

ASA 8.0 SSLVPN (WebVPN): Расширенная настройка портала

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Требования к конфигурации](#)

[Условные обозначения](#)

[Обзор возможностей пользовательской настройки](#)

[Улучшение восприятия интерфейса](#)

[Виртуализация](#)

[Поддерживаемые страницы](#)

[Пользовательская настройка web-портала](#)

[Панель заголовка](#)

[URL-адрес логотипа](#)

[Панель инструментов](#)

[Web-закладки с эскизами](#)

[Пользовательские области: Трансляция RSS](#)

[Пользовательские области: Пользовательская страница интрасети](#)

[Пользовательские названия вкладок приложений](#)

[Пользовательские эскизы приложений](#)

[Пользовательские страницы справки для приложений](#)

[Проверка пользовательских настроек](#)

[Пользовательская настройка страницы входа](#)

[Подготовка собственного HTML-файла](#)

[Изменение ссылок на место хранения изображений](#)

[Переименование HTML-файла](#)

[Добавление кода в файл login.inc](#)

[Загрузка файла login.inc и файлов изображений в ASA в виде web-контента](#)

[Выбор файла login.inc для полной пользовательской настройки](#)

[Проверка полной пользовательской настройки](#)

[Поддержка интерфейса командной строки](#)

[Резервное копирование пользовательских настроек](#)

[Заключение](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

Введение

В версии 8.0 программного обеспечения для устройств адаптивной защиты Cisco ASA серии 5500 введены развитые возможности пользовательской настройки, позволяющие создавать эстетичные web-порталы для пользователей с бесклиентским доступом. В этом документе рассмотрено множество доступных вариантов пользовательской настройки страницы входа в систему, также называемой экраном приветствия, и страницы web-портала.

Предварительные условия

Требования

Для настройки групповых политик и профилей подключения на ASA компания Cisco рекомендует ознакомиться с Менеджером устройств адаптивной защиты Cisco (ASDM).

Для получения общих сведений см. следующие документы:

- [Раздел Настройка бесклиентской сети VPN на основе SSL в Руководстве Cisco по настройке безопасности в командной строке, версия 8.0](#)
- [Руководство пользователя ASDM 6.0](#)

Перед настройкой пользовательского web-портала необходимо выполнить несколько базовых шагов для настройки ASA. [Для получения дополнительных сведений см. раздел Требования к конфигурации данного документа.](#)

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco ASA версии 8.x
- Cisco ASDM версии 6.x

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

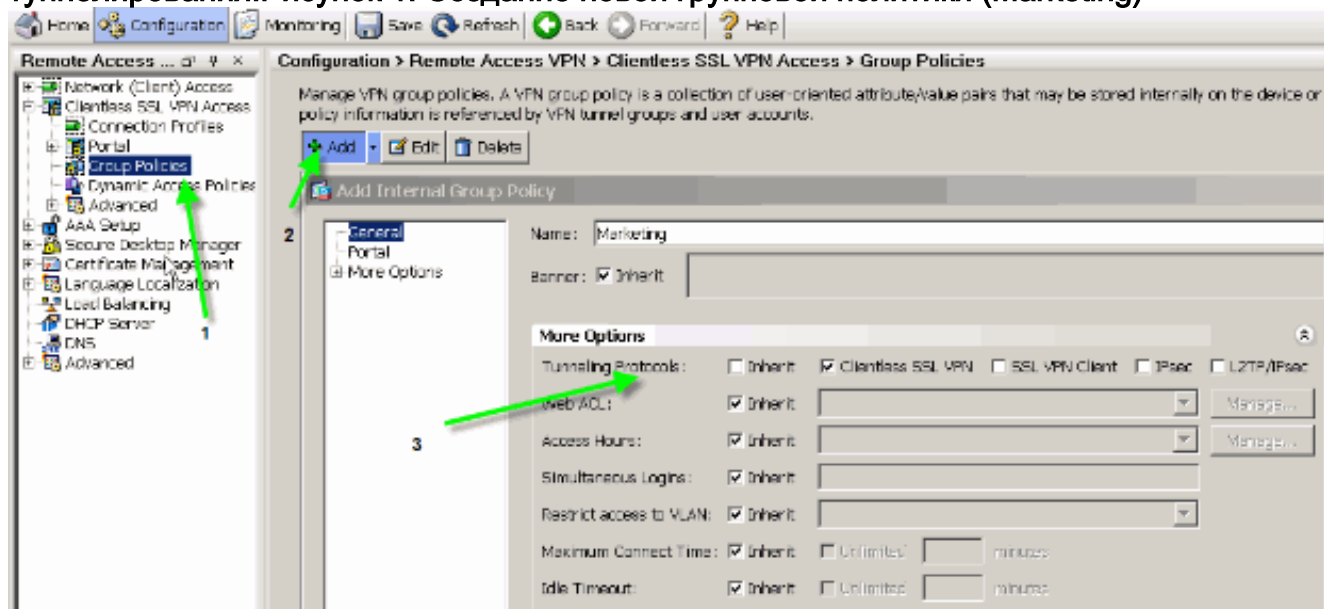
Требования к конфигурации

Необходимо предварительно настроить устройство ASA для выполнения операций настройки, описанных в этом документе.

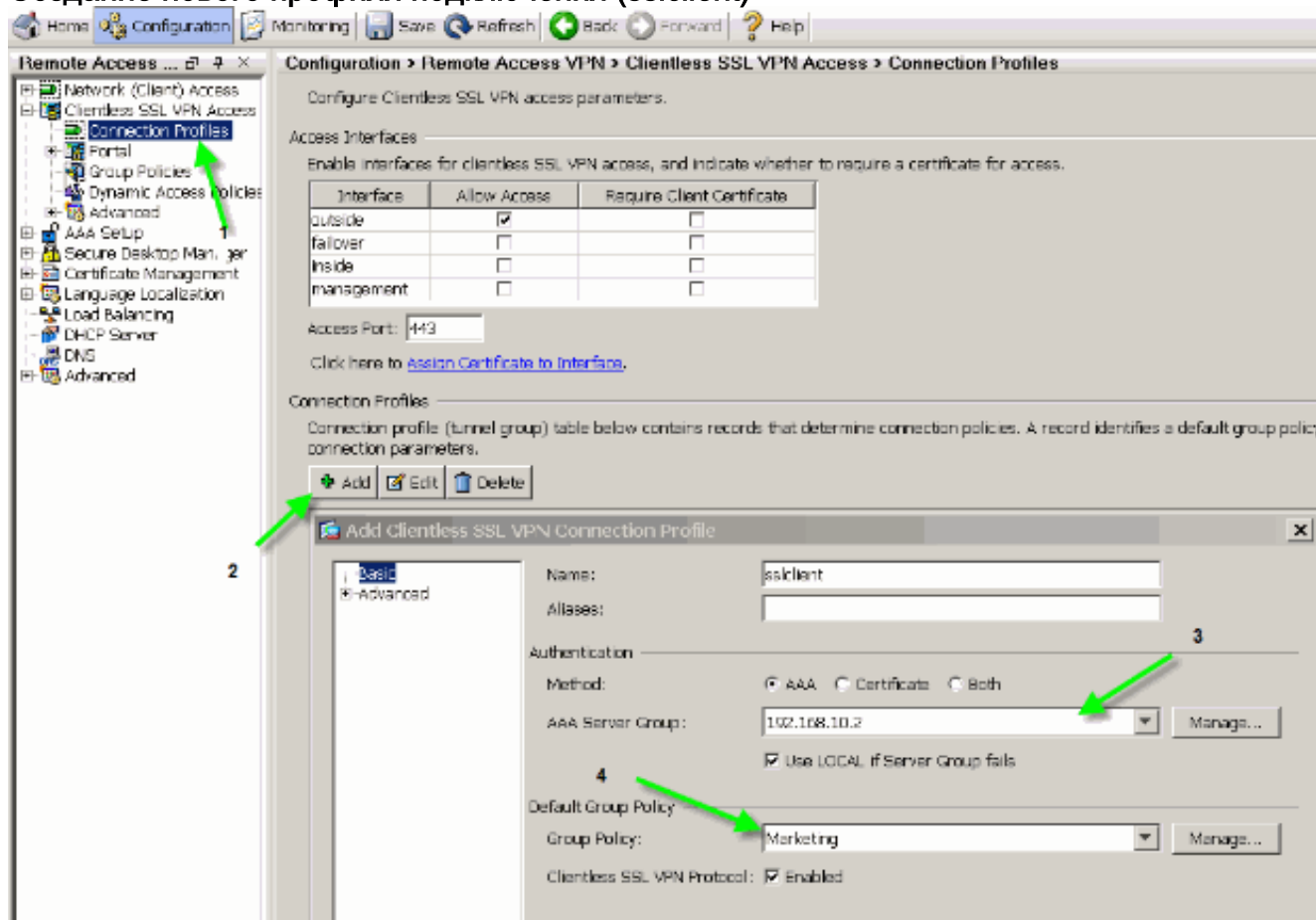
Выполните следующие действия:

1. Для создания групповой политики (например, Marketing) в ASDM выберите Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies (Конфигурация > VPN для удаленного доступа > Доступ по бесклиентской сети VPN на основе SSL > Групповые политики) и отметьте флажок Clientless SSL VPN (Бесклиентская сеть VPN на основе SSL) в разделе протоколов

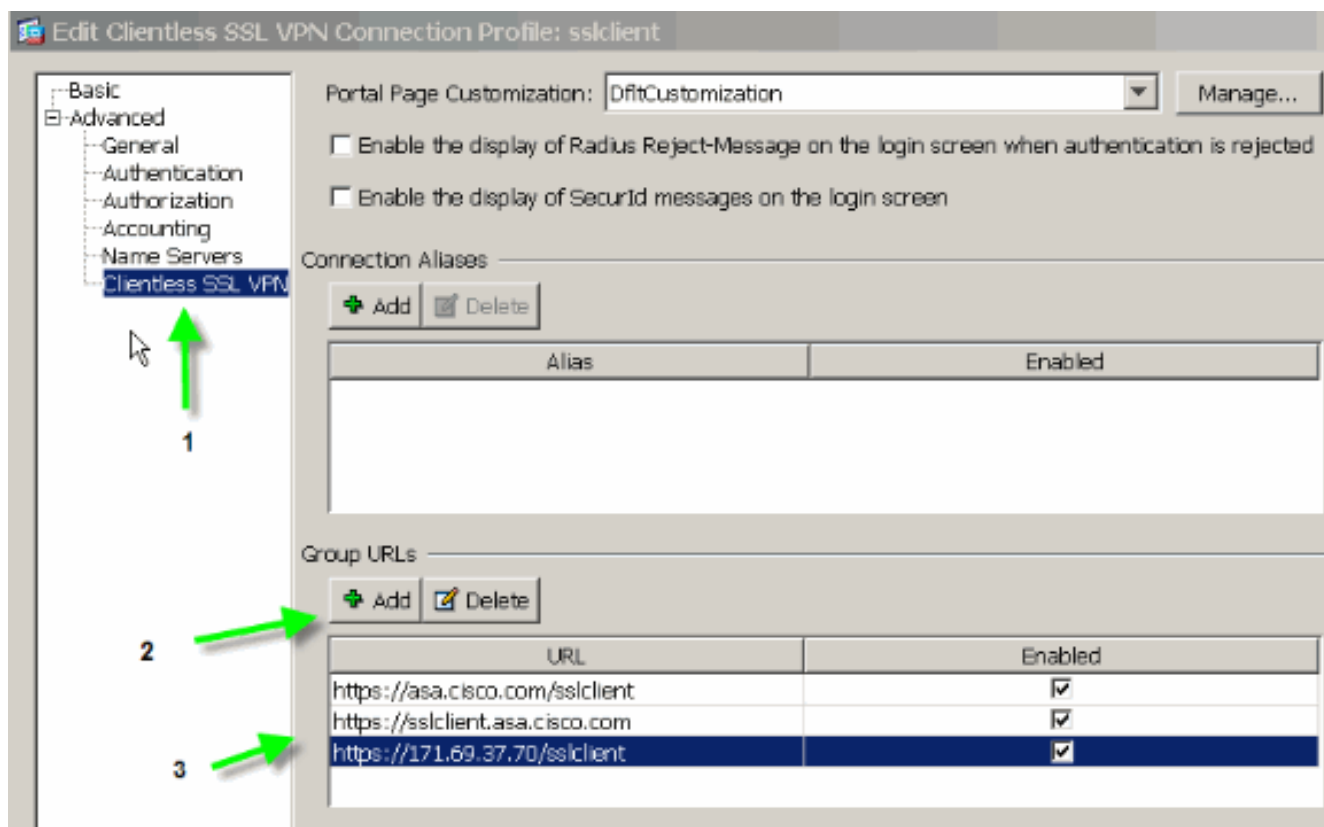
тунnelирования. Рисунок 1: Создание новой групповой политики (Marketing)



