Openconnect VPN

Nikos Mavrogiannopoulos
Security Technologies
Red Hat
February, 2016
• VPN story
• The server
• Future plans
VPN story
VPN story

- Task
  - Setup a VPN service to inter-connect router devices
VPN story
VPN story
VPN story
VPN story

• Requirements:
  – Simple setup for users
VPN story

• Requirements:
  − Standards based solution
VPN story

• Requirements:
  – The administrator should be able to view who is connected on every moment
VPN story

• Requirements:
  - The administrator should be able to disconnect and block access to users
VPN story

- Solution:
  - Based on OpenVPN and lots of custom scripts
VPN story

• Solution:
  − Based on OpenVPN and lots of custom scripts
VPN story

• Requirements:
  - Simple setup for users [X]
  - Standards based solution
  - The administrator should be able to view who is connected on every moment
  - The administrator should be able to disconnect and block access to users

Involved configuration files for client setup, TCP/UDP had to be selected by user
VPN story

- Requirements:
  - Simple setup for users
  - Standards based solution
  - The administrator should be able to view who is connected on every moment
  - The administrator should be able to disconnect and block access to users

Was using TLS for key exchange; everything else was custom
**VPN story**

- Requirements:
  - Simple setup for users
  - Standards based solution
  - The administrator should be able to view who is connected on every moment
  - The administrator should be able to disconnect and block access to users
VPN story

• Requirements:
  - Simple setup for users
  - Standards based solution
  - The administrator should be able to view who is connected on every moment
  - The administrator should be able to disconnect and block access to users

No support
VPN story

• AnyConnect VPN

---

**DTLS and Cisco AnyConnect compatibility.**

[David Woodhouse](mailto:dwmw2@infradead.org)

to Nikos

Hi,

I am the author of the OpenConnect VPN client for Cisco AnyConnect ([http://www.infradead.org/openconnect.html](http://www.infradead.org/openconnect.html)).

At the time I wrote OpenConnect, GnuTLS didn’t have DTLS support so I was forced to use OpenSSL. I note with interest that GnuTLS *does* have DTLS support now, so I’d like to switch over to using GnuTLS, at least optionally. Thanks for working on DTLS in GnuTLS!

I just have one slight problem — Cisco used a pre-standardisation version of the DTLS protocol with a few differences. OpenSSL continues to support this as ‘DTLS1_BAD_VER’. You probably know more about the details than I do… the ChangeCipherSpec message contains a sequence number (and is hence 3 bytes instead of 1), and the Finished MAC *does* include the initial ClientHello and HelloVerifyRequest.

Would you be willing to take patches to implement that same compatibility in GnuTLS?

There’s more background in [http://rt.openssl.org/Ticket/Display.html?id=1751&user=guest&pass=guest](http://rt.openssl.org/Ticket/Display.html?id=1751&user=guest&pass=guest)
VPN story

• CISCO AnyConnect VPN
  - A proprietary VPN implementation based on standard protocols
  - A VPN channel established over an HTTPS session (TLS 1.x)
  - Supports dual TCP/UDP; UDP via a pre-draft DTLS version
  - Open-source compatible client → openconnect

• Implements a compatible protocol we call “Openconnect protocol”
VPN story

• CISCO AnyConnect VPN
  - A proprietary VPN implementation based on standard protocols
  - A VPN channel established over an HTTPS session (TLS 1.x)
  - Supports dual TCP/UDP; UDP via a pre-draft DTLS version
  - Open-source compatible client → openconnect

  • Implements a compatible protocol we call “Openconnect”
• OpenConnect doesn't need any user configuration

# openconnect server.example.com:443
POST https://server.example.com/
Attempting to connect to server 127.0.0.1:443
SSL negotiation with server.example.com
Connected to HTTPS on server.example.com
XML POST enabled
Please enter your username
Username:test
POST https://server.example.com/auth
Please enter your password.
Password:
POST https://server.example.com/auth
Got CONNECT response: HTTP/1.1 200 CONNECTED
CSTP connected. DPD 90, Keepalive 32400
Connected tun0 as 192.168.1.191, using SSL
• OpenConnect doesn't need any user configuration

# openconnect server.example.com:443
POST https://server.example.com/
Attempting to connect to server 127.0.0.1:443
SSL negotiation with server.example.com
Connected to HTTPS on server.example.com
XML POST enabled
Please enter your username
Username: test
POST https://server.example.com/auth
Please enter your password.
Password:
POST https://server.example.com/auth
Got CONNECT response: HTTP/1.1 200 CONNECTED
CSTP connected. DPD 90, Keepalive 32400
Connected tun0 as 192.168.1.191, using SSL
Established DTLS connection (using GnuTLS). Cipher
RSA-(AES-128-GCM).
VPN story

• Requirements:
  – Simple setup for users
  – Standards-based solution
  – The administrator should be able to view who is connected on every moment
  – The administrator should be able to disconnect and block access to users
VPN story

• Requirements:
  – Simple setup for users
  – Standards-based solution
  – The administrator should be able to view who is connected on every moment
  – The administrator should be able to disconnect and block access to users
  – The server should isolate users between them
  – The server should operate under the least possible privilege
The server
The server

• Openconnect server: started in 2013

• Today the server interoperates with both openconnect and Anyconnect clients
  – Is available for Linux and *BSD systems
The server

• Features:
  - Supports for password (file, PAM, radius), certificate or Kerberos authentication
  - Supports setting resource limits per client or groups of clients (e.g., cgroups, bandwidth)
  - Processing scales with the number of CPUs
  - Supports LZS, LZ4 compression
  - Supports TLS 1.2, DTLS 1.2 and AES-GCM
  - Supports online user management
The server

• Features:
  – Privilege separation between main server and worker processes
  – Isolation of worker processes (using seccomp)
  – Isolated software security module handles PAM/radius and keys
The server

• Features:
  − Privilege separation between main server and worker processes
  − Isolation of worker processes (using seccomp)
  − Isolated software security module handles PAM/radius and keys

User isolation + Least privilege
The server

• occtl: Control tool to administer the server and view clients
The server

nmavrogi@dhcp-2-127:$ sudo ./occtl
OpenConnect server control (occtl) version 0.9.0
Copyright (C) 2014 Red Hat and others.
ocserv comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to redistribute it under the conditions of the
GNU General Public License version 2.

