Cisco IOS SSL VPN Policy Groups

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 SSL VPN-capable 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 the uses of WebVPN contexts, and the policy groups. Basically, we will look at how the policy group is used and set up in the context. We will also look at how each setup is used from the end-user perspective.

This document discusses some of the configuration concepts and usage. The policy group is the template of parameters an end-user SSL VPN session will embody during session establishment. The enforcement of policy is an important part of any SSL VPN service.

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.

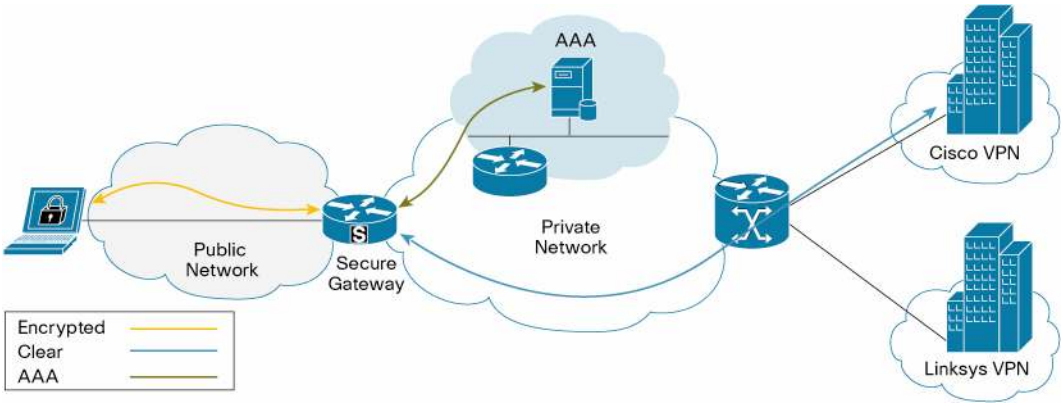
2. Audience

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. Basic Cisco IOS SSL VPN Topology with AAA Server

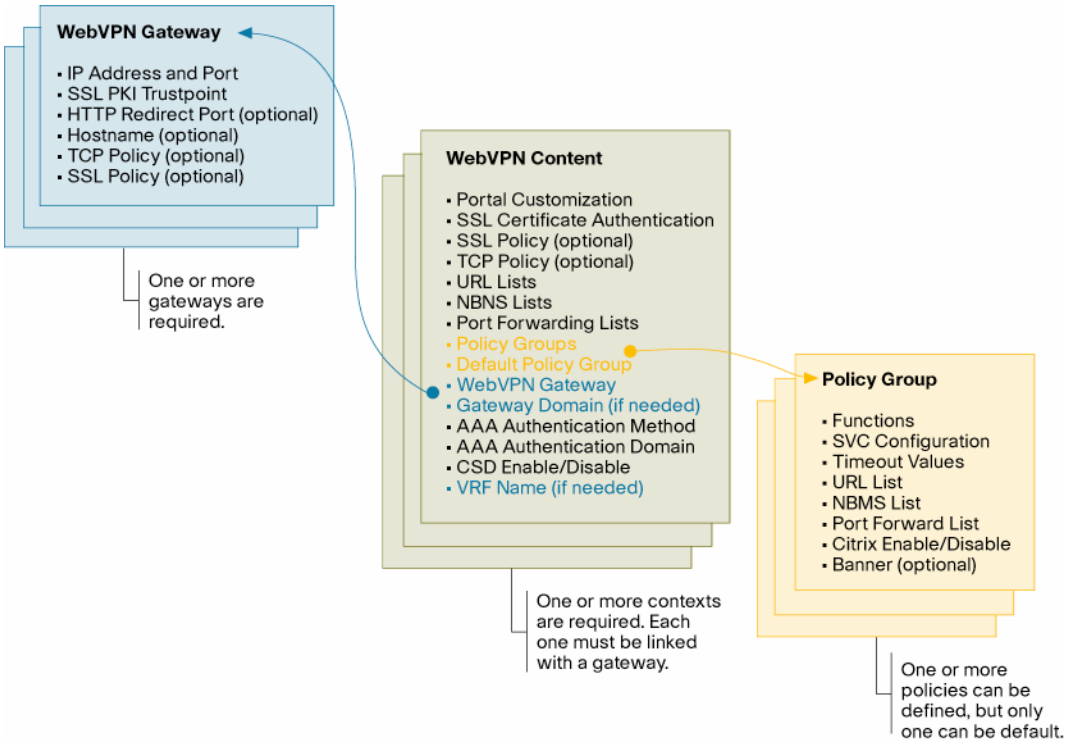


4. Basic Configurations

4.1 Configuration Overview

This document only considers the configuration of the SSL VPN policy groups, and how these components work with the contexts. In Figure 2, you can see how the gateways, contexts, and policy groups are related. You can also see that the context is the main focus for the user sessions. The gateway is just the destination IP endpoint for the user session, and the context is where the policy group is defined and applied to the user session. The policy group determines the parameters of the user session, and how the session will behave.