2. Для создания нового профиля подключения (например, sslclient) выберите Configuration > Remote Access VPN > Clientless SSL VPN > Connection Profiles (Конфигурация > VPN для удаленного доступа > Бесклиентская сеть VPN на основе SSL > Профили подключения), укажите необходимые реквизиты сервера аутентификации, например сервера AAA, и назначьте группу политик Marketing. Рис. 2: Создание нового профиля подключения (sslclient)

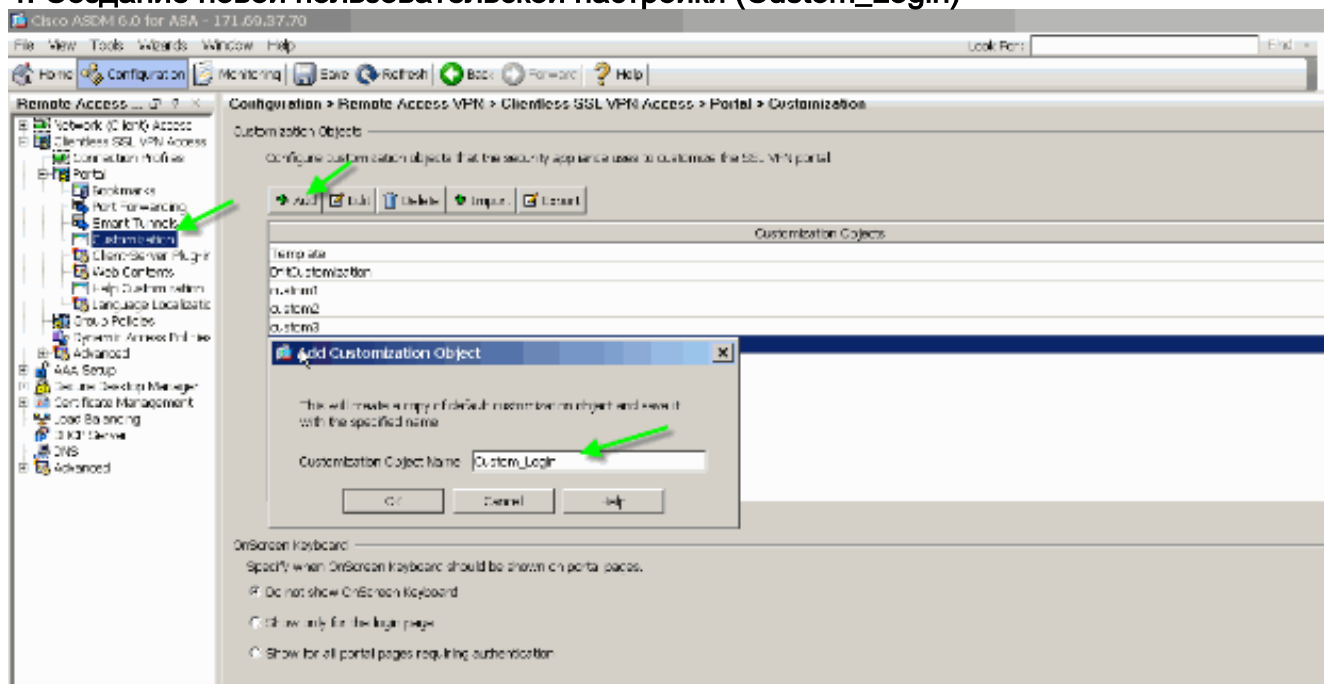


3. Для продолжения настройки профиля подключения выберите Advanced и укажите URL-адрес группы для профиля подключения. Рис. 3: Настройка URL-адресов группы для профиля подключения



Примечание: В данном примере URL группы настроен в трех различных форматах. Для подключения к ASA посредством профиля подключения sslclient пользователь может ввести любой из них.

4. Выберите Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization (Конфигурация > VPN для удаленного доступа > Доступ по бесклиентской сети VPN на основе SSL > Портал > Пользовательская настройка) и добавьте два объекта пользовательской настройки: Custom_Login Custom_Marketing
- Рис. 4: Создание новой пользовательской настройки (Custom_Login)**



Примечание: [Рис. 4 иллюстрирует создание объекта Custom_Login](#). Повторите эти шаги для добавления объекта пользовательской настройки Custom_Marketing. Пока не редактируйте добавленные объекты. Разные варианты конфигурации обсуждаются в последующих разделах этого документа.

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

Обзор возможностей пользовательской настройки

В типичном бесклиентском сценарии удаленный пользователь вводит в браузере полное имя домена (FQDN) устройства ASA для регистрации на устройстве. При этом появляется страница входа в систему или экран приветствия. После успешного прохождения аутентификации пользователю становится доступен для просмотра web-портал со всеми разрешенными приложениями.

В версиях ниже 8.0 web-портал поддерживает ограниченные возможности пользовательской настройки: всем пользователям ASA представляется один и тот же набор web-страниц. Эти web-страницы имеют ограниченное графическое оформление и заметно отличаются от типичного вида страниц в интрасети.

Улучшение восприятия интерфейса

ASA предусматривает полноценные средства пользовательской настройки, позволяющие совместить функциональный механизм входа в систему с существующим набором web-страниц. Существенные усовершенствования претерпела и пользовательская настройка web-портала. Рассмотренные в этом документе примеры показывают настройку страницы ASA, позволяющую приблизить вид страниц ASA к существующим страницам интрасети для создания более последовательного пользовательского интерфейса при работе со страницами ASA.

Виртуализация

Гибкость пользовательской настройки подкрепляет возможности ASA в части виртуализации взаимодействия с пользователем. Например, страница входа в систему и web-портал, доступные группе маркетинга, могут полностью отличаться от внешнего вида страниц для групп, представляющих отдел продаж и проектный отдел.

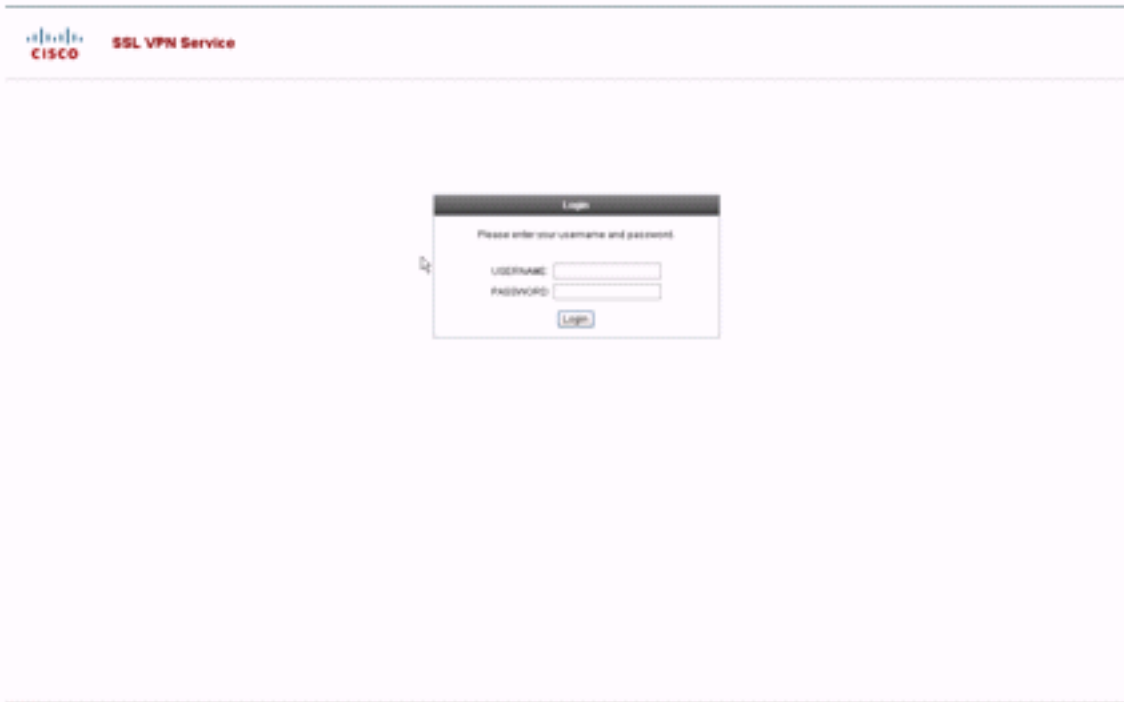
Поддерживаемые страницы

ASA поддерживает два различных типа страниц WebVPN, которые являются настраиваемыми.

Страница входа в систему

Когда пользователь вводит в браузере URL-адрес группы `https://asa.cisco.com/sslclient` для подключения к устройству ASA, появляется следующая страница входа в систему по умолчанию:

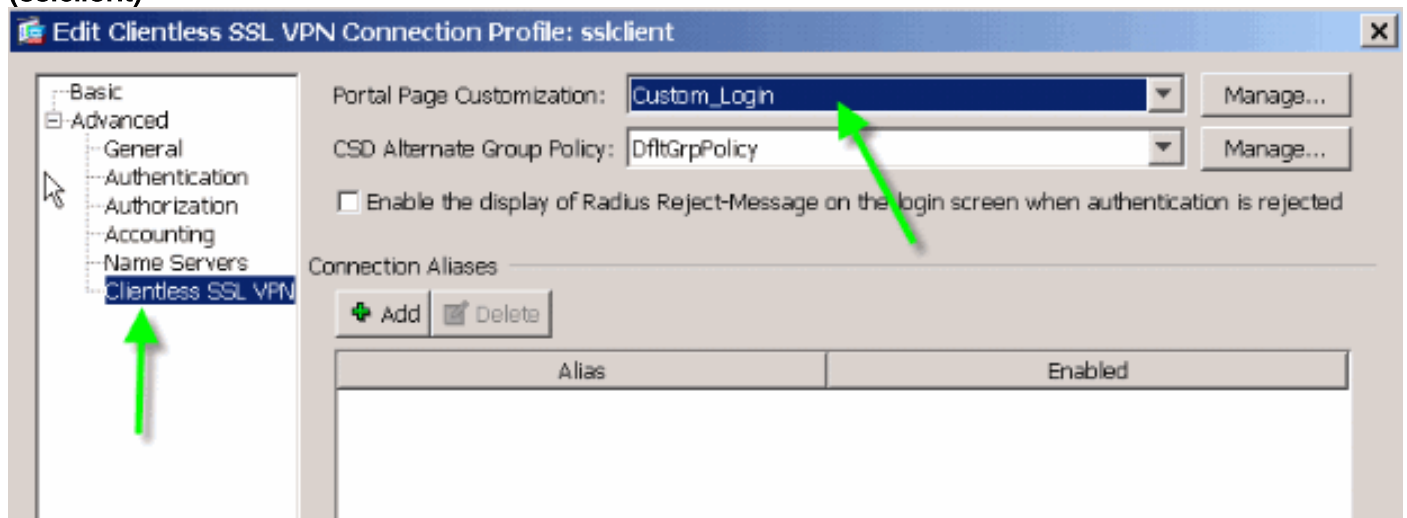
Рис. 5: Страница входа по умолчанию



Для изменения этой страницы входа в систему необходимо отредактировать конфигурацию, связанную с профилем подключения. [Шаги, необходимые для изменения соответствующих настроек, описаны в разделе данного документа Пользовательская настройка страницы входа.](#) Пока же выполните следующие действия:

1. Выберите Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles (Конфигурация > VPN для удаленного доступа > Доступ по бесклиентской сети VPN на основе SSL > Профили подключений).
2. Отредактируйте профиль подключения sslclient и свяжите с ним пользовательскую настройку Custom_Login.

