Cisco IOS SSL VPN Backup AAA

1. Overview

This document provides configuration guidance for users of Cisco® IOS SSLVPN. This feature is designed to terminate SSL VPN connections on Cisco IOS Software-based routers (1800, 2800, 3700, 3800, 7200, and 7301). SSL VPN is comparable to and complements the popular IP Security (IPsec) remote-access VPN.

The testing was performed at the NSITE lab in Research Triangle Park, North Carolina (RTP) on the devices defined above. The objective of the testing was to configure and test interaction of Cisco IOS SSLVPN with authentication, authorization, and accounting (AAA) policies using the backup authentication setup. This is typically used by a provider with redundant AAA servers.

Advantage: The primary advantage of backup AAA authentication is the provider can have redundant AAA servers. In the event of failure, users will still be authenticated. This setup can be used with any of the AAA designs, and will work with authentication domains.

Note: All Cisco IOS SSL VPN/WebVPN features are included in a single, cost-effective license that would be purchased separately. You can purchase the feature license in packs of 10, 25, or 100 simultaneous users directly from the Cisco.com configuration tool. If you already have a router, use the following SKUs to order the license: FL-WEBVPN-10-K9=, FL-WEBVPN-25-K9=, FL WEBVPN 100-K9=. Check the data sheet to find the maximum supported users for your platform.

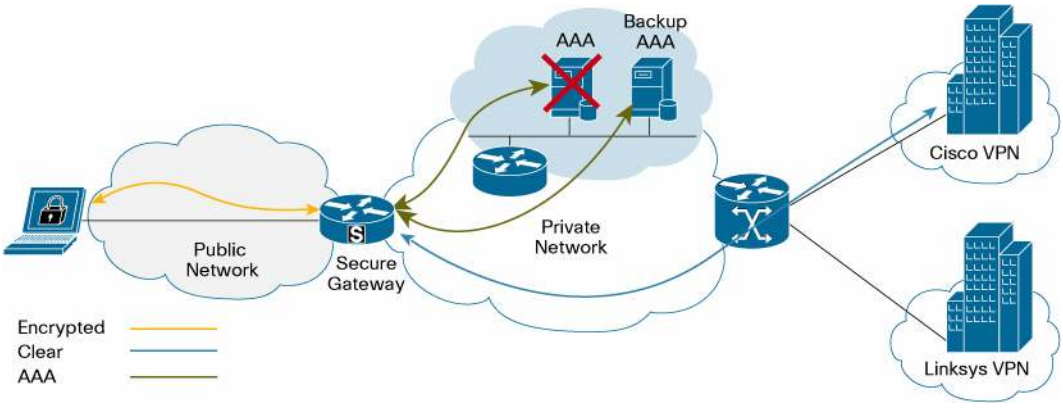
2. Audience

This configuration guide is intended for customers and partners working to provide configuration guidelines and best practices for smaller SSL VPN deployments.

3. Network Topology

Figure 1 shows a Cisco IOS SSL VPN topology that uses redundant AAA servers.

Figure 1. Cisco IOS SSL VPN Topology with Redundant AAA Servers



4. Basic Configurations

4.1 Global AAA Configuration

When the primary AAA server is unreachable, the service provider will typically have a backup AAA server. When the router does not get a pass/fail response from the primary server, it will eventually time out. Next it will send the request to the secondary server. It will work with the authentication domains as well, but this will need to be set up on both servers.

The authentication configuration can be set up in other ways, such as local backup, but this is not the best way to back up the AAA. If you do not have a secondary AAA server, local backup is your only backup option.

