

Prerequisites

You must attach from the route processor to the VFW application before you can perform this task. See the [“Attaching to the VFW Application”](#) section on page VFC-14.

SUMMARY STEPS

1. **configure**
2. **resource-class** *name*
3. **limit-resource** {acl-memory | all | buffer {syslog} | conc-connections | mgmt-connections | proxy-connections | rate {bandwidth | connections | inspect-conn | mgmt-traffic | syslog} | regexp | xlates} {minimum *number*} {maximum {equal-to-min | unlimited}}
4. **exit**
5. **context** *name*
6. **member** *class*
7. **do changeto** *name*
8. **exit**
9. **domain** *name*
10. **add-object** {access-list | all | class-map | interface | parameter-map | policy-map | script} *name*
11. **exit**
12. **role** *name*
13. **rule** *number* {permit | deny} {create | modify | debug | monitor} [feature {AAA | access-list | config-copy | connection | fault-tolerant | inspect | interface || nat | syslog}]
14. **username** *name1* [password [0 | 5] {*password*}] [expire *date*] [role *name2* {domain *name3* *name4* ... *namen*}]
15. **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure</p> <p>Example: firewall/Admin# configure Enter configuration commands, one per line. End with CNTL/Z. firewall/Admin(config)#</p>	<p>Enters global configuration mode. You are now within configuration mode of the VFW application.</p>
Step 2	<p>resource-class name</p> <p>Example: firewall/Admin(config)# resource-class RC1</p>	<p>Creates a resource class to allocate and manage the use of system resources by one or more contexts. The VFW application supports a maximum of 100 resource classes.</p>
Step 3	<p>limit-resource {acl-memory all buffer {syslog} conc-connections mgmt-connections proxy-connections rate {bandwidth connections inspect-conn mgmt-traffic syslog} regexp xlates} {minimum number} {maximum {equal-to-min unlimited}}</p> <p>Example: firewall/Admin(config-resource)# limit resource all minimum 10 maximum equal-to-min</p>	<p>Limits resources used by user contexts. The arguments and keywords are:</p> <ul style="list-style-type: none"> • acl-memory—Limits memory space allocated for ACLs. • all—Limits all resources to the specified value for all contexts assigned to this resource class. • buffer—Limits the number of syslog buffers. • conc-connections—Limits the number of simultaneous connections. • mgmt-connections—Limits the number of management (to-the-VFW application) connections. • proxy-connections—Limits the number of proxy connections. • rate—Limits the resource as a number per second for: <ul style="list-style-type: none"> – bandwidth—Limits context throughput in bytes per second – connections—Limits the number of connections of any kind per second – inspect conn—Limits the number of application protocol inspection connections per second for FTP and RTSP only – mgmt-traffic—Limits management (to-the-VFW application) traffic in bytes per second – syslog—Limits the number of syslog messages per second • regexp—Limits the amount of regular expression memory. • xlates—Limits the number of network and port address translations entries.

Command or Action	Purpose
	<ul style="list-style-type: none"> • minimum <i>number</i>—Specifies the lowest acceptable value. Enter an integer from 0.00 to 100.00 percent (two-decimal places of granularity). The <i>number</i> argument specifies a percentage value for all contexts that are members of the class. When used with the rate keyword, the <i>number</i> argument specifies a value per second. • maximum {equal-to-min unlimited}—Specifies the maximum resource value: either the same as the minimum value or no limit. <p>Note The limit you set for individual resources using the limit-resource command overrides the limit you set for all resources using the limit-resource all command.</p>
<p>Step 4 exit</p> <p>Example: <pre>firewall/Admin(config-resource)# exit firewall/Admin(config)#</pre></p>	<p>Exits resource configuration mode.</p>
<p>Step 5 context <i>name</i></p> <p>Example: <pre>firewall/Admin(config)# context C1 firewall/Admin(config-context)#</pre></p>	<p>Creates a new context.</p>
<p>Step 6 member <i>class</i></p> <p>Example: <pre>firewall/Admin(config-context)# member RC1</pre></p>	<p>Associates the context with the resource class that you created in Step 2.</p>
<p>Step 7 do changeto <i>name</i></p> <p>Example: <pre>firewall/Admin(config-context)# do changeto C1 firewall/C1(config-context)#</pre></p>	<p>Changes to the context (<i>name</i>) that you created in Step 5 and enters configuration mode in that context.</p>
<p>Step 8 exit</p> <p>Example: <pre>firewall/C1(config-context)# exit firewall/C1(config)#</pre></p>	<p>Exits context configuration mode.</p>
<p>Step 9 domain <i>name</i></p> <p>Example: <pre>firewall/C1(config)# domain D1 firewall/C1(config-domain)#</pre></p>	<p>(Optional) Creates a domain for the context.</p>