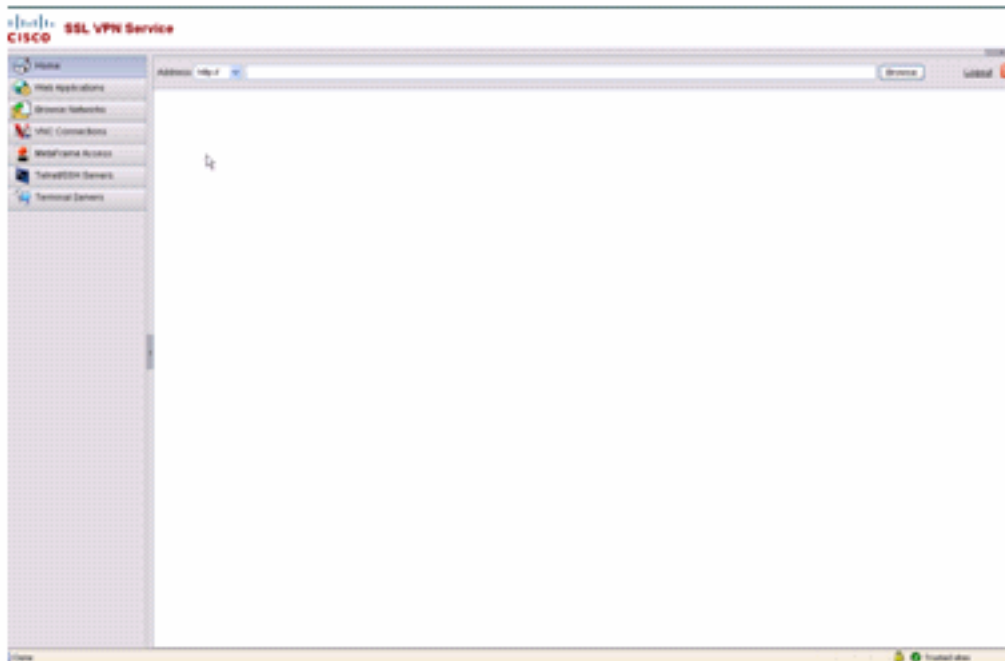
Рис. 6: Связывание пользовательской настройки (Custom_Login) с профилем подключения (sslclient)



[Страница портала](#)

После того как пользователь пройдет аутентификацию, появится следующая страница web-портала по умолчанию1:

Рисунок 7: Страница портала по умолчанию

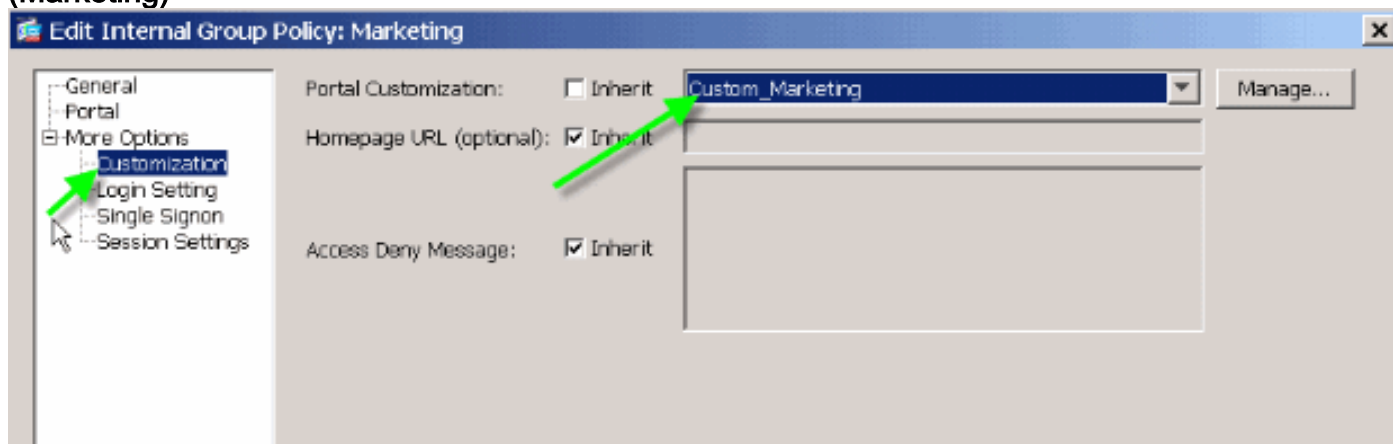


1. Предполагается, что активны все подключаемые модули (VNC, ICA, SSH и RDP). Если подключаемые модули не активированы, то их вкладки будут отсутствовать.

Для изменения этой страницы web-портала необходимо отредактировать настройку, связанную с групповой политикой. [Шаги, необходимые для изменения соответствующих настроек, описаны в разделе данного документа Пользовательская настройка web-портала.](#) Пока же выполните следующие действия:

1. Выберите Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies (Конфигурация > VPN для удаленного доступа > Доступ по бесклиентской сети VPN на основе SSL > Групповые политики).
2. Отредактируйте групповую политику Marketing и свяжите с ней пользовательскую настройку Custom_Marketing.

Рис. 8: Связывание пользовательской настройки (Custom_Marketing) с групповой политикой (Marketing)



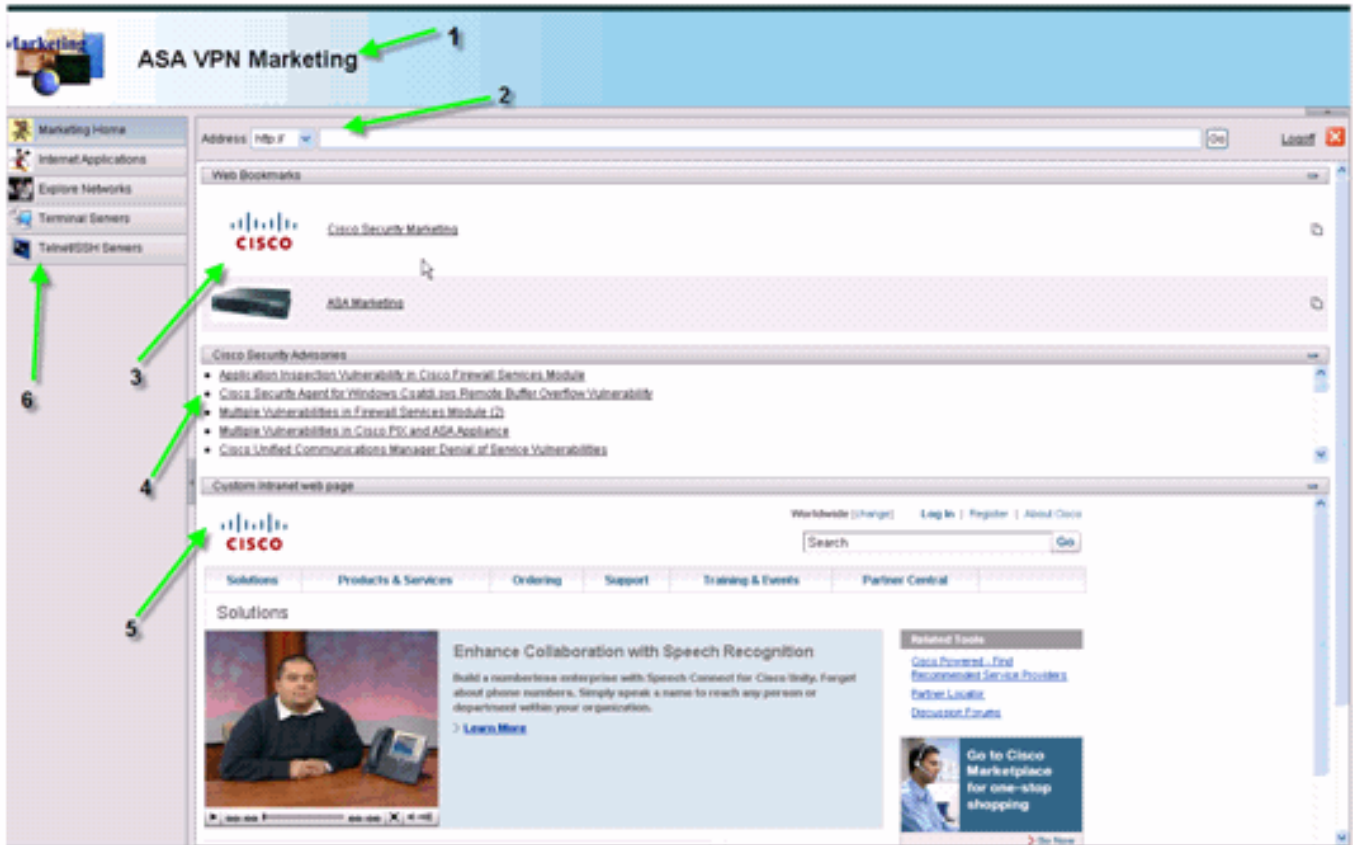
Примечание: Профили множественного соединения, каждый с их собственной схемой проверки подлинности, такие как RADIUS, LDAP, или Сертификаты, может быть привязан к одиночной групповой политике. Поэтому можно создать несколько страниц входа в систему, например предусмотрев индивидуальные настройки входа в систему для каждой конфигурации подключения, и связать их все с одной настройкой web-портала, которая

связана с групповой политикой Marketing.

Пользовательская настройка web-портала

Ниже приведен пример пользовательской настройки web-портала:

Рис. 9: Пользовательская страница web-портала



Можно заметить, что на странице имеются: заголовок с градиентной цветовой схемой, логотип отдела маркетинга, несколько web-закладок с эскизами, трансляция RSS и пользовательская страница интрасети. Пользовательская страница интрасети позволяет конечному пользователю перемещаться по своей странице интрасети и одновременно использовать другие вкладки на web-портале.

Примечание: Все еще необходимо сохранить план веб-страницы с вершиной и оставленными кадрами, что означает, что строго говоря эта страница не полностью настраиваема. Можно изменить множество второстепенных компонентов для максимального приближения к виду порталов в интрасети.

Этот раздел освещает настройку каждого отдельного компонента в web-портале посредством редактора настройки в ASDM.

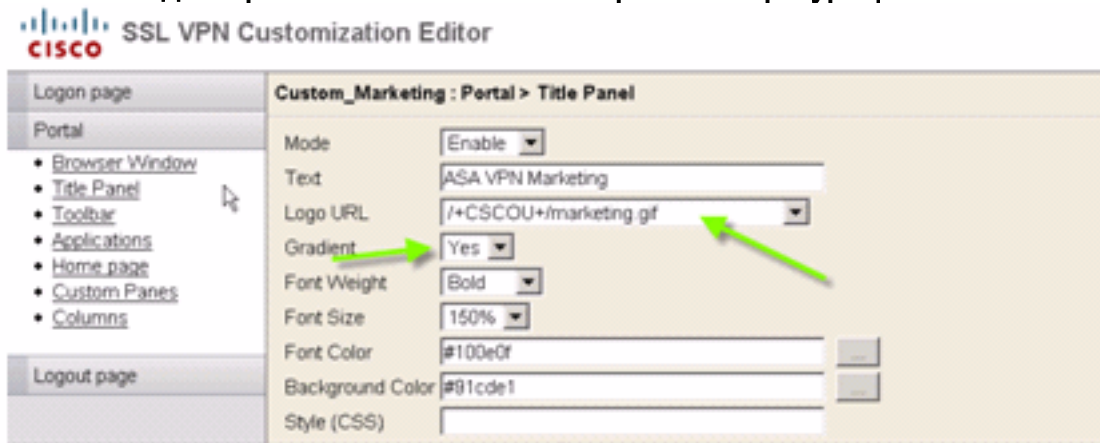
Панель заголовка

Рис. 10: Панель заголовка



Для настройки панели заголовка действуют следующие параметры:

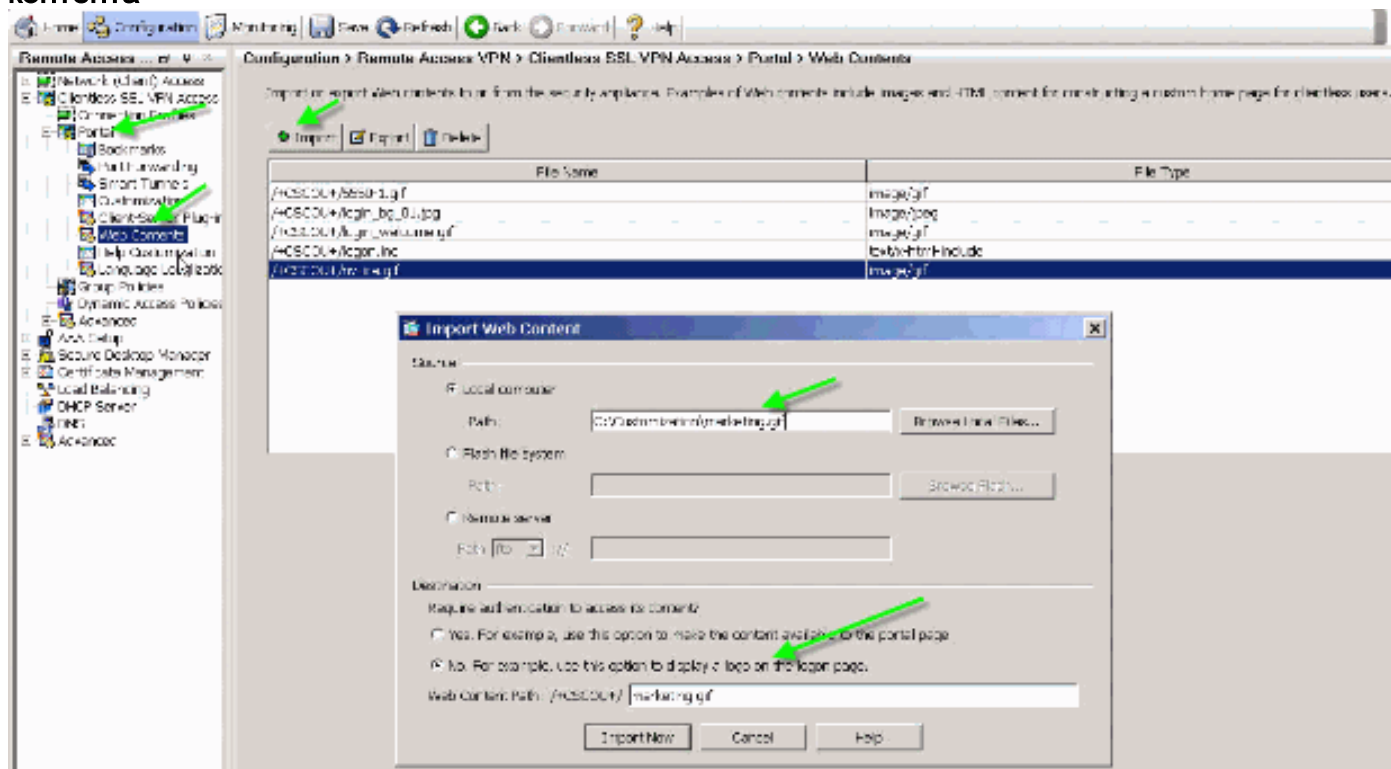
Рис. 1-1: Редактор пользовательских настроек: Конфигурация панели заголовка



URL-адрес логотипа

Для настройки логотипа в панели заголовка загрузите изображение логотипа в устройство ASA.