This is the configuration of the primary AAA server, which is not connected to the network to simulate the AAA server being unreachable. Also you can see the additional configs for the AAA local backup in the last three lines of configuration. This is only an example. In the next step, these will be removed, and the secondary AAA server will be configured.

```
!
! The RADIUS server at 100.1.1.204 is not connected.
!
aaa new-model
!
aaa group server radius FAKE
 server-private 100.1.1.204 auth-port 1645 acct-port 1646 key cisco123
 ip radius source-interface Ethernet0/0.700
!
aaa authentication login ssl_local_backup group FAKE local
!
username labuser@cisco password 0 cscolab
username labuser@linksys password 0 linklab
!
```

For the global backup, we need to set up a second AAA server to back up the first. It is a similar configuration, and all output in the rest of this document was gathered using the configuration below. We are not using the configs for local backup.

```
!
! The RADIUS server at 100.1.1.204 is not connected.
!
aaa new-model
!
aaa group server radius AR
 server-private 100.1.1.2 auth-port 1645 acct-port 1646 key cisco123
 ip radius source-interface Ethernet0/0.700
!
aaa group server radius FAKE
 server-private 100.1.1.204 auth-port 1645 acct-port 1646 key cisco123
 ip radius source-interface Ethernet0/0.700
!
aaa authentication login ssl_global_backup group FAKE group AR
!
```

The AAA backup is a simple process, and Cisco.com has more information on the AAA configuration options. This document is only meant to show how it works with Cisco IOS SSL VPN.

4.1.1 WebVPN Gateway Configuration

```
webvpn gateway ssl-gw1
 ip address 172.18.143.195 port 443
 ssl trustpoint win2k3
 inservice
 !
```

4.1.2 WebVPN Context Configuration

In the configuration, we have setup both contexts to use the global RADIUS servers. For this reason, we have added the AAA authentication domain for security. This is not mandatory, but it is good to use when you have a shared set of AAA servers.

```
!
! The two contexts are configured for authentication local backup.
!
webvpn context vpn1
 ssl authenticate verify all
 !
 url-list “eng”
   url-text “wwwin-eng” url-value “http://wwwin-eng.cisco.com”
 !
 policy group vpn1
   url-list “eng”
 !
 default-group-policy vpn1
 aaa authentication list ssl_global_backup
 aaa authentication domain @cisco
 gateway ssl-gw1 domain cisco
 inservice
!
webvpn context vpn2
 ssl authenticate verify all
 !
 policy group vpn2tunnel
   functions svc-enabled
   svc address-pool “ssl_addr_pool1”
 !
 default-group-policy vpn2
 aaa authentication list ssl_global_backup
 aaa authentication domain @linksys
 gateway ssl-gw1 domain linksys
 inservice
!
```

Note: The configurations above do not include the configuration of virtual routing and forwarding (VRF) on the contexts. If you need to use internal VRF instances, add the command "**vrf** *vrf-name*" to the context configuration. If the internal network is a service provider, or VRF-aware RADIUS groups are used, you may have to apply VRF to the context.

4.1.3. Static Routing Configuration

```
!
! The Global default route is to allow the SSL session to work with
the user on the
! public network. Any routes on the backend need to be handled with
additional
! routing.
!
ip route 0.0.0.0 0.0.0.0 172.18.143.1
!
```

5. Context Configuration Verification

Note: All the output below is from Cisco IOS Software Release 12.4(9)T.

The global table is configured with a default route back to the public Internet. You will notice the route to the 100.1.1.0/24 network. This is the management network of the provider, and the secondary AAA server is at 100.1.1.2. Remember that the primary AAA

```
server is unreachable, but it exists on the same LAN, though it can
exist on another subnet as well.
sslvpn1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     100.0.0.0/24 is subnetted, 1 subnets
C       100.1.1.0 is directly connected, Ethernet0/0.700
     172.18.0.0/24 is subnetted, 1 subnets
C       172.18.143.0 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 172.18.143.1
```