	Command or Action	Purpose
Step 10	<p>add-object {access-list extended all class-map interface parameter-map policy-map script} <i>name</i></p> <p>Example: <pre>firewall/C1(config-domain)# add-object access-list extended acl1</pre></p>	<p>Allocates objects (for example, ACLs, and so on) to the domain as needed. The keywords, arguments, and options are:</p> <ul style="list-style-type: none"> • access-list extended—Specifies an existing access control list (ACL) that you want to associate with the domain. • all—Specifies that all existing configuration objects in the context are added to the domain. • class-map—Specifies an existing class map for flow classification that you want to associate with the domain. • interface—Specifies an existing interface that you want to associate with the domain. • parameter-map—Specifies an existing parameter map that you want to associate with the domain. • policy-map—Specifies an existing policy map that you want to associate with the domain. • script—Specifies an existing script that you created with the VFW application TCL scripting language. • <i>name</i>—Identifier of the specified object. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
Step 11	<p>exit</p> <p>Example: <pre>firewall/C1(config-domain)# exit firewall/C1(config)#</pre></p>	<p>Exits domain configuration mode.</p>
Step 12	<p>role <i>name</i></p> <p>Example: <pre>firewall/C1(config)# role UR1 firewall/C1(config)#</pre></p>	<p>(Optional) Creates roles to define the object and resource permissions for different groups of users.</p>

Command or Action	Purpose
<p>Step 13 <code>rule number {permit deny} {create modify debug monitor} [feature {AAA access-list config-copy connection fault-tolerant inspect interface nat syslog}]</code></p> <p>Example: <pre>firewall/C1(config-role)# rule 1 deny create feature acl</pre></p>	<p>Creates rules to define the role permissions. The keywords, arguments, and options are:</p> <ul style="list-style-type: none"> • number—An identifier of the rule and order of precedence, with a higher-numbered rule applied after a lower-numbered rule. Enter a unique integer from 1 to 16. • deny—Disallows the role to perform the operations defined by the rest of the command keywords. • permit—Allows the role to perform the operations defined by the rest of the command keywords. • create—Specifies commands for the creation of new objects or the deletion of existing objects (includes modify, debug, and monitor commands). • debug—Specifies commands for debugging problems (includes monitor commands). • modify—Specifies commands for modifying existing configurations (includes debug and monitor commands). • monitor—Specifies commands for monitoring resources an objects (show commands). • feature—(Optional) Specifies a particular VFW application feature for which you are configuring this rule. <ul style="list-style-type: none"> – AAA—Specifies commands for authentication, authorization, and accounting. – access-list—Specifies commands for access control lists (ACLs). Includes ACL configuration, class maps for ACL, and policy maps containing ACL class maps. – config-copy—Specifies commands for copying the running-config to the startup-config, startup-config to the running-config, and copying both config files to the flash disk (disk0:) or a to remote server. – connection—Specifies commands for network connections. – fault-tolerant—Specifies commands for redundancy. – inspect—Specifies commands for packet inspection used in data-center security. – interface—Specifies all interface commands. – nat—Specifies commands for network address translation (NAT) associated with a class map in a policy map used in data-center security. – syslog—Specifies the system logging facility setup commands.