Рисунок 12: Загрузка файла логотипа marketing.gif в устройство ASA в качестве web-контента



1. Выберите Clientless SSL VPN Access > Portal > Web Contents (Доступ по бесклиентской сети VPN на основе SSL > Портал > Web-контент), нажмите Import (Импортировать) и укажите путь к файлу логотипа на локальном компьютере. Загрузите это в каталог /+CSCOU+/ в качестве web-контента.
2. Введите URL-адрес логотипа /+CSCOU+/marketing.gif в виде, показанном на рис. 12.
3. В качестве текста введите ASA VPN Marketing.
4. Для выбора цвета шрифта и цвета фона нажмите кнопку .
5. Для создания эстетичного цветового перехода включите параметр Gradient (Градиент).

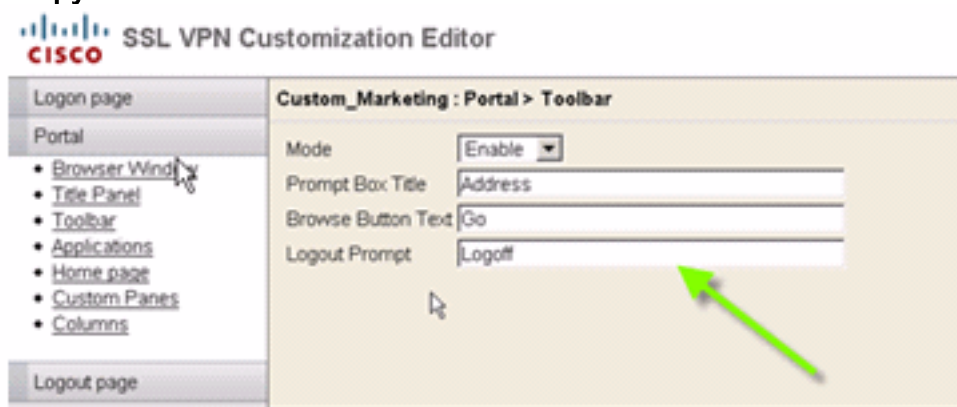
[Панель инструментов](#)

Рисунок 13: Панель инструментов с пользовательской настройкой



Для настройки этого адреса/панели инструментов отредактируйте следующие параметры:

Рисунок 14: Редактор пользовательских настроек: Пользовательская настройка панели инструментов



Примечание: По умолчанию Панель инструментов включена. В этом примере в соответствии с иллюстрацией переименовываются остальные поля, такие как Prompt Box Title (Заголовок поля приглашения), текст кнопки Browse (Обзор) и Logout Prompt (Приглашение при выходе из системы).

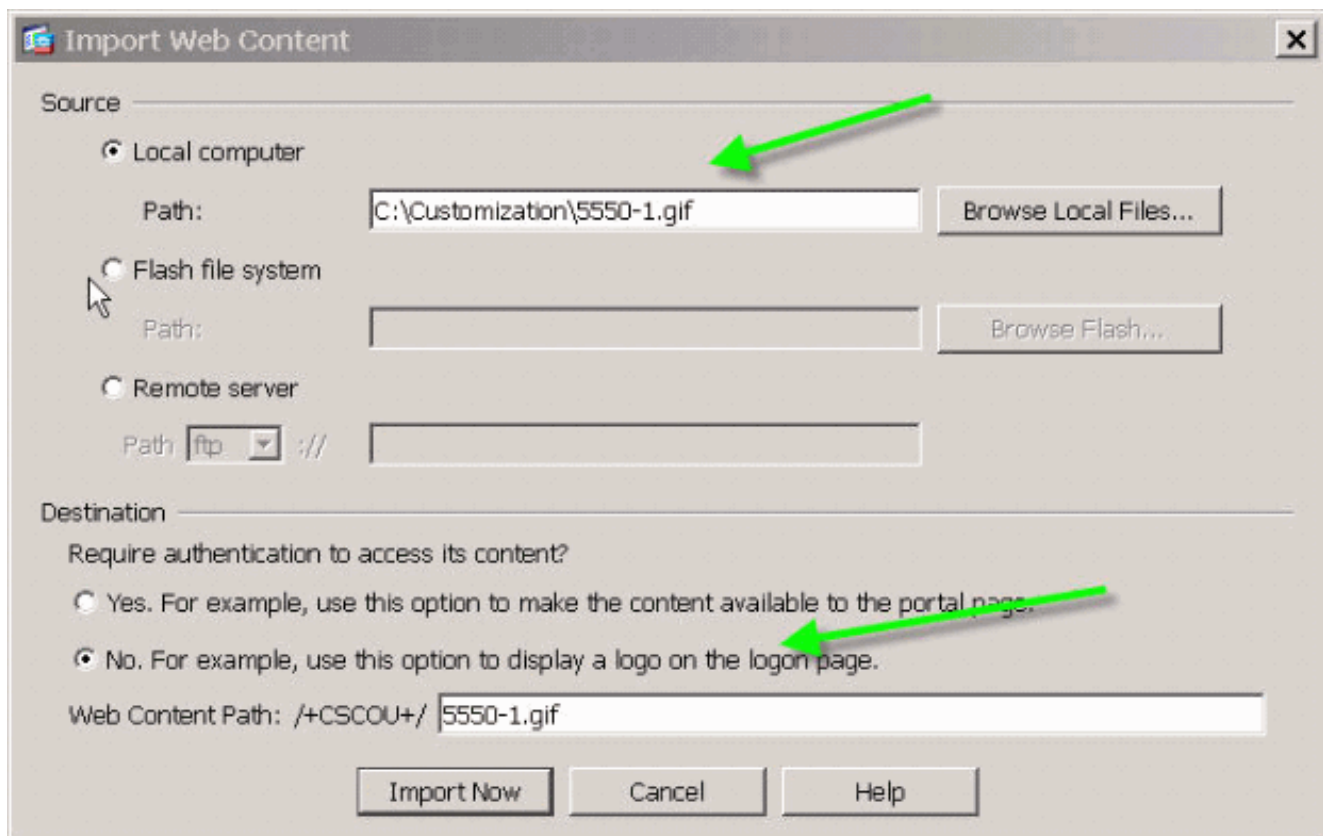
[Web-закладки с эскизами](#)

Рисунок 15: Пользовательская настройка web-закладок с эскизами

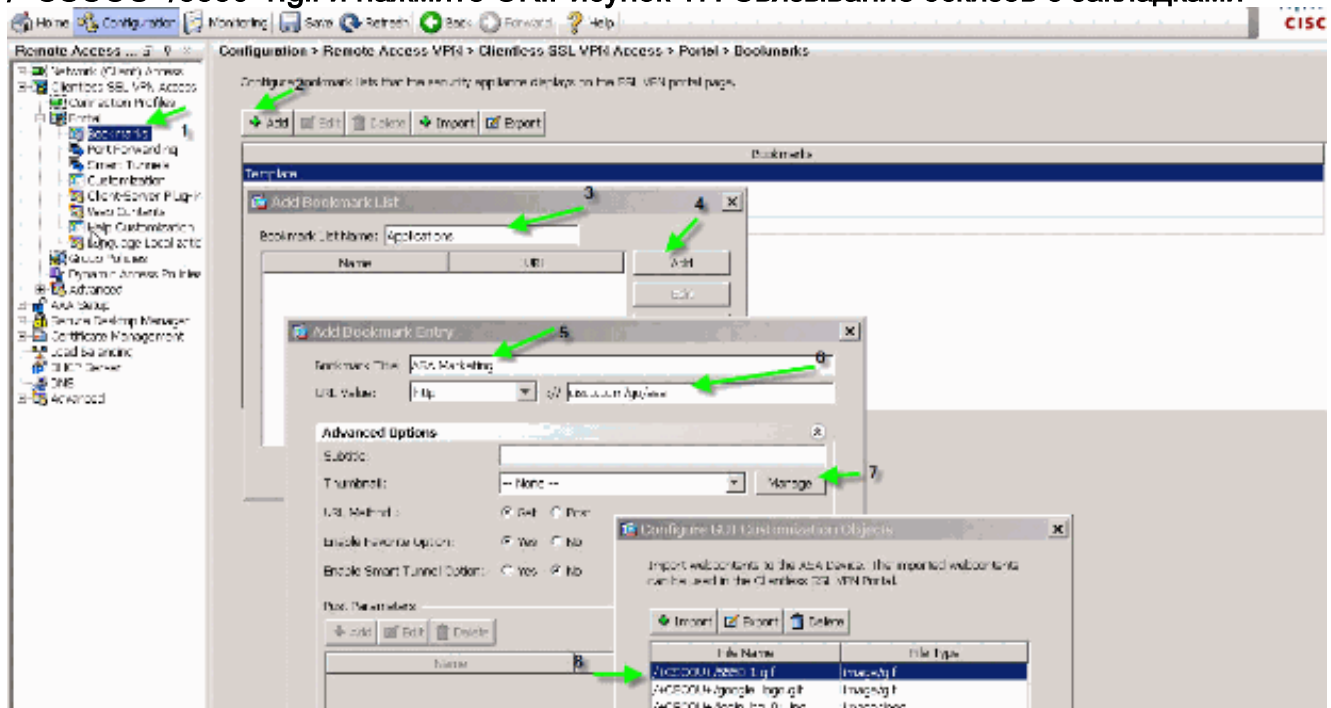


Для добавления эскизов рядом с закладками выполните следующие шаги:

1. Загрузите требуемое изображение в каталог /+CSCOU+/. **Рисунок 16: Загрузка эскиза, связываемого с закладками**

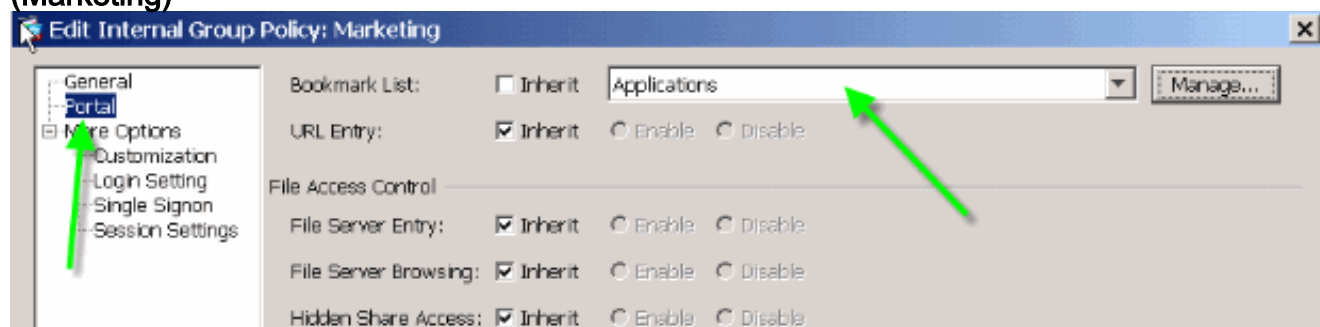


2. Свяжите эскиз с закладками ASA. Выберите Portal > Bookmarks (Портал > Закладки). Нажмите Add. В поле Bookmark List Name (Наименование списка закладок) введите Applications (Приложения). Нажмите Add. В поле Bookmark Title (Заголовок закладки) введите ASA Marketing (ASA-маркетинг). В качестве URL-адреса введите <http://cisco.com/go/asa>, затем выберите Advanced Options (Дополнительные параметры). Щелкните Manage (Управление). Выберите ранее загруженный эскиз /+CSCOU+/5550-1.gif и нажмите ОК. Рисунок 17: Связывание эскизов с закладками