5.1 AAA Authentication List

The AAA authentication list we are using is the ssl_global_backup, which uses two global service provider AAA servers on the management network. The Cisco Access Registrar (AR) is backing up the FAKE server. For our test, the FAKE server is not responding.

```
sslvpn1#show aaa method-lists authentication
authen queue=AAA_ML_AUTHEN_LOGIN
  name=ssl_global_backup valid=TRUE id=29000003 : SERVER_GROUP FAKE
SERVER_GROUP AR
authen queue=AAA_ML_AUTHEN_ENABLE
authen queue=AAA_ML_AUTHEN_PPP
authen queue=AAA_ML_AUTHEN_SGBP
authen queue=AAA_ML_AUTHEN_ARAP
authen queue=AAA_ML_AUTHEN_DOT1X
authen queue=AAA_ML_AUTHEN_EAPOUDP
authen queue=AAA_ML_AUTHEN_8021X
permanent lists
  name=Permanent Enable None valid=TRUE id=0 : ENABLE NONE
  name=Permanent Enable valid=TRUE id=0 : ENABLE
  name=Permanent None valid=TRUE id=0 : NONE
  name=Permanent Local valid=TRUE id=0 : LOCAL
sslvpn1#
```

5.2. WebVPN Gateway

```
sslvpn1#show webvpn gateway ssl-gw1
Admin Status: up
Operation Status: up
IP: 172.18.143.195, port: 443
SSL Trustpoint: win2k3
5.3  WebVPN Context
You can see in the output below that the context for vpn1 is set up
for AAA authentication using the policy configured with backup.
sslvpn1#show webvpn context vpn1
Admin Status: up
Operation Status: up
CSD Status: Disabled
Certificate authentication type: All attributes (like CRL) are
verified
AAA Authentication List: ssl_global_backup
AAA Authentication Domain: @cisco
Default Group Policy: vpn1
Associated WebVPN Gateway: ssl-gw1
Domain Name: cisco
Maximum Users Allowed: 1000 (default)
NAT Address not configured
VRF Name not configured

sslvpn1#show webvpn context vpn2
```

```
Admin Status: up
Operation Status: up
CSD Status: Disabled
Certificate authentication type: All attributes (like CRL) are
verified
AAA Authentication List: ssl_global_backup
AAA Authentication Domain: @nortel
Default Group Policy: vpn2
Associated WebVPN Gateway: ssl-gw1
Domain Name: linksys
Maximum Users Allowed: 1000 (default)
NAT Address Range not configured
VRF Name not configured
```

6. Context Operation and Verification

Note: All the output below is from Cisco IOS Software Release 12.4(9)T.

6.1 User "labuser" Logged Into Context vpn1

```
sslvpn1#show webvpn session context vpn1
WebVPN context name: vpn1
Client_Login_Name  Client_IP_Address  No_of_Connections  Created
Last_Used
labuser            192.82.240.250            1          00:20:07
00:20:04

sslvpn1#show webvpn session user labuser context vpn1

WebVPN user name = labuser ; IP address = 192.82.240.250 ; context =
vpn1
    No of connections: 1
    Created 00:20:21, Last-used 00:20:18
    Client Port: 2214
    User Policy Parameters
      Group name = vpn1
    Group Policy Parameters
      url list name = "vpn1"
      idle timeout = 2100 sec
      session timeout = 43200 sec
      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep sslvpn client installed = disabled
      rekey interval = 3600 sec
      rekey method = ssl
      lease duration = 43200 sec
```

