Cisco IOS SSL VPN AAA Authentication Domain

1. Overview

This document provides configuration guidance for users of Cisco IOS® SSL VPN. This feature is designed to terminate SSL VPN connections on Cisco IOS Software-based routers (Cisco 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 SSL VPN with authentication, authorization, and accounting (AAA) policies using the authentication domain setup. This is typically used by a provider offering the Cisco IOS SSL VPN service to enterprise customers for their SSL VPN termination.

Advantage: The primary advantage of AAA authentication domain is that the provider can maintain the user list in the “user@domain” format. This way, if the same username exists in two different VPNs, the WebVPN gateway domain is automatically appended to the username, creating a user@domain. This is comparable to the Group Lock feature in IPsec. Basically, it creates better security and manageability for the VPN because the @domain is always appended, and it is unlikely that two users will have the same password.

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 the network topology of the Cisco IOS SSL VPN with the AAA server.
**Figure 1.** Cisco IOS SSL VPN Topology with AAA Server

### 4. Basic Configurations

**4.1 Global AAA Configuration**

```
!  The RADIUS server is located at 100.1.1.2 on the management LAN.
!  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 authentication login ssl_global group AR
  aaa authorization console
  aaa session-id common
!

**4.2 WebVPN Gateway Configuration**

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

**4.3 WebVPN Context Configuration**

The authentication configuration has a minor problem, since the user list is shared by all contexts. If both contexts have a user “labuser”, that user can access both contexts, and therefore be a security hole.
There is a simple way to enhance this scenario and make it secure with the use of authentication domains. The username passed to the context from the VPN user is concatenated with the string specified in the authentication domain command. This string is then sent to the AAA server.

**Note:** The user must be configured on the AAA server to handle the parsing of the domain. You may have to set up the users in the AAA server with the domain appended to the username. Please refer to the documentation or guides for your AAA server for more information on how to configure this feature.

```plaintext
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
    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
    aaa authentication domain @linksys
    gateway ssl-gw1 domain linksys
    inservice
  !
```

Now, the context vpn1 has the authentication string "@cisco". When a user logs into the context, the username sent to AAA is "<user>@cisco". However, if user "<user>" logs into context vpn2, the username will be "<user>@linksys", and the password will not match.

**Note:** The configurations above do not include the configuration of virtual routing and forwarding (VRF) on the contexts. If you are 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.

### 4.4 Static Routing Configuration

All contents are Copyright © 1992–2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.
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 AAA server is at 100.1.1.2.

```
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
 C  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 ssl_global, which uses the global AAA server on the management network.

```
sslvpn1#show aaa method-lists authentication
   authen queue=AAA_ML_AUTHEN_LOGIN
     name=ssl_global valid=TRUE id=7E000001 : 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

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 to the local user list.
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
AAA Authentication Domain: @cisco
Default Group Policy: vpn1
Associated WebVPN Gateway: ssl-gw1
Domain Name: cisco
Maximum Users Allowed: 1000 (default)
NAT Address Range 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
AAA Authentication Domain: @linksys
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

This output shows 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            192.102.38.240             2          00:00:21 00:00:18

sslvpn1#show webvpn session user labuser context vpn1
WebVPN user name = labuser ; IP address = 192.102.38.240 ; context = vpn1
No of connections: 2
Created 00:00:37, Last-used 00:00:35
Client Port: 2089
Client Port: 2090
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. In the RADIUS debugs, you see that labuser@cisco was sent to the RADIUS server.

```
sslvpn1#
.Feb 25 00:35:23.905: AAA/AUTHEN/LOGIN (00000000): Pick method list 'ssl_global'
.Feb 25 00:35:23.905: SSLVPN: AAA authentication request sent for user: "labuser"
.Feb 25 00:35:23.905: RADIUS(00000000): Config NAS IP: 100.1.1.20
.Feb 25 00:35:23.905: RADIUS(00000000): sending
.Feb 25 00:35:23.905: RADIUS(00000000): Send Access-Request to 100.1.1.2:1645 id 1645/1, len 56
```
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 Website: http://www.cisco.com/go/iossslvpn

9. Acknowledgements

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