Command or Action	Purpose
<p>Step 14 <code>username name1 [password [0 5] {password}] [expire date] [role role {domain domain1 domain2 ... domain10}]</code></p> <p>Example: <pre>firewall/C1(config)# username user1 password 5 MYPASSWORD role Network-Admin domain D1</pre></p>	<p>Configures users as required and associates roles and domains with the users. The keywords, arguments, and options are:</p> <ul style="list-style-type: none"> • <i>name1</i>—Identifier of the user you are creating. Enter an unquoted text string with no spaces and a maximum of 24 characters. • password—(Optional) Keyword that indicates that a password follows. • 0—(Optional) Specifies a clear text password. • 5—(Optional) Specifies an MD5-hashed strong encryption password. • <i>password</i>—(Optional) Password in clear text, encrypted text, or MD5 strong encryption, depending on the numbered option (0, 5, or 7) you enter. If you do not enter a numbered option, the password is in clear text by default. If you enter the password keyword, you must enter a password. Enter a password as an unquoted text string with a maximum of 32 characters. • expire date—(Optional) Specifies the expiration date of the user account. Enter the expiration date in the format <i>yyyy-mm-dd</i>. • role role—(Optional) Specifies role that you want to assign to the user. Use the show role command to display available roles and their associated permissions. The <i>role</i> argument is context sensitive. • domain domain1 domain2 ... domain10—Specifies the domains in which the user can operate. You can enter multiple domain names up to a maximum of 10, including default-domain.
<p>Step 15 <code>show running-config</code></p> <p>Example: <pre>firewall/C1# show running-config context firewall/C1# show running-config domain firewall/C1# show running-config resource-class firewall/C1# show running-config role</pre></p>	<p>(Recommended) Verifies the virtualization configuration.</p>

Table 4 lists the managed system resources of the VFW application. You can limit these resources per context or for all contexts associated with the resource class using the **limit-resource** command. See Step 3 in the task table.

Table 4 System Resource Maximum Values

Resource	Maximum Value
ACL Memory	78,610,432 bytes
Buffer Memory (Syslog)	4,000,000 bytes

Table 4 System Resource Maximum Values (continued)

Resource	Maximum Value
Concurrent Connections	4,000,000 connections
Management Connections	5000 connections
Proxy Connections	524286 connections
Rate	
Bandwidth	4 gigabits per second (Gbps) You can upgrade the VFW application maximum bandwidth to 8 Gbps by purchasing a separate license from Cisco Systems.
Connections (any kind)	1,000,000 connections per second
Management Traffic	125,000,000 connections per second
Syslog	For to the VFW application traffic, 5 K messages per second For through the VFW application traffic, 400 K messages per second
Regular Expression Memory	1,048,576 bytes
Xlates (network and port address translation entries)	524286 translations

The permissions of each of the system-defined roles are displayed using the **show role** command:

```
firewall/Admin# show role
```

```
Role: Admin (System-defined)
Description: Administrator
Number of rules: 4
```

```
-----
Rule    Type    Permission    Feature
-----
1.    Permit    Create        all
2.    Permit    Create        user access
3.    Permit    Create        system
4.    Permit    Create        changeto
```

```
Role: Network-Admin (System-defined)
Description: Admin for L3 (IP and Routes) and L4 VIPs
Number of rules: 5
```

```
-----
Rule    Type    Permission    Feature
-----
1.    Permit    Create        interface
2.    Permit    Create        connection
3.    Permit    Create        nat
4.    Permit    Create        config_copy
5.    Permit    Create        changeto
```

```
Role: Security-Admin (System-defined)
Description: Administrator for all security features
Number of rules: 8
```

```

-----
Rule      Type      Permission      Feature
-----
1.    Permit    Create          access-list
2.    Permit    Create          inspect
3.    Permit    Create          connection
4.    Permit    Modify          interface
5.    Permit    Create          aaa
6.    Permit    Create          nat
7.    Permit    Create          config_copy
8.    Permit    Create          changeto

```

```

Role: Network-Monitor (System-defined)
Description: Monitoring for all features
Number of rules: 2

```

```

-----
Rule      Type      Permission      Feature
-----
1.    Permit    Monitor         all
2.    Permit    Monitor         changeto

```

Displaying Virtualization Configuration and Statistics

This task describes the available commands to display to display configuration and statistical information for the contexts configured on your VFW application. There is no specific order to the steps in this task.