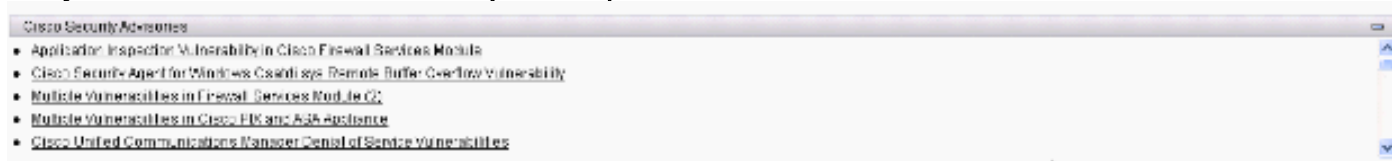
3. Свяжите закладки с групповой политикой ASA. Выберите Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies (Конфигурация > VPN для удаленного доступа > Доступ по бесклиентской сети VPN на основе SSL > Групповые политики) и отредактируйте политику Marketing. Выберите Portal (Портал). Снимите

флажок Inherit рядом со списком закладок и выберите Applications (Приложения) в раскрывающемся меню. Рисунок 18: Связывание закладок с групповой политикой (Marketing)



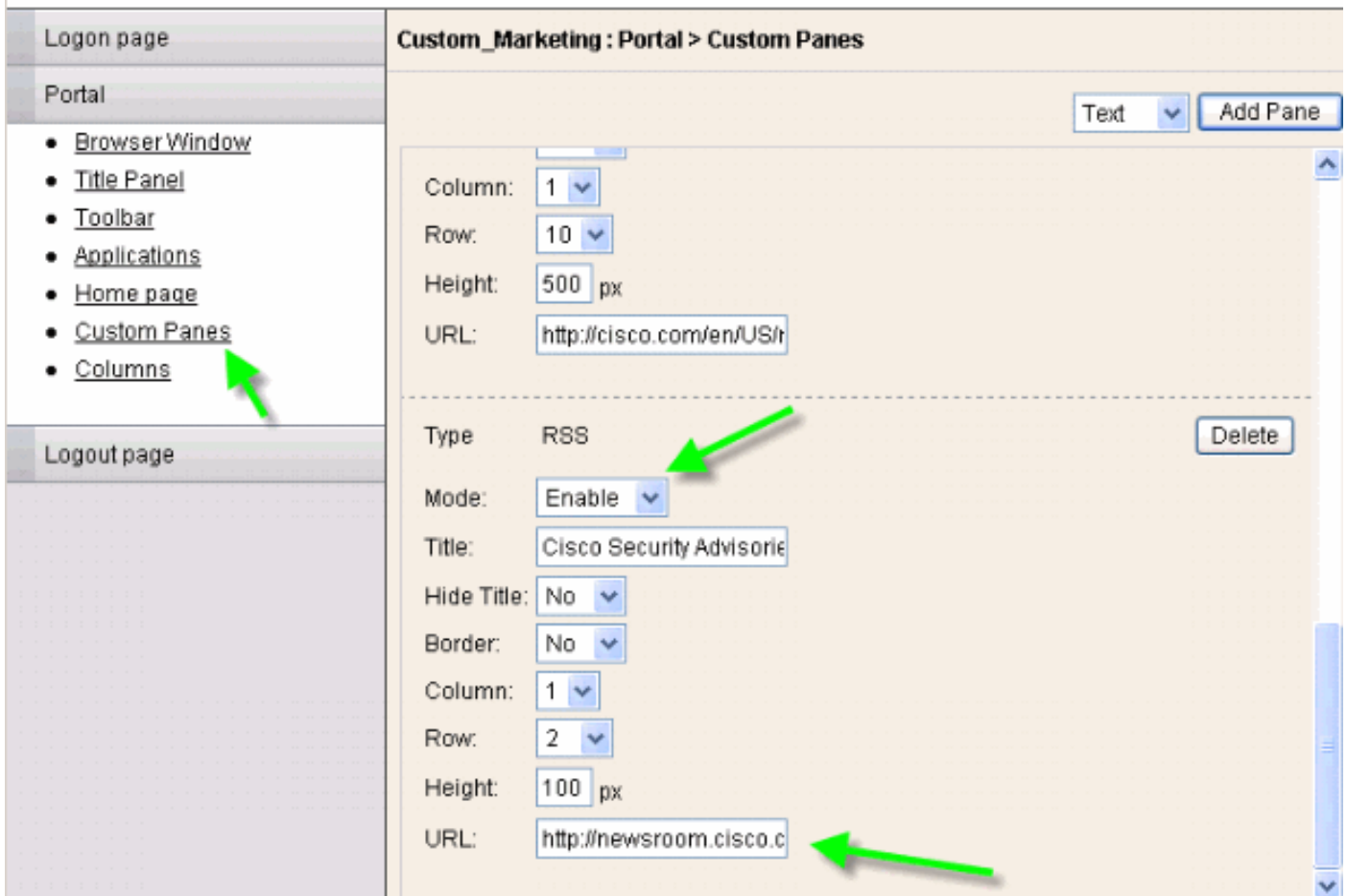
Пользовательские области: Трансляция RSS

Рисунок 19: Пользовательская трансляция RSS



Для отображения пользовательской трансляции RSS отредактируйте следующие элементы настройки:

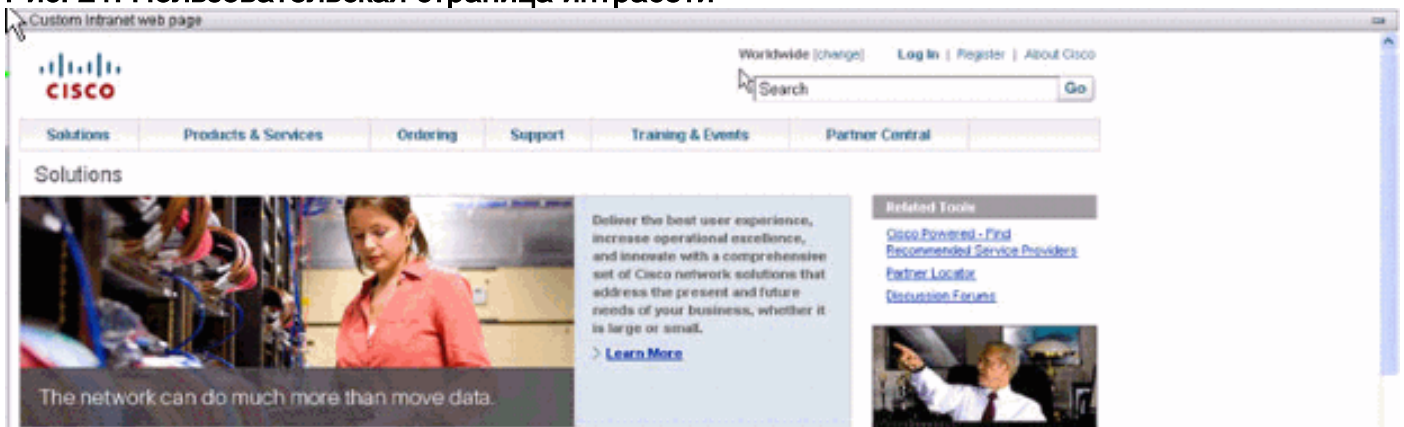
Рис. 20: Пользовательские области: Настройка трансляции RSS



Примечание: Каналы RSS для рекомендации по вопросам безопасности Cisco: http://отдел_новостей.cisco.com/data/syndication/rss2/SecurityAdvisories_20.xml.

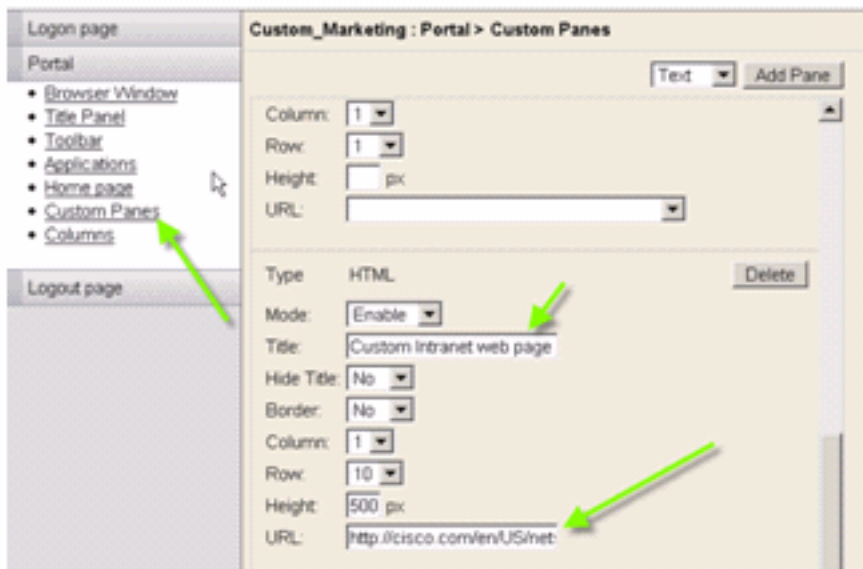
Пользовательские области: Пользовательская страница интрасети

Рис. 21: Пользовательская страница интрасети



Для настройки пользовательской страницы интрасети отредактируйте следующие элементы:

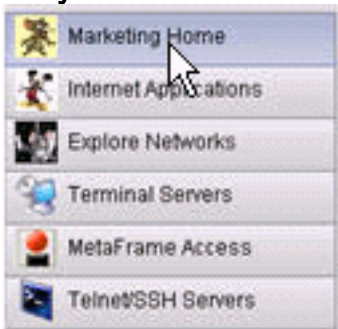
Рисунок 22: Редактор пользовательских настроек: Настройка пользовательских областей



Примечание: URL для страницы Cisco CCO: <http://cisco.com/en/US/netsol>.




























Пользовательские названия вкладок приложений

Рисунок 23: Пользовательские названия вкладок приложений



Для настройки названий вкладок приложений отредактируйте следующие элементы:

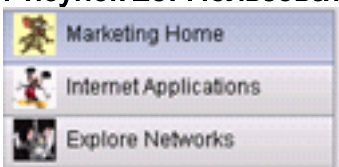
Рисунок 24: Пользовательская настройка названий вкладок приложений

Logon page	Custom_Marketing : Portal > Applications																																				
Portal																																					
<ul style="list-style-type: none"> • Browser Window • Title Panel • Toolbar • Applications • Home page • Custom Panes • Columns 	<table border="1"> <tr> <td>1. </td> <td>Marketing Home</td> <td>Enable</td> <td>Down</td> </tr> <tr> <td>2. </td> <td>Internet Applications</td> <td>Enable</td> <td>Up Down</td> </tr> <tr> <td>3. </td> <td>Explore Networks</td> <td>Enable</td> <td>Up Down</td> </tr> <tr> <td>4. </td> <td>Application Access</td> <td>Disable</td> <td>Up Down</td> </tr> <tr> <td>5. </td> <td>Corporate Network - AnyConnect</td> <td>Disable</td> <td>Up Down</td> </tr> <tr> <td>6. </td> <td>VNC Connections</td> <td>Disable</td> <td>Up Down</td> </tr> <tr> <td>7. </td> <td>Terminal Servers</td> <td>Enable</td> <td>Up Down</td> </tr> <tr> <td>8. </td> <td>Telnet/SSH Servers</td> <td>Enable</td> <td>Up Down</td> </tr> <tr> <td>9. </td> <td>MetaFrame Access</td> <td>Enable</td> <td>Up</td> </tr> </table>	1. 	Marketing Home	Enable	Down	2. 	Internet Applications	Enable	Up Down	3. 	Explore Networks	Enable	Up Down	4. 	Application Access	Disable	Up Down	5. 	Corporate Network - AnyConnect	Disable	Up Down	6. 	VNC Connections	Disable	Up Down	7. 	Terminal Servers	Enable	Up Down	8. 	Telnet/SSH Servers	Enable	Up Down	9. 	MetaFrame Access	Enable	Up
1. 	Marketing Home	Enable	Down																																		
2. 	Internet Applications	Enable	Up Down																																		
3. 	Explore Networks	Enable	Up Down																																		
4. 	Application Access	Disable	Up Down																																		
5. 	Corporate Network - AnyConnect	Disable	Up Down																																		
6. 	VNC Connections	Disable	Up Down																																		
7. 	Terminal Servers	Enable	Up Down																																		
8. 	Telnet/SSH Servers	Enable	Up Down																																		
9. 	MetaFrame Access	Enable	Up																																		
Logout page																																					

Примечание: Вы выборочно включаете приложения и также перестраиваете их с Вверх и вниз по ссылкам.

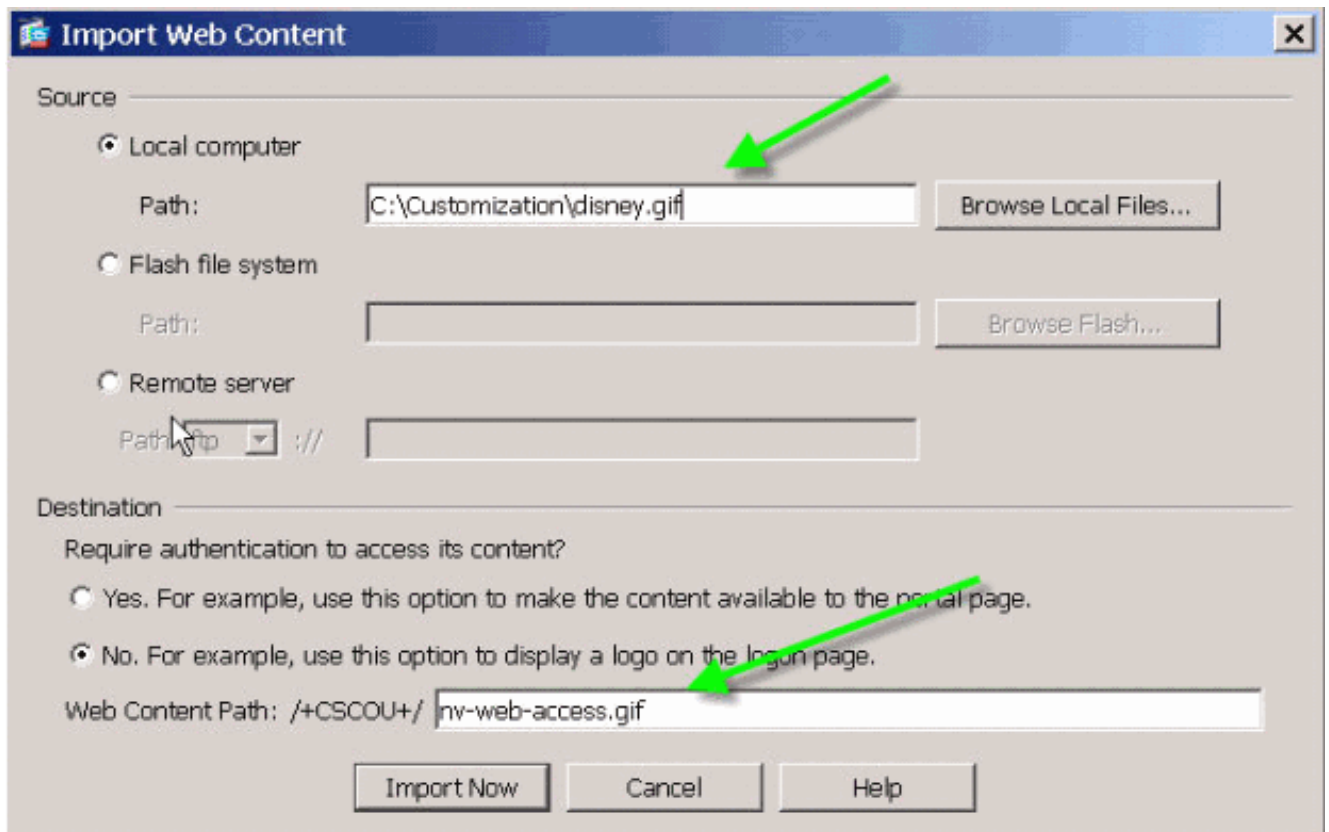
[Пользовательские эскизы приложений](#)

Рисунок 25: Пользовательские эскизы приложений



Для того чтобы сопроводить имена приложений эскизами предпочтительного вида, наподобие показанных в примере значков, выполните следующие шаги:

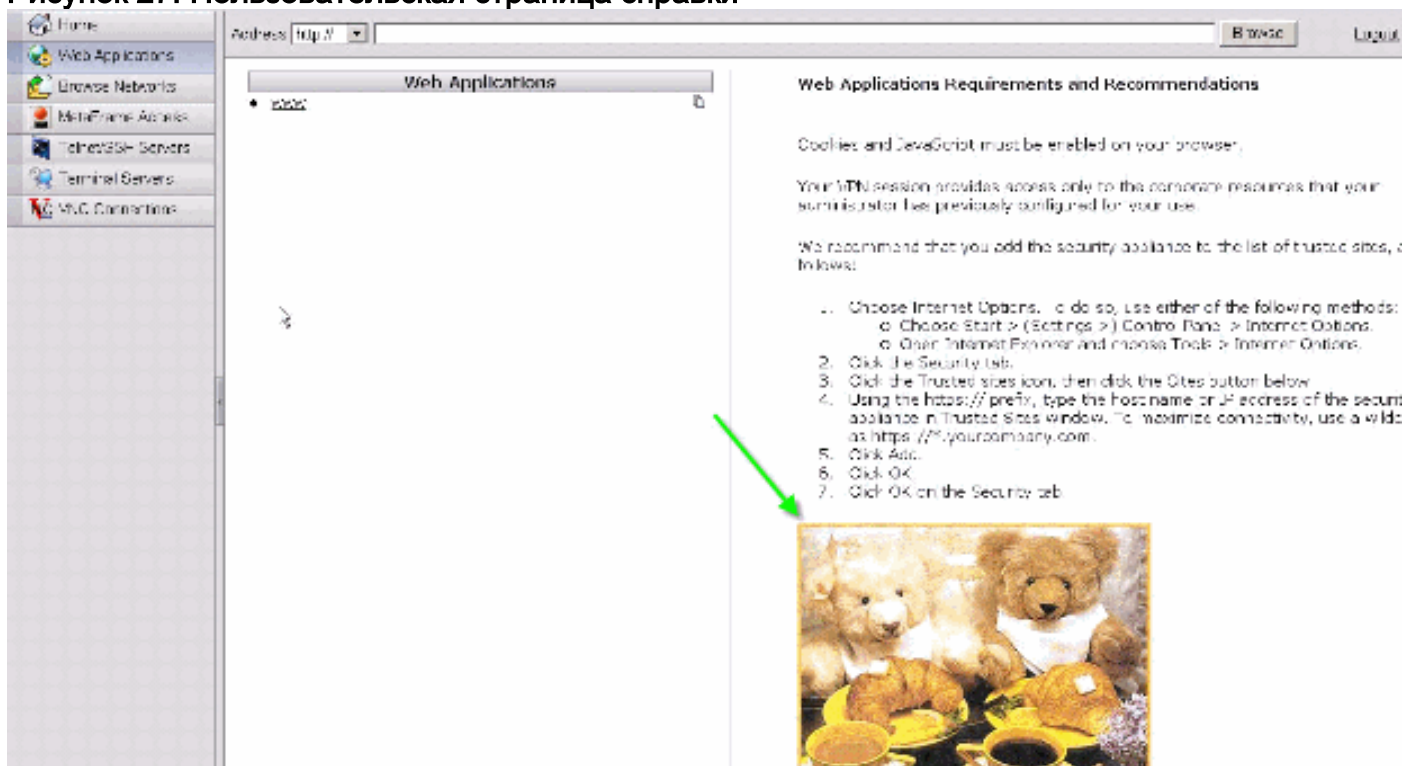
1. Со страницы портала щелкните правой кнопкой мыши на эскизе по умолчанию, чтобы найти его имя и местоположение. **На вкладке Home (Начало) местоположение эскиза `~/+CSCOU+/nv-home.gif`. На вкладке Web Applications (Web-приложения) местоположение эскиза `~/+CSCOU+/nv-web-access.gif`.**
2. Импортируйте требуемое изображение в ASA в виде web-контента с названием, зафиксированным на первом шаге. **Например, если с вкладкой Web Applications (Web-приложения) требуется связать файл `disney.gif`, импортируйте его как `nv-web-access.gif`.** Рисунок 26: Импорт эскизов для вкладок приложений



[Пользовательские страницы справки для приложений](#)

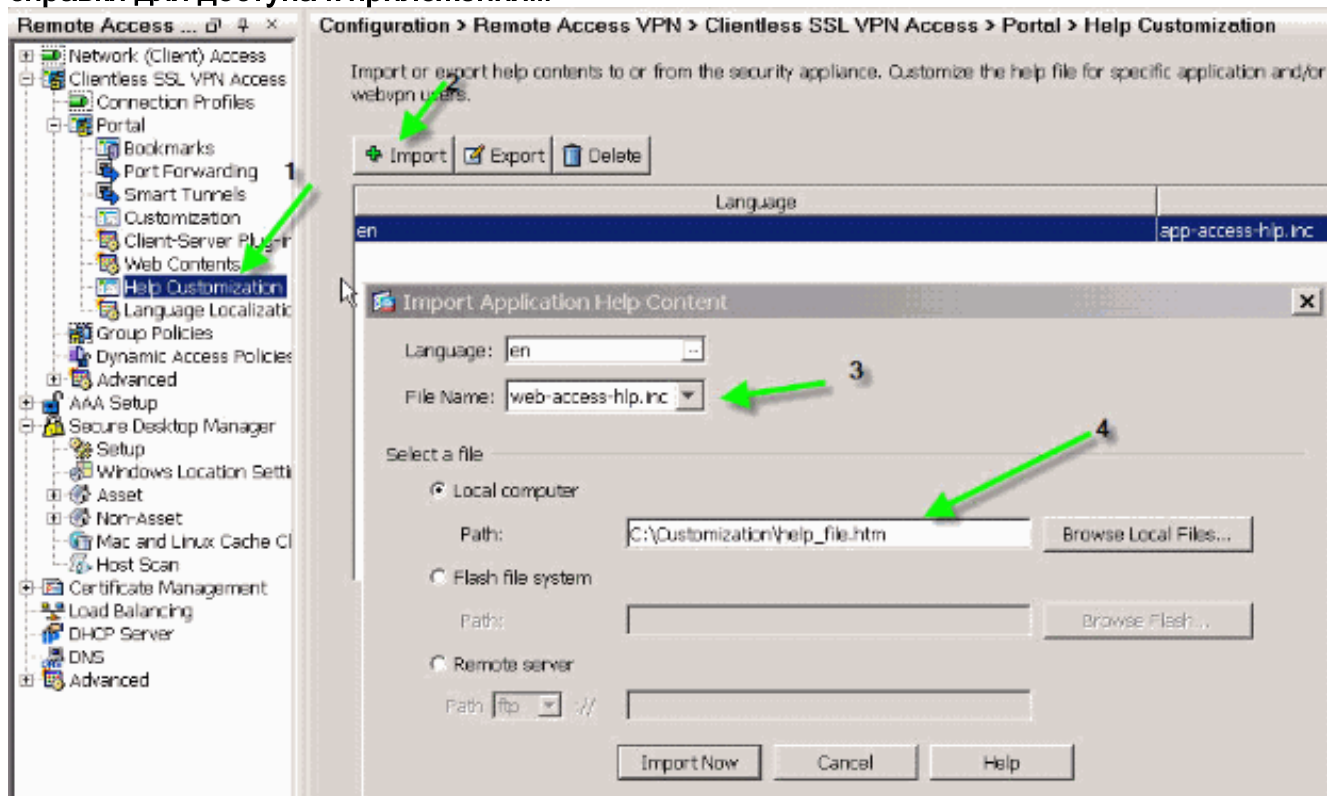
Компания Cisco поставляет файлы справки по умолчанию для использования в приложениях. Эти страницы можно заменить собственными пользовательскими HTML-страницами. [Например, на рис. 27 можно добавить к странице справки собственное изображение.](#)

Рисунок 27: Пользовательская страница справки



Для настройки файлов справки выполните следующие действия:

1. Выберите Portal > Help Customization (Портал > Пользовательская настройка справки) и щелкните Import (Импортировать).
2. Укажите язык в поле Language.
3. Выберите файл .inc. Например, для редактирования страницы справки, соответствующей вкладке доступа к web-приложениям, откройте файл web-access-hlp.inc.
4. Выберите пользовательский HTML-файл. Схема 28: Импорт пользовательских файлов справки для доступа к приложениям



[Проверка пользовательских настроек](#)

На этом этапе зайдите в устройство ASA по адресу: <https://asa.cisco.com/sslclient>. После успешной аутентификации появится web-портал с пользовательской настройкой.

[Пользовательская настройка страницы входа](#)

Это страница входа в систему по умолчанию:

Рис. 29: Страница входа по умолчанию

Login

Please enter your username and password.

USERNAME:

PASSWORD:

Это страница входа в систему с полной пользовательской настройкой:

Рисунок 30: Страница входа в систему с полной пользовательской настройкой



Welcome to SSL VPN Lab

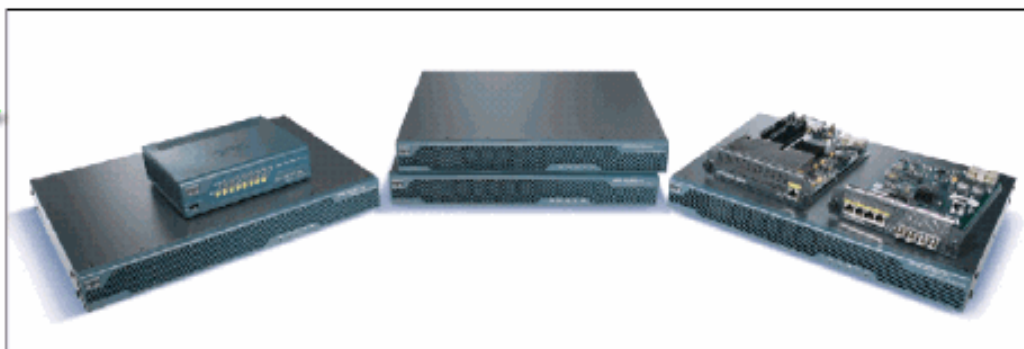


Please enter your username and password.

USERNAME:

PASSWORD:

Login



Copyright Cisco Systems, Inc. 2007

Новая страница входа в систему содержит пользовательский логотип, заголовок и изображение с диалоговым окном для ввода имени учетной записи и пароля. Страница входа в систему является полностью настраиваемой: можно создать любую HTML-страницу и вставить в требуемом месте диалоговое окно для ввода имени учетной записи/пароля.

Примечание: В то время как вся страница входа настраивается, определенный вход в систему/диалоговое окно пароля, что загрузки ASA конечному пользователю не полностью настраиваемы.

Механизм полной настраиваемости позволяет задать HTML-код собственного экрана входа в систему и затем вставить HTML-код Cisco, вызывающий функции устройства защиты для создания формы входа в систему и раскрывающегося списка выбора языка.

В последующих разделах этого документа описаны изменения, необходимые в коде HTML, и задачи, которые нужно выполнить для настройки устройства защиты на использование нового кода.

[Подготовка собственного HTML-файла](#)

Этот HTML-файл получен в редакторе Microsoft FrontPage. Он содержит заголовок,

пользовательский логотип, изображение и нижний колонтитул.

```
<head>
<meta http-equiv="Content-Type" content="text/html;
charset=windows-1252">
<title>SSL VPN Class</title>
<base target="_self">
</head>

<p align="center">
<font face="Snap ITC" size="6" color="#FF00FF"></font>
<font face="Snap ITC" color="#FF00FF" size="7"> &nbsp;</font>
<i><b>
<font color="#FF0000" size="7" face="Sylfaen">Welcome to SSL VPN
Lab</font>
</b></i></p>

<p>&nbsp;</p>
<p>&nbsp;</p>
<p>&nbsp;</p>
<p>&nbsp;</p>
<p>&nbsp;</p>
<p>&nbsp;</p>

<table><tr><td width="251"></td>
<td width="1"></td><td align=right valign=right width="800">

</td></tr>
</table>

<div id="footerText" class="yui-u">
<div><p align="center"><font size="1">CopyRight Cisco Systems,
Inc. 2007</font></div>
</div>

</body>
```

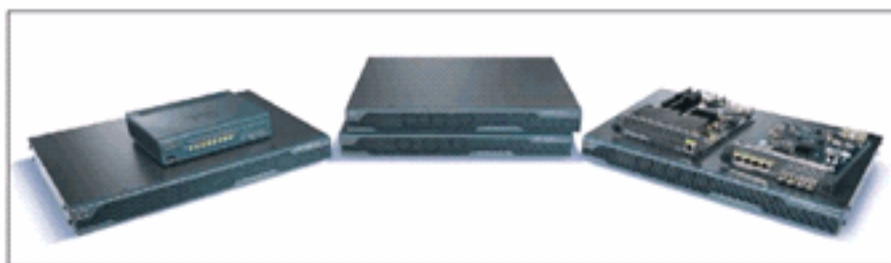
Примечание: Образы 5550.gif и asa.gif сохранены в каталоге login_files. Пробелы обязательны. На последующих шагах они заменяются диалоговым окном имени учетной записи/пароля.

[В этот момент страница имеет вид, показанный на рис. 31.](#) Следует обратить внимание на пустое пространство, оставленное для диалогового окна на последующих шагах.

Рисунок 31: Начальная web-страница



Welcome to SSL VPN Lab



Copyright Cisco Systems, Inc. 2007

Изменение ссылок на место хранения изображений

Для всех изображений замените путь ключевым словом `/+CSCOU+`, которое соответствует внутреннему каталогу в устройстве ASA. При загрузке изображения в устройство ASA оно сохраняется во внутреннем каталоге `/+CSCOU+` файловой системы ASA. Позднее, при загрузке этого измененного HTML-кода, устройство ASA надлежащим образом загружает файлы изображений.

Рис. 32: Измененный HTML-код

```

<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>SSL VPN Class</title>
<base target="_self">
</head>

<p align="center">
<font face="Snap ITC" size="6" color="#FF00FF"></font>
<font face="Snap ITC" color="#FF00FF" size="7">&nbsp;</font>
<i><b>
<font color="#FF0000" size="7" face="Sylfaen">Welcome to SSL VPN Lab</font>
</b></i></p>

<p>&nbsp;</p>
<p>&nbsp;</p>
<p>&nbsp;</p>
<p>&nbsp;</p>
<p>&nbsp;</p>
<p>&nbsp;</p>
<p>&nbsp;</p>
<p>&nbsp;</p>

<table>
<tr><td width="251"></td>
<td width="1"></td>
<td align="right" valign="right" width="800">

</td></tr>
</table>

<div id="footerText" class="yui-u">
<div><p align="center"><font size="1">CopyRight Cisco Systems, Inc. 2007</font></p></div>
</div>

</body>

```

Replaced "login_files" with "+CSCOU/"

Примечание: В первой ссылке login_files/5550.gif заменен / +CSCOU +/5550.gif.

Переименование HTML-файла

На следующем шаге этот файл login.html переименоывается в login.inc.

Расширение .inc необходимо для того, чтобы устройство ASA распознало этот файл как файл особого типа и включило необходимый сценарий JavaScript для поддержки диалогового окна имени учетной записи/пароля.

Добавление кода в файл login.inc

Этот HTML-код должен быть добавлен в том месте, где должно отображаться диалоговое окно ввода имени учетной записи и пароля.

```

<body onload="cscs_ShowLoginForm('lform'); cscs_ShowLanguageSelector('selector')"
bgcolor="white"> <table> <tr><td colspan=3 height=20 align=right> <div id="selector"
style="width: 300px"></div> </td></tr> <tr> <td align=middle valign=middle> <div id=lform>
Loading... </div> </td> </tr> </table>

```

Примечание: Первые две функции cscs_ShowLoginForm (lform) и cscs_ShowLanguageSelector (селектор) являются двумя функциями сценария Java, определение которых импортировано ASA, когда это представляет .inc файл. В этом коде просто вызывается функция для отображения диалогового окна имени учетной записи/пароля со списком для выбора языка.

Примечание: Диалоговое окно представлено как элемент таблицы. На своей HTML-

странице его можно расположить в окружении других изображений или текста или выровнять требуемым образом.

В этом сценарии диалоговое окно имени учетной записи/пароля появляется выше изображения asa.gif посередине. При вставке кода окончательная HTML-страница будет иметь следующий вид:

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-
1252">
<title>SSL VPN Class</title>
<base target="_self">
</head>

<p align="center">
<font face="Snap ITC" size="6" color="#FF00FF"></font>
<font face="Snap ITC" color="#FF00FF" size="7">&nbsp;&nbsp;&nbsp;</font>
<i><b>
<font color="#FF0000" size="7" face="Sylfaen">Welcome to SSL VPN
Lab</font>
</b></i></p>

<body onload="cscs_ShowLoginForm('lform');
cscs_ShowLanguageSelector('selector')" bgcolor="white">

<table> <tr><td colspan=3 height=20 align=right>

<div id="selector" style="width: 300px"></div> </td></tr>

<tr> <td align=middle valign=middle>

<div id=lform>

Loading...

</div> </td> </tr> </table>

<table>
<tr><td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">|

</td></tr>
</table>

<div id="footerText" class="yui-u">
<div><p align="center"><font size="1">CopyRight Cisco Systems, Inc.
2007</font></p></div>
</div>

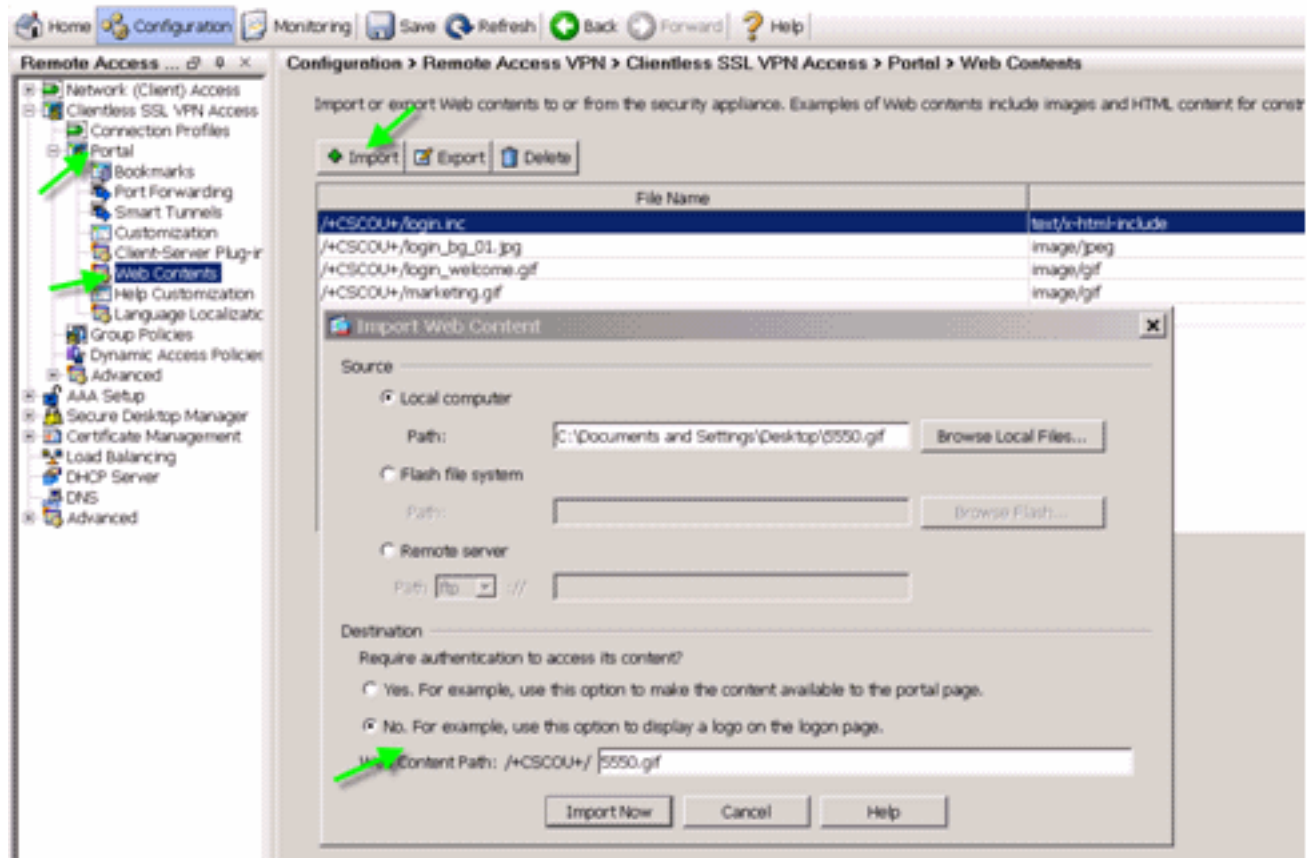
</body>
```

[Загрузка файла login.inc и файлов изображений в ASA в виде web-контента](#)

Следующий шаг – загрузка итогового файла login.inc и загрузочных модулей в устройство ASA в виде web-контента. Необходимо убедиться в том, что выбран нижний параметр для

сохранения файлов в каталоге /+CSCOU+/.

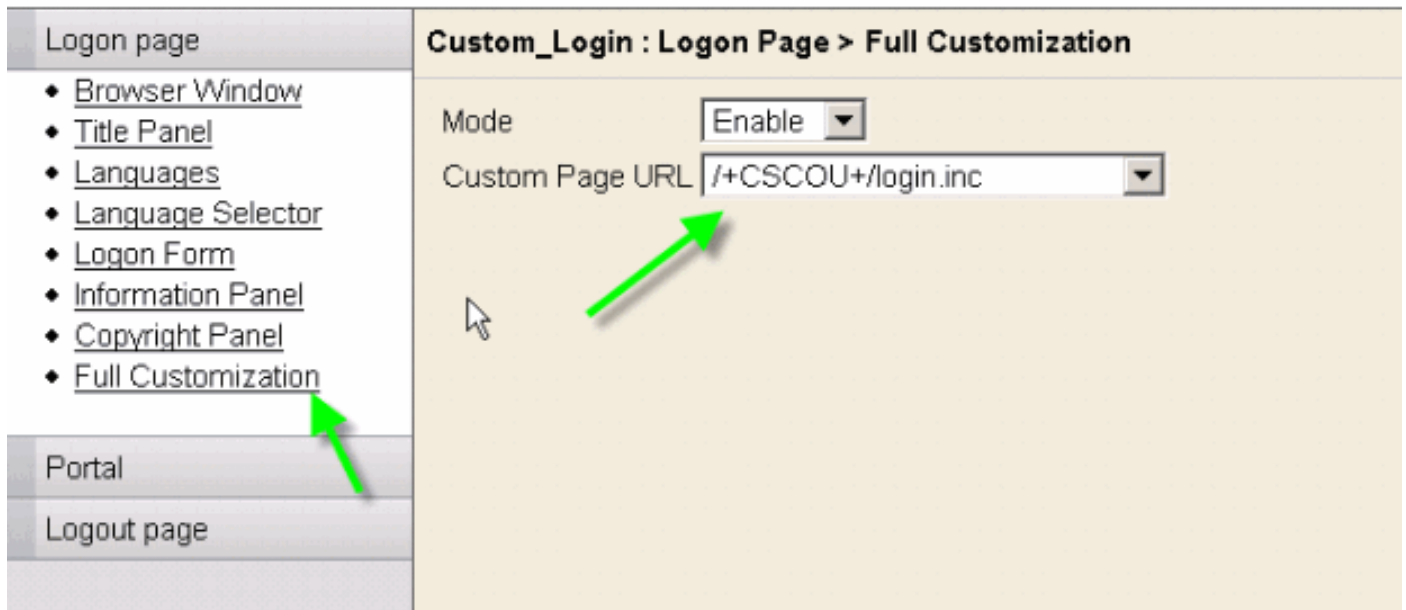
Рис. 33: Импорт файлов изображений в устройство ASA в качестве web-контента



[Выбор файла login.inc для полной пользовательской настройки](#)

Наконец, в редакторе пользовательской настройки выберите вкладку Full Customization (Полная настройка) и укажите ссылку на загруженный файл login.inc. При подключении конечного пользователя из профиля подключения, связанного с этой настройкой, например sslclient, пользователю представляется страница входа в систему с полной настройкой.

Рисунок 34: Связывание файла login.inc для полной пользовательской настройки



[Проверка полной пользовательской настройки](#)

При подключении к ASA по адресу <https://asa.cisco.com/sslclient> должна появиться страница входа в систему с полной пользовательской настройкой.

Рисунок 35: Окончательный вид страницы входа в систему с полной пользовательской настройкой



Welcome to SSL VPN Lab

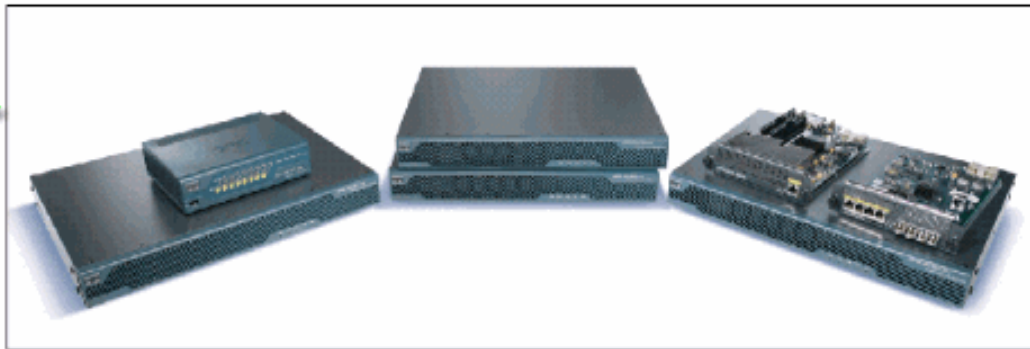


Please enter your username and password.

USERNAME:

PASSWORD:

Login



Copyright Cisco Systems, Inc. 2007

Поддержка интерфейса командной строки

Как пояснялось выше, редактирование всех настроек выполняется в инструменте ASDM. Тем не менее, для удаления пользовательских настроек и другого контента WebVPN можно также использовать следующие команды интерфейса командной строки:

revert webvpn:

all	Revert all webvpn related data
customization	Revert customization file
plug-in	Revert plug-in options
translation-table	Revert translation table
url-list	Revert a list of URLs for use with WebVPN
webcontent	Revert webcontent

Пример:

- Для удаления пользовательской настройки выполните в интерфейсе командной строки команду `revert webvpn customization Custom_Marketing`.
- Для удаления файла логотипа выполните команду `revert webvpn webcontent /+CSCOU+/marketing.gif`.

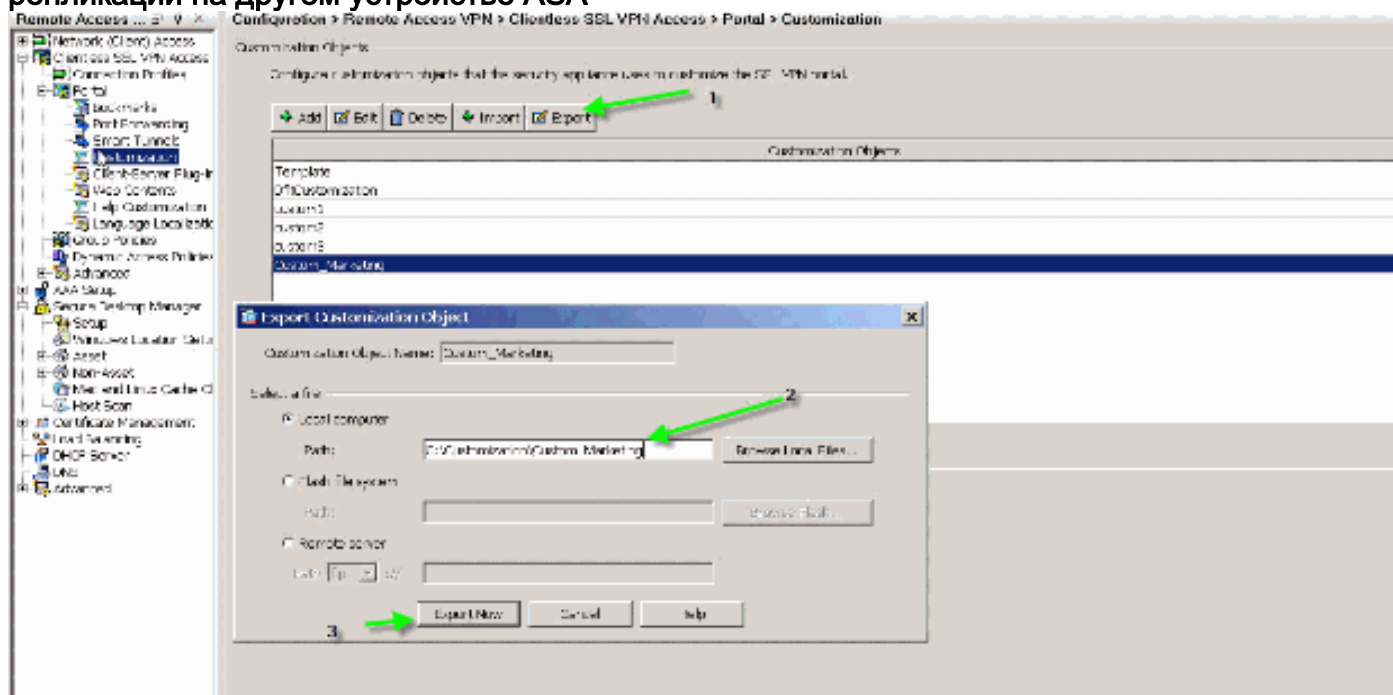
- Для удаления закладок выполните команду `revert webvpn url-list Marketing_URL_List`.
- Для удаления всех пользовательских настроек, web-контента, подключаемых модулей и закладок выполните команду `revert webvpn all`.

Примечание: Так как настройки решения WebVPN не сохранены в рабочей конфигурации, типичном `write erase`, последовательность повторной загрузки не стирает кастомизации или webcontents от ASA. Необходимо в явном виде выполнить команды `revert webvpn` или вручную удалить пользовательские настройки из ASDM.

Резервное копирование пользовательских настроек

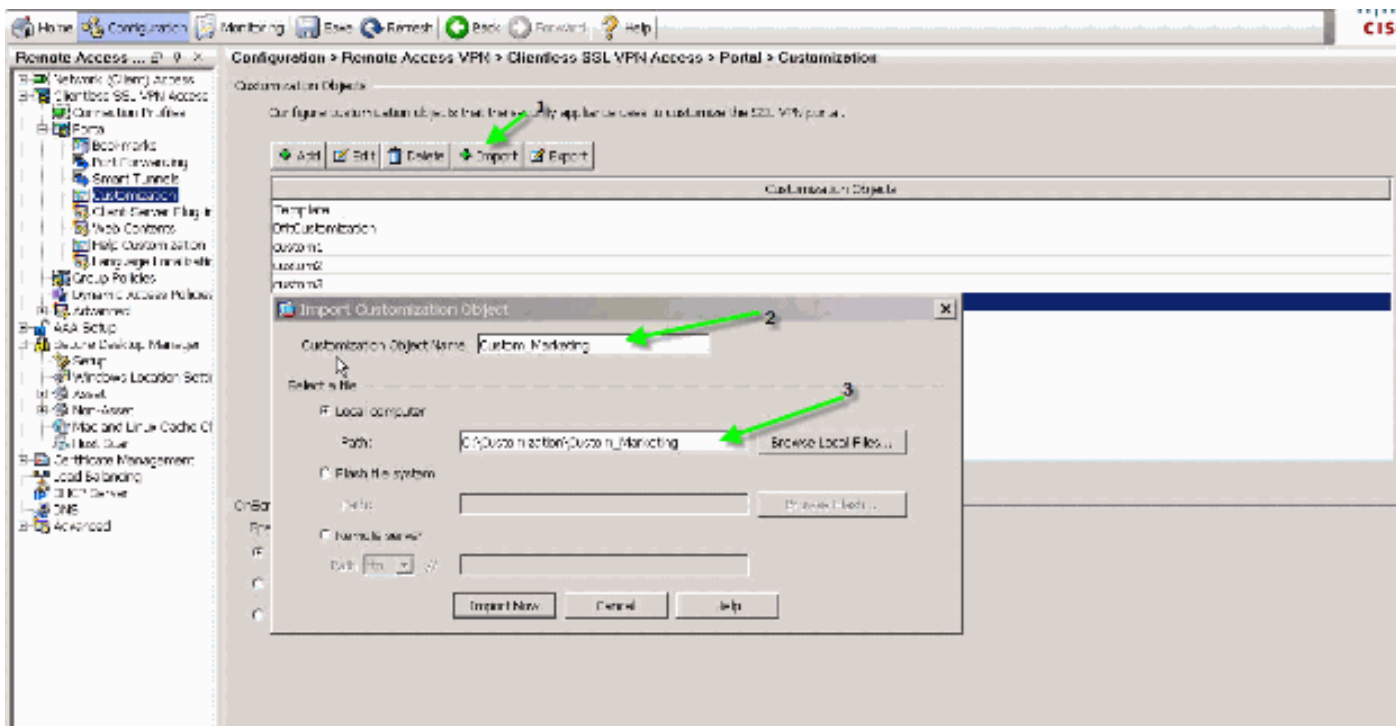
В отличие от других команд интерфейса командной строки, настройки не сохраняются в рабочей конфигурации. Необходимо в явном виде экспортировать настройки и сохранять их в формате XML на компьютере-хосте.

Рисунок 36: Экспорт пользовательских настроек для резервного копирования или репликации на другом устройстве ASA



Для восстановления импортируйте пользовательские настройки с файлом XML, полученным на предыдущем шаге.

Рисунок 37: Импорт пользовательских настроек из предварительно экспортированного файла XML



Примечание: В дополнение к экспортированию/импортированию кастомизации также необходимо вручную резервировать/восстанавливать webcontent, который включает графические файлы, справочные файлы и эскизы изображения, явно. Иначе настройки не будут полностью работоспособны.

Заключение

Развитые возможности настройки, представленные в версии ASA 8.0, позволяют создавать эстетичные страницы web-портала. Можно реализовать виртуализацию путем создания различным образом настроенных web-порталов для различных групп. Кроме того, страница входа в систему допускает полную пользовательскую настройку для приведения к виду обычных web-порталов интрасети в интересах унификации пользовательского интерфейса.

Устранение неполадок

При разрешении пользовательской настройки WebVPN может появиться следующее сообщение об ошибке:

```
%ERROR: cisco_config.lua:36: cisco_config.lua:552: copying
'disk0:/cisco_config/locale/ja/LC_MESSAGES/PortForwarder.po' to a temporary ramfs file
failed
```

```
%ERROR: cisco_config.lua:36: cisco_config.lua:552: copying
'disk0:/cisco_config/locale/ja/LC_MESSAGES/webvpn.po' to a temporary ramfs file failed
```

```
%ERROR: cisco_config.lua:36: cisco_config.lua:552: copying
'disk0:/cisco_config/locale/fr/LC_MESSAGES/customization.po' to a temporary ramfs file
failed.
```

Для устранения этой проблемы выполните команду `revert webvpn all` и перезагрузите устройство ASA.

Дополнительные сведения

- [Страница поддержки устройств адаптивной безопасности Cisco ASA серии 5500](#)
- [Настройка страниц бесклиентской сети VPN на основе SSL](#)
- [ASA 8. 0: Изменение логотипа WebVPN](#)
- [Cisco Systems – техническая поддержка и документация](#)