6.2 Debugging the Session Login

The debug output in this case shows that user “labuser” was authenticated. The username “labuser@cisco” was sent to the FAKE server, which is unreachable or unresponsive. Next, the authentication request is sent to the AR since it is the secondary AAA group listed. If you notice the timestamp in the debugs, the time from the beginning of the authentication to the “passed” response is about 21 seconds, because the first request has to time out.

```
sslvpn1#
.Feb 28 01:27:17.781: AAA/AUTHEN/LOGIN (00000000): Pick method list
'ssl_global_backup'
.Feb 28 01:27:17.781: SSLVPN: AAA authentication request sent for
user: "labuser"
.Feb 28 01:27:17.781: RADIUS/ENCODE(00000000):Orig. component type =
INVALID
.Feb 28 01:27:17.781: RADIUS/ENCODE(00000000): dropping service type,
"radius-server attribute 6 on-for-login-auth" is off
.Feb 28 01:27:17.781: RADIUS(00000000): Config NAS IP: 100.1.1.20
.Feb 28 01:27:17.781: RADIUS(00000000): sending
.Feb 28 01:27:17.781: RADIUS(00000000): Send Access-Request to
100.1.1.204:1645 id 1645/7, len 50
.Feb 28 01:27:17.781: RADIUS:  authenticator B7 6B 9B 77 F5 B9 BF 96 -
54 9A A8 34 03 58 48 CE
.Feb 28 01:27:17.781: RADIUS:  User-Name           [1]   6   "labuser"
.Feb 28 01:27:17.781: RADIUS:  User-Password       [2]   18  *
.Feb 28 01:27:17.781: RADIUS:  NAS-IP-Address      [4]   6
100.1.1.20
.Feb 28 01:27:22.945: RADIUS: no sg in radius-timers: ctx 0xBE02924 sg
0x0000
.Feb 28 01:27:22.945: RADIUS: Retransmit to (100.1.1.204:1645,1646)
for id 1645/7
.Feb 28 01:27:28.170: RADIUS: no sg in radius-timers: ctx 0xBE02924 sg
0x0000
.Feb 28 01:27:28.170: RADIUS: Retransmit to (100.1.1.204:1645,1646)
for id 1645/7
.Feb 28 01:27:33.811: RADIUS: no sg in radius-timers: ctx 0xBE02924 sg
0x0000
.Feb 28 01:27:33.811: RADIUS: Retransmit to (100.1.1.204:1645,1646)
for id 1645/7
.Feb 28 01:27:39.068: RADIUS: no sg in radius-timers: ctx 0xBE02924 sg
0x0000
.Feb 28 01:27:39.068: RADIUS: No response from (100.1.1.204:1645,1646)
for id 1645/7
.Feb 28 01:27:39.068: RADIUS/DECODE: parse response no app start; FAIL
.Feb 28 01:27:39.068: RADIUS/DECODE: parse response; FAIL
.Feb 28 01:27:39.068: RADIUS/ENCODE(00000000):Orig. component type =
INVALID
.Feb 28 01:27:39.068: RADIUS/ENCODE(00000000): dropping service type,
"radius-server
attribute 6 on-for-login-auth" is off
.Feb 28 01:27:39.068: RADIUS(00000000): Config NAS IP: 100.1.1.20
.Feb 28 01:27:39.068: RADIUS(00000000): sending
.Feb 28 01:27:39.068: RADIUS(00000000): Send Access-Request to
100.1.1.2:1645 id
1645/8, len 50
```

```
.Feb 28 01:27:39.068: RADIUS:  authenticator 11 F3 E8 A5 86 D1 62 24 –
BD F5 A9 E2
76 11 9E 51
.Feb 28 01:27:39.068: RADIUS:  User-Name           [1]   6   "labuser"
.Feb 28 01:27:39.068: RADIUS:  User-Password       [2]   18  *
.Feb 28 01:27:39.068: RADIUS:  NAS-IP-Address      [4]   6
100.1.1.20
.Feb 28 01:27:39.080: RADIUS: Received from id 1645/8 100.1.1.2:1645,
Access-Accept,
len 20
.Feb 28 01:27:39.080: RADIUS:  authenticator 47 EB 5D 52 5B E4 10 C1 -
8D 34 D3 37 68
F5 71 22
.Feb 28 01:27:39.080: RADIUS(00000000): Received from id 1645/8
*Feb 28 01:27:38.451: WEBVPN-slave#1: SSLVPN: AAA Authentication
Passed !
sslvpn1#
```

Note: The debugs above are from the following debug commands:

```
sslvpn1#sh deb
General OS:
  AAA Authentication debugging is on
WebVPN Subsystem:
 WebVPN AAA debugs debugging is on
Radius protocol debugging is on
Radius packet protocol debugging is on
```

7. Limitations, Caveats, Integration Issues, and Guidelines

- None

8 .Related Documents

- Cisco IOS SSL VPN page: http://www.cisco.com/go/iossslvpn
- Data sheet: http://www.cisco.com/en/US/products/ps6635/products_data_sheet0900aecd80405e25.html
- Configuration guide: http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00805eeaea.html

9. Acknowledgements

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-362467-01 02/08