Prerequisites

You must attach from the route processor to the VFW application before you can perform this task. See the [“Attaching to the VFW Application”](#) section on page VFC-14.

SUMMARY STEPS

1. **show context** *context-name*
2. **show resource allocation**
3. **show resource usage context** *name* **resource conc-connections counter denied** *count_threshold*
4. **show role**
5. **show domain** *name*
6. **show users** *name*
7. **show user-account** *name*
8. **clear user** *name*
9. **clear statistics all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>show context <i>context-name</i></p> <p>Example: firewall/Admin# show context C1</p>	(Optional) Displays a list of contexts including the name, description, resource class, and interfaces.
Step 2	<p>show resource allocation</p> <p>Example: firewall/C1# show resource allocation</p>	(Optional) Displays the allocation for each resource across all resource classes and class members. This command shows the resource allocation, but does not show the actual resources being used.
Step 3	<p>show resource usage context <i>name</i> resource conc-connections counter denied <i>count_threshold</i></p> <p>Example: firewall/C1# show resource allocation context C1 resource concurrent-connections counter denied 0</p>	(Optional) Displays the resource usage for each context from the Admin context.
Step 4	<p>show role</p> <p>Example: firewall/C1# show role</p>	(Optional) Displays predefined and user-configured roles.
Step 5	<p>show domain <i>name</i></p> <p>Example: firewall/C1# show domain D1</p>	(Optional) Displays information about the configured domains in the VFW application.
Step 6	<p>show users <i>name</i></p> <p>Example: firewall/C1# show users admin</p>	(Optional) Displays information about users that are currently logged in to the VFW application.
Step 7	<p>show user-account <i>name</i></p> <p>Example: firewall/C1# show user-account admin</p>	(Optional) Displays user account information.
Step 8	<p>clear user <i>name</i></p> <p>Example: firewall/C1# clear user John</p>	(Optional) Forces a user to log out (clears the user session).
Step 9	<p>clear stats all</p> <p>Example: firewall/C1# clear stats all</p>	(Optional) Clears all statistical information in a context.

Configuration Examples for Virtualization

The following running-configuration example illustrates a basic virtualization configuration with one user-defined context, one resource class, one domain, and one user.

```
firewall/Admin(config)# resource-class RC1
firewall/Admin(config-resource)# limit-resource rate syslog minimum 10.00 maximum
equal-to-min
firewall/Admin(config-resource)# limit-resource acl-memory minimum 10.00 maximum unlimited
firewall/Admin(config-resource)# exit

firewall/Admin(config)# access-list ACL1 line 10 extended permit ip any any

firewall/Admin(config)# domain D1
firewall/Admin(config-domain)# add-object access-list extended ACL1
firewall/Admin(config-domain)# exit

firewall/Admin(config)# role Admin

firewall/Admin(config)# context C1
firewall/Admin(config-context)# description accounting department
firewall/Admin(config-context)# member RC1
firewall/Admin(config-context)# exit

firewall/Admin(config)# username JANE password 5 adropgijaeprgja9erjg2uWgtce1 role Admin
domain D1
```

Additional References

The following sections provide references related to virtualization.

Related Documents

Related Topic	Document Title
Virtual firewall virtualization command syntax	“Virtualization Commands on the Virtual Firewall” module in <i>Cisco IOS XR Virtual Firewall Command Reference</i>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport