Содержание

Введение

Этот документ описывает, как генерировать Запрос подписи сертификата (CSR) и установить получающийся сертификат идентификации для использования с Менеджером Шасси для Огневая мощь расширяемая Операционная система (FXOS) на Огневой мощи 4100 и 9300 устройств серии.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Настройка FXOS из командной строки
- Использование CSR
- Понятия Инфраструктуры с закрытым ключом (PKI)

Используемые компоненты

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

- Огневая мощь 4100 и 9300 оборудования серии
- Версии 1.1 и 2.0 FXOS

Общие сведения

После начальной конфигурации самоподписанный сертификат SSL генерируется для использования с Менеджером Шасси web - приложение. Так как тот сертификат

самоподписан, ему не будут автоматически доверять клиентские браузеры. Первоначально, что новый клиентский браузер обращается к Менеджеру Шасси веб-интерфейс впервые, браузер бросит SSL, предупреждающий подобный Вашему соединению, не является частным и потребует, чтобы пользователь принял сертификат прежде, чем обратиться к Менеджеру Шасси. Этот процесс позволит сертификату, подписанному доверенным центром сертификации быть установленным, который может позволить клиентскому браузеру доверять соединению и переводить веб-интерфейс в рабочее состояние без предупреждений.

Данные для документа были получены в специально созданных лабораторных условиях. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если используемая сеть является действующей, убедитесь в понимании возможного влияния любой из применяемых команд.

Настройка

> **Примечание:** В настоящее время нет никакого способа генерировать CSR в Графическом интерфейсе пользователя менеджера Шасси. Это должно быть сделанный через командную строку.

Генерируйте запрос подписи сертификата

Выполните эти шаги для получения сертификата, который содержит IP-адрес или Полное доменное имя (FQDN) устройства (который позволяет клиентскому браузеру определять сервер должным образом):

- Создайте брелок и выберите размер модуля секретного ключа

  Примечание: Название брелока может быть любым вводом. В примерах используется firepower_cert

```
fp4120# scope securityfp4120 /security # create keyring firepower_certfp4120 /security/keyring*
# set modulus <size>fp4120 /security/keyring* # commit-buffer
```

- Настройте поля CSR. CSR может генерироваться только с основными параметрами как subject-name. Это вызывает для пароля запроса сертификата также.

```
fp4120 /security/keyring # create certreq subject-name fp4120.test.local
Certificate request password:
Confirm certificate request password:
```

- CSR может также генерироваться с большими расширенными настройками, которые позволяют информации как локаль и организация быть встроенной в сертификат.

```
fp4120 /security/keyring # create certreq fp4120 /security/keyring/certreq* # set country
USfp4120 /security/keyring/certreq* # set state Californiafp4120 /security/keyring/certreq* #
set locality "San Jose"fp4120 /security/keyring/certreq* # set org-name "Cisco Systems"fp4120
/security/keyring/certreq* # set org-unit-name TACfp4120 /security/keyring/certreq* # set
subject-name fp4120.test.localfp4120 /security/keyring/certreq* # commit-buffer
```

- Экспортируйте CSR для обеспечения центру сертификации. Скопируйте выходные данные начиная с (и включая) "-----ЗАПРОС СЕРТИФИКАТА BEGIN-----" заканчивающийся (и включая) "-----КОНЕЧНЫЙ ЗАПРОС СЕРТИФИКАТА-----".

```
fp4120 /security/keyring/certreq # show certreq Certificate request subject name:
```

```
fp4120.test.localCertificate request ip address: 0.0.0.0Certificate request FI A ip address:
0.0.0.0Certificate request FI B ip address: 0.0.0.0Certificate request e-mail name:Certificate
request ipv6 address: ::Certificate request FI A ipv6 address: ::Certificate request FI B ipv6
address: ::Certificate request country name: USState, province or county (full name):
CaliforniaLocality name (eg, city): San JoseOrganisation name (eg, company): Cisco
SystemsOrganisational Unit Name (eg, section): TACDNS name (subject alternative name):Request:--
---BEGIN CERTIFICATE REQUEST-----
MIIC6zCCAdMCAQAwdzELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExETAPBgNVBAcMCFNhbiBKb3NlMRYwFAYD
VQQKDA1DaXNjbyBTeXN0ZW1zMQwwCgYDVQQLDANUQUMxGjAYBgNVBAMMEWZwNDEyMC50ZXN0LmxvY2FsMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0ON5gagkfZ2fi4JVEANG+7YGgcHbnUt7LpVyMChnKOPJjBwkUMNQA1mQsRQDcbJ232/
sK0fMSnyqOL8JzC7itxeVEZRyz7/ax7WGNveg/XP+zd03nt4GXM63FsrPcPmA7EwgqDSLoShtBEV10hhf4+Nw4pKCZ+eSSkS
JkTB1ZHaKV9bttYg3kf/UEUUgk/EyrVq3B+u2DsooPVq76mTm8BwYMqHbJEv4PmuRjWE88yEvVwH7JTEij9OvxbatjDjVSJH
ZBURtCanvyBvGuLP/Q/Nmv3Lo3G9ITbLL5gIYZVatTxp6HTUezH2MIIzOavU6d1tB9rnyxgGth5dPV0dhQIDAQABoC8wLQYJ
KoZIhvcNAQkOMSAwHjAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDANBgkqhkiG9w0BAQsFAAOCAQEAZUfCbwx9vt5a
VDcL+tATu5xFE3LA310ck6GjlNv6W/6rjBNLxusYi1rZZcW+CgnvNs4ArqYGyNVBySOavJO/VvQ1KfyxxJ1OIkyx3RzEjgK0
zzyoyrG+EZXC5ShiraS8HuWvE2wFM2wwWNtHWtvcQy55+/hDPD2Bv8pQOC2Zng3IkLfG1dxWf1xAxLzf5J+AuIQ0CM5HzM9Z
m8zREoWT+xHtLSqAqg/aCuomN9/vEwyUOYfoJMvAqC6AZyUnMfUfCoyuLpLwgkxB0gyaRdnea5RhiGjYQ2lDXYDjEXp7rCx9
+6bvDl1n70JCegHdCWtP75SaNyaBEPkO0365rTckbw==-----END CERTIFICATE REQUEST-----
```

Импортируйте цепочку сертификатов Центра сертификации

Примечание: Все сертификаты должны быть в формате Base64, который будет импортирован в FXOS. Если сертификат или цепочка, полученная от Центра сертификации, находятся в другом формате, необходимо сначала преобразовать его с программным средством SSL, таким как OpenSSL.

- Создайте новую точку доверия для удержания цепочки сертификатов

  Примечание: Точка доверия name name может быть любым вводом. В примерах используется firepower_chain.

```
fp4120 /security/keyring/certreq # exitfp4120 /security/keyring # exitfp4120 /security # create
trustpoint firepower_chainfp4120 /security/trustpoint* # set certchainEnter lines one at a time.
Enter ENDOFBUF to finish. Press ^C to abort.Trustpoint Certificate Chain:>-----BEGIN
CERTIFICATE-----
>MIICDTCCAbOgAwIBAgIQYIutxPDPw6BOp3uKNgJHZDAKBggqhkjOPQQDAjBTMRUw
>EwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>MB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTUwNzI4MTc1NjU2
>WhcNMjAwNzI4MTgwNjU2WjBTMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJ
>kiaJk/IsZAEZFghuYWF1c3RpbjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4t
>UEMtQ0EwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASvEA27V1Enq1gMtLkvJ6rx
>GXRpXWIEyuiBM4eQRoqZKnkeJUkm1xmqlubaDHPJ5TMGfJQYszLBRJPq+mdrKcDl
>o2kwZzATBgkrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0T
>AQH/BAUwAwEB/zAdBgNVHQ4EFgQUyInbDHPrFwEEBcbxGSgQW7pOVIkwEAYJKwYB
>BAGCNxUBBAMCAQAwCgYIKoZIzj0EAwIDSAAwRQIhAP++QJTUmniB/AxPDDN63Lqy
>18odMDoFTkG4p3Tb/2yMAiAtMYhlsv1gCxsQVOw0xZVRugSdoOak6n7wCjTFX9jr
>RA==
>-----END CERTIFICATE----->ENDOFBUF fp4120 /security/trustpoint* # commit-buffer
```

Примечание: Для Центра сертификации, который использует промежуточные сертификаты, должны быть объединены корневые и промежуточные сертификаты. В текстовом файле вставьте корневой сертификат наверху, придерживавшийся каждым промежуточным сертификатом в цепочке (включая весь СЕРТИФИКАТ BEGIN и КОНЕЧНЫЕ флаги СЕРТИФИКАТА). Затем вставка, что весь файл перед формированием рисунка ENDOFBUF.

Импортируйте Сертификат идентификации со знаком для сервера

- Привяжите точку доверия, созданную в предыдущем шаге с брелоком, который был создан для CSR.

```
fp4120 /security/trustpoint # exitfp4120 /security # scope keyring firepower_certfp4120
/security/keyring # set trustpoint firepower_chain
```

- Вставьте содержание сертификата идентификации, предоставленного Центром сертификации

```
fp4120 /security/keyring* # set cert Enter lines one at a time. Enter ENDOFBUF to finish. Press
^C to abort.Keyring certificate:>-----BEGIN CERTIFICATE-----
>MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkjOPQQDAjBT
>MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
>bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
>OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs
>aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoTDUNpc2NvIFN5c3Rl
>bXMxDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
>MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
>BwdudS3sulXIwKGco48mMHCRQw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
>RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
>ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
>yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
>/cujcb0hNssvmAhhlVq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2Hl09XR2FAgMB
>AAGjggJYMIICVDAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
>FgQU/1WpstiEYExs8DlZWcuHZwPtu5QwHwYDVR0jBBgwFoAUyInbDHPrFwEEBcbx
>GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
>dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
>YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
>b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlz
>dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHMBggrBgEF
>BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
>QVVTVElOLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
>Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
>P2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0
>aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBlAGIAUwBlAHIAdgBlAHIwDgYDVR0P
>AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
>IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
>sgoIK60akbjotOTvUdUd9b6K1Uw=
>-----END CERTIFICATE----->ENDOFBUFfp4120 /security/keyring* # commit-buffer
```

Настройте Менеджера Шасси для использования нового сертификата

Сертификат был теперь установлен, но веб-сервис еще не настроен для использования его.

```
fp4120 /security/keyring # exitfp4120 /security # exitfp4120# scope systemfp4120 /system # scope
servicesfp4120 /system/services # set https keyring firepower_certWarning: When committed, this
closes all the web sessions.fp4120 /system/services* # commit-buffer
```

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

- показать https? Выходные данные отображают брелок, привязанный к серверу HTTPS. Это должно отразить название, созданное в шагах выше. Это, если все еще показывает по умолчанию тогда, он не был обновлен для использования нового сертификата.

```
fp4120 /system/services # show https Name: https    Admin State: Enabled    Port: 443
Operational port: 443    Key Ring: firepower_cert    Cipher suite mode: Medium Strength
```

Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL

- **показать брелок <keyring_name> подробность**? Выходные данные отображают содержание сертификата, который импортирован, и покажите, допустимо ли это или нет.

```
fp4120 /security #  scope securityfp4120 /security #  show keyring firepower_cert detailKeyring
firepower_cert:    RSA key modulus: Mod2048    Trustpoint CA: firepower_chain    Certificate
status: Valid    Certificate:    Data:        Version: 3 (0x2)        Serial Number:
45:00:00:00:0a:de:86:55:16:82:24:f3:be:00:00:00:00:00:0a    Signature Algorithm: ecdsa-with-
SHA256        Issuer: DC=local, DC=naaustin, CN=naaustin-NAAUSTIN-PC-CA        Validity
Not Before: Apr 28 13:09:54 2016 GMT            Not After : Apr 28 13:09:54 2018 GMT
Subject: C=US, ST=California, L=San Jose, O=Cisco Systems, OU=TAC, CN=fp4120.test.local
Subject Public Key Info:            Public Key Algorithm: rsaEncryption                Public-
Key: (2048 bit)                Modulus:
00:b3:43:8d:e6:06:a0:91:f6:76:7e:2e:09:54:40:
0d:1b:ee:d8:1a:07:07:6e:75:2d:ec:ba:55:c8:c0:
a1:9c:a3:8f:26:30:70:91:43:0d:40:0d:66:42:c4:
50:0d:c6:c9:db:7d:bf:b0:ad:1f:31:29:f2:a8:e2:
fc:27:30:bb:8a:dc:5e:54:46:51:cb:3e:ff:6b:1e:
d6:18:db:de:83:f5:cf:fb:37:74:de:7b:78:19:73:
3a:dc:5b:2b:3d:c3:e6:03:b1:30:82:a0:d2:2e:84:
a1:b4:11:15:d7:48:61:7f:8f:8d:c3:8a:4a:09:9f:
9e:49:29:12:26:44:c1:d5:91:da:29:5f:5b:b6:d6:
20:de:47:ff:50:45:14:82:4f:c4:ca:b5:6a:dc:1f:
ae:d8:3b:28:a0:f5:6a:ef:a9:93:9b:c0:70:60:ca:
87:6c:91:2f:e0:f9:ae:46:35:84:f3:cc:84:bd:5c:
07:ec:94:c4:8a:3f:4e:bf:16:da:b6:30:e3:55:22:
47:64:15:11:b4:26:a7:bf:20:6f:1a:e2:cf:fd:0f:
cd:9a:fd:cb:a3:71:bd:21:36:cb:2f:98:08:61:95:
5a:b5:3c:69:e8:74:d4:7b:31:f6:30:82:33:39:ab:
d4:e9:dd:6d:07:da:e7:cb:18:06:b6:1e:5d:3d:5d:                    1d:85                Exponent:
65537 (0x10001)        X509v3 extensions:            X509v3 Subject Alternative Name:
DNS:fp4120.test.local            X509v3 Subject Key Identifier:
FF:55:A9:B2:D8:84:60:4C:6C:F0:39:59:59:CB:87:67:03:ED:BB:94            X509v3 Authority Key
Identifier:                keyid:C8:89:DB:0C:73:EB:17:01:04:05:C6:F1:19:28:10:5B:BA:4E:54:89
X509v3 CRL Distribution Points:                Full Name:
URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=naaustin-
pc,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,DC=local?certifica
teRevocationList?base?objectClass=cRLDistributionPoint            Authority Information Access:
CA Issuers - URI:ldap:///CN=naaustin-NAAUSTIN-PC-
CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,DC=local?cACertifi
cate?base?objectClass=certificationAuthority            1.3.6.1.4.1.311.20.2:
...W.e.b.S.e.r.v.e.r            X509v3 Key Usage: critical                Digital Signature, Key
Encipherment            X509v3 Extended Key Usage:                TLS Web Server Authentication
Signature Algorithm: ecdsa-with-SHA256
30:45:02:20:57:b0:ec:d7:09:8a:b1:2d:15:1b:f2:c6:39:10:
e3:f7:55:a3:6a:08:e8:24:41:df:4f:16:41:b6:07:35:4b:bf:
02:21:00:ed:47:4e:6e:24:89:04:6f:cf:05:98:e6:b2:0a:08:
2b:ad:1a:91:b8:e8:b4:e4:ef:51:d5:1d:f5:be:8a:d5:4c-----BEGIN CERTIFICATE-----
MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkjOPQQDAjBTMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwx
GDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTERMA8GA1UEBxMIU2FuIEpv
c2UxFjAUBgNVBAoTDUNpc2NvIFN5c3RlbXMxDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tgaBwdudS3sulXIwKGco48mMHCRQw1ADWZC
xFANxsnbfb+wrR8xKfKo4vwnMLuK3F5URlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBgyodskS/g+a5GNYTzzIS9XAfslMSKP06/
Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a/cujcb0hNssvmAhhlVq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2Hl09XR2FAgMB
AAGjggJYMIICVDAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4EFgQU/1WpstiEYExs8DlZWcuHZwPtu5Qw
HwYDVR0jBBgwFoAUyInbDHPrFwEEBcbxGSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENO
PVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlz
dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHMBggrBgEFBQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKG
```

```
gaxsZGFwOi8vL0NOPW5hYXVzdGluLU5BQVVTVElOLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2FsP2NBQ2VydGlmaWNhdGU/YmFzZT9vYmpl
Y3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBlAGIAUwBlAHIAdgBlAHIwDgYDVR0P
AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUCIFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB
308WQbYHNUu/AiEA7UdObiSJBG/PBZjmsgoIK60akbjotOTvUdUd9b6K1Uw=-----END CERTIFICATE-----
Zeroized: No
```

- Перейдите к Менеджеру Шасси Огневой мощи путем ввода https://<FQDN_or_IP> / в строке адреса web-браузера и проверьте, что представлен новый надежный сертификат.

  % Warning: Браузеры также проверяют subject-name сертификата против ввода в строке адреса, поэтому если сертификат выполнен к полному доменному имени, это должно быть, обратился к тому пути в браузере. Если к этому обращаются через IP-адрес, другая ошибка SSL брошена (Недопустимое Общее имя), даже если используется надежный сертификат.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Доступ к CLI FXOS
- Cisco Systems – техническая поддержка и документация