For help type ? or 'help'
======================================================================

> help
Available Commands
  disconnect user [NAME]  Disconnect the specified user
  disconnect id [ID]     Disconnect the specified ID
  reload                 Reloads the server configuration
  show status           Prints the status of the server
  show users            Prints the connected users
  show user [NAME]      Prints information on the specified user
  show id [ID]          Prints information on the specified ID
  stop now              Terminates the server
  reset                 Resets the screen and terminal
  help or ?             Prints this help
  exit                  Exits this application

>
The server

[root@devconf ~]# occtl
OpenConnect server control (occtl) version 0.10.8
Copyright (C) 2014 Red Hat and others.
ocserv comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to redistribute it under the conditions of the
GNU General Public License version 2.

For help type ? or 'help'
=====================================================================
> show users
    id      user   group  ip        vpn-ip device since  dtls-cipher   status
  10261   vpntest2 vpntest2 213.175.37.10 19.64.1.255  vpns1      44s  (AES-128-GCM) connected
  10257   vpntest1 vpntest1 213.175.37.10 19.64.1.100  vpns0      53s  (AES-128-GCM) connected
>
The server

[root@devconf ~]# ocserv
OpenConnect server control (ocserv) version 0.10.8
Copyright (C) 2014 Red Hat and others.
ocserv comes with ABSOLUTELY NO WARRANTY. This is free software, and
you are welcome to redistribute it under the conditions of the
GNU General Public License version 2.

For help type ? or 'help'

> show users

  id  user    group    ip     vpn-ip device since  dtls-cipher status
  10261  vpntest2 vpntest2 213.175.37.10 19.64.1.255 vpns1  44s   (AES-128-GCM) connected
  10257  vpntest1 vpntest1 213.175.37.10 19.64.1.180 vpns0  53s   (AES-128-GCM) connected

>
The server

```
root@devconf:~ # occtl
OpenConnect server control (occtl) version 0.10.8
Copyright (C) 2014 Red Hat and others.
ocserv comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to redistribute it under the conditions of the
GNU General Public License version 2.

For help type ? or 'help'
=================================
> show user vpntest1
   ID: 10257
   Username: vpntest1  Groupname: vpntest1
   State: connected
   Device: vpns0  MTU: 1360
   Remote IP: 213.175.37.10  Local Device IP: 193.110.157.103
   IPv4: 10.64.1.180  P-t-P IPv4: 10.64.1.129
   User-Agent: Open AnyConnect VPN Agent v7.06-3.fc23
   RX: 10826 (10.8 KB)  TX: 0 (0 bytes)
   Average bandwidth RX: 88 bytes/sec  TX: 0 bytes/sec
   Connected at: 2016-01-14 07:51 ( 2m:03s)
   TLS ciphersuite: (TLS1.2)-ECDHE-RSA-SECP256R1-(AES-128-GCM)
   DTLS cipher: (DTLS1.2)-(RSA)-(AES-128-GCM)
   DNS: 10.64.1.1
   Routes: 10.64.1.0/24
> 
```
The server

```
[root@devconf ~]# ocserv
OpenConnect server control (ocserv) version 0.10.8
Copyright (C) 2014 Red Hat and others.
Ocserv comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to redistribute it under the conditions of the
GNU General Public License version 2.

For help type ? or 'help'
-------------------------------------------------------------------------------------
> show users
   id        user      group     ip        vpn-ip device  since  dtls-cipher  status
10257  vpntest1  vpntest1  213.175.37.10  10.64.1.180  vpns0  3m:34s  (AES-128-GCM)  connected
> disconnect id 10257
connection ID '10257' was disconnected
> 
```
The server

[root@devconf ~]# octl
OpenConnect server control (occtl) version 0.10.8
Copyright (C) 2014 Red Hat and others.
occtl comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to redistribute it under the conditions of the
GNU General Public License version 2.

For help type ? or 'help'

> show users
    id      user     group     ip      vpn-ip  device     since      dtls-cipher status
  10257   vpntest1  vpntest1  213.175.37.10  19.64.1.180 vpns0  3m:34s  (AES-128-GCM) connected
> disconnect id 10257
connection ID '10257' was disconnected
>
VPN story

• Requirements:
  - Simple setup for users
  - Standards-based solution
  - The administrator should be able to view who is connected on every moment
  - The administrator should be able to disconnect and block access to users
  - The server should isolate users between them
  - The server should operate under the least possible privilege
Future plans
Future plans

• Extend and simplify the openconnect protocol
  - e.g., drop legacy pre-DTLS 1.0 support
  - Publish and standardize on an SSL/VPN protocol

• Improve performance by utilizing an in-kernel TLS/DTLS stack
Questions

- www.infradead.org/openconnect
- www.infradead.org/ocserv