Figure 2. Cisco IOS SSL VPN Configuration Map



4.2 Policy Groups

The policy group is where the administrator can specify the SSL VPN user session parameters and set up the appearance of the login/portal page. Its scope is limited for use within a given context. The policies can be used to specify the common session parameters for a group of users. Typically, the administrator will set up multiple policy groups; however, only one policy can be applied as default.

In Clientless mode the portal, including the toolbars and links, is set up under the policy. In Tunnel mode, the administrator can set up the tunnel mode capabilities, and specify the SSL VPN Client user parameters.

4.2.1 Multiple Policy Groups

It is common to have multiple groups of users; not every user will have the same needs, or permissions to resources on the VPN. For each group of users, you may want to define a unique policy group.

Since you can only define one default policy group, there needs to be a way to dynamically assign a user to any group. RADIUS attributes are used to do this. During authentication, the RADIUS server can push down the *webvpn:user-vpn-group* attribute (Appendix A), which selects one of the configured policy groups. If the policy group name does not exist, or this attribute is not pushed down for the authenticated user, the default policy group will be used if configured. So, it is possible to only allow policy group assignment using RADIUS attributes.

```
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"
 !
 policy group vpn1tunnel
   functions svc-enabled
   svc address-pool "ssl_addr_pool1"
 !
 vrf-name vpn1
 default-group-policy vpn1
 gateway ssl-gw1 domain cisco
 inservice
!
webvpn context vpn2
 ssl authenticate verify all
 !
 url-list "linksys"
   url-text "Linksys" url-value "http://www.linksys.com"
 !
 policy group vpn2
   url-list "linksys"
 !
 policy group vpn2tunnel
   functions svc-enabled
   svc address-pool "ssl_addr_pool2"
 !
 default-group-policy vpn2
 gateway ssl-gw1 domain nsite
 inservice
!
```

Note: Policy groups can either be applied to a user session using the '*default-group-policy*' command or can be applied to a user session through the RADIUS attribute *webvpn:user-vpn-group* (Appendix A).

4.2.2 Default Policy Group

The '*default-group-policy*' command is used to apply a policy to any user that logs in, and is not assigned a policy through RADIUS. Only one policy group can be configured as default under the context using the *default-group-policy* <*name*> command.

There are a few reasons to set up one policy group as the default:

1. If the context has only one policy group, and does not use RADUIS authentication and attributes, the *default policy group* command is the only way to apply a policy.
2. If the context does use RADIUS authentication, and the *webvpn:user-vpn-group* attribute does not match any of the configured policies, the default policy will be applied.
3. It can be used as a "catch-all", where most of the remote users will fall into the policy but only special cases need to be handled through the RADIUS attribute.

```
webvpn context vpn1
 title "SSLVPN Cisco"
 logo file flash:/nsitelogo.gif
 title-color #4186BE
 secondary-color #9ABEDC
 ssl authenticate verify all
 !
 policy group aswan
   functions svc-enabled
   svc address-pool "ssl_addr_pool1"
 !
 policy group eng
   functions svc-required
   svc address-pool "ssl_addr_pool1"
 !
 default-group-policy aswan
 gateway ssl-gw1 domain cisco
 inservice
!
```

5. SSL VPN Session Establishment

5.1 End-to-End User Data Flow

Figure 3 shows the sequence of events that take place when a user establishes an SSL VPN session to the IOS SSL VPN router.

Figure 3. End-to-End SSL VPN

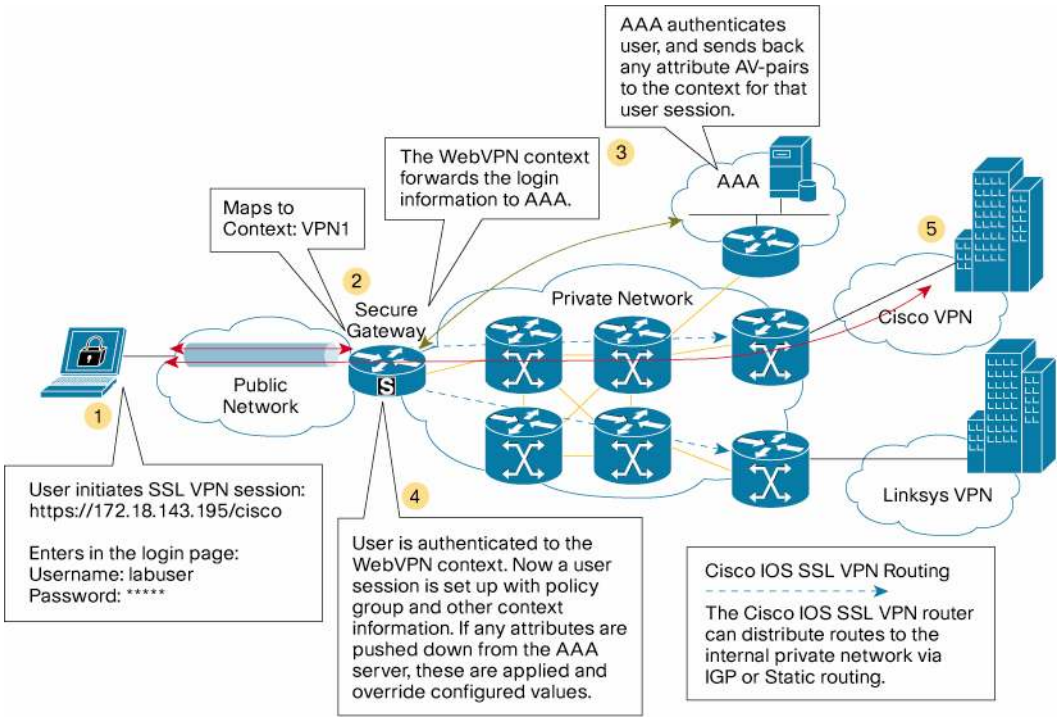


Figure 3 shows how the end-to-end SSL VPN is established. This basically applies to all SSL VPN modes.

1. The end user initiates the SSL VPN connection to the WebVPN gateway. This can be a DNS name or IP address. Depending on the method being used to log into the gateway, the user will have to enter the username and password.
2. The context a user is attempting to connect to is identified by the URL or login information. Now the user must be authenticated under the context they belong to.
3. The secure gateway must determine if it will let this user into the WebVPN context, so it will send the username and password to the AAA server. The method of AAA does not matter, just so authentication can be done.
4. The AAA server authenticates the user and it will indicate this to the context. It may also push down any RADIUS attributes for that user. The WebVPN context will build a user session under the context, and apply the policy group information and RADIUS attributes. Now the workflow changes depending on the policy group parameters applied to the user session.
   - If the user is using Clientless mode, which is the default mode for a context, the process is complete. The WebVPN portal will now be displayed to the end user in the Web browser. The user will have the specified access to the VPN.
   - If the user is going to do Tunnel mode, using function **svc-enabled** or **svc-required** in the group policy or RADIUS attributes, the process to push down the SSL VPN Client will happen next. This will mean that the SSL VPN Client once installed on the client PC will establish a new SSL session to the context, and the original context will be removed. Furthermore, it will alter the PC routing table to do the specified tunnel function defined in the policy.
5. Now that the user session is established to the WebVPN secure gateway, the backend interfaces handle the access to the inside network.

Once a user is authenticated under a given context, the user session is established. This user session will embody the parameters specified globally in the context, the group policy, and any RADIUS attributes pushed down during authentication for that user.

Note: RADIUS attributes pushed from the AAA server for a user session will override the equivalent configured values. This allows the group policy to apply the entire default configuration for a group of users, and the RADIUS attributes will fine-tune the user session.

6. Limitations, Caveats, Integration Issues, and Guidelines

- None.

7. Related Documents

- Cisco IOS SSL VPN page: http://www.cisco.com/go/iossslvpn
- Data sheet: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet0900aecd802aff73.html
- Configuration guide: http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_book09186a008047b40c.html

Acknowledgements

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

Appendix A—SSL VPN RADIUS Attribute-Value Pairs

Note: All WebVPN attributes (except for the standard IETF RADIUS attributes) start with **webvpn**.

For example:

- webvpn:urllist-name=cisco
- webvpn:nbnslist-name=cifs
- webvpn:default-domain=cisco.com

Attribute	Type of Value	Values	Default
addr (Framed-IP-Address)[1]	ipaddr	IP_address	
addr-pool	string	name	
banner	string		
default-domain	string		
dns-servers	ipaddr	IP_address	
dpd-client-timeout	integer (seconds)	0 (disabled)-3600	300
dpd-gateway-timeout	integer (seconds)	0 (disabled)-3600	300
file-access	integer	0 (disable) 1 (enable)[2]	0
file-browse	integer	0 (disable) 1 (enable)[2]	0
file-entry	integer	0 (disable) 1 (enable)[2]	0
hide-urlbar	integer	0 (disable) 1 (enable)[2]	0
home-page	string		
idletime (Idle-Timeout)[1]	integer (seconds)	0-3600	2100
ie-proxy-exception	string	DNS_name	
	ipaddr	IP_address	
ie-proxy-server	ipaddr	IP_address	
inacl	integer	1-199, 1300-2699	
	string	name	
keep-svc-installed	integer	0 (disable) 1 (enable)[2]	1
nbnslist-name	string	name	
netmask (Framed-IP-Netmask)[1]	ipaddr	IP_address_mask	
port-forward-name	string	name	
primary-dns	ipaddr	IP_address	
rekey-interval	integer (seconds)	0-43200	3600
secondary-dns	ipaddr	IP_address	
split-dns	string		
split-exclude[3]	ipaddr ipaddr	IP_address IP_address_mask	

[1] Standard IETF RADIUS attributes.
[2] Any integer other than 0 enables this feature.
[3] You can specify either split-include or split-exclude, but you cannot specify both options.

Attribute	Type of Value	Values	Default
	word	local-lans	
split-include[3]	ipaddr ipaddr	IP_address IP_address_mask	
svc-enabled[4]	integer	0 (disable) 1 (enable)[2]	0
svc-ie-proxy-policy	word	none, auto, bypass-local	
svc-required[4]	integer	0 (disable) 1 (enable)[2]	0
timeout (Session-Timeout)[1]	integer (seconds)	1-1209600	43200
urllist-name	string	name	
user-vpn-group	string	name	
wins-server-primary	ipaddr	IP_address	
wins-servers	ipaddr	IP_address	
wins-server-secondary	ipaddr	IP_address	

2

-6

[4] You can specify either svc-enable or svc-required, but you cannot specify both options.

Appendix B—Cisco IOS SSL VPN Configuration

```
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname VXR-SSL-AGG
!
enable password lab
!
aaa new-model
!
aaa group server radius ACS
 server-private 217.1.1.1 auth-port 1645 acct-port 1646 key cisco123
 ip vrf forwarding vpn1
 ip radius source-interface GigabitEthernet0/0.501
!
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
!
aaa authentication login ssl_ent group ACS
aaa authentication login ssl_global group AR
!
aaa session-id common
!
ip subnet-zero
!
ip cef
ip domain name cisco.com
ip name-server 64.102.6.247
ip name-server 172.18.138.14
!
crypto pki trustpoint win2k3
 enrollment mode ra
 enrollment url http://nsite-ipsec5:80/certsrv/mscep/mscep.dll
 serial-number
 fqdn VXR-SSL-AGG.cisco.com
 revocation-check crl
 rsakeypair rsakey
!
!
crypto pki certificate chain win2k3
 certificate 12DF1640000000000009
 certificate ca 18D72EA3CA8438B7423E4553363F9E85
!
username lab password 0 lab
username labuser@cisco password 0 lab
```

```
!
interface Ethernet0/0
 description management to 7600-3:f3/7
 ip address 100.1.1.220 255.255.255.0
 duplex auto
 ntp broadcast client
!
interface GigabitEthernet0/0
 description to 7600-3:g8/3
 no ip address
 duplex full
 speed 1000
 media-type gbic
 no negotiation auto
!
interface GigabitEthernet0/0.143
 description Connection to Lab BB
 encapsulation dot1Q 143
 ip address 172.18.143.194 255.255.255.0
 no snmp trap link-status
!
interface GigabitEthernet0/0.501
 encapsulation dot1Q 501
 ip address 120.1.1.250 255.255.255.0
 no snmp trap link-status
!
interface GigabitEthernet0/0.502
 encapsulation dot1Q 502
 ip address 120.1.2.250 255.255.255.0
 no snmp trap link-status
!
ip classless
!
ip local pool ssl_addr_pool2 120.1.2.200 120.1.2.210 group vpn2
!
ip route 0.0.0.0 0.0.0.0 172.18.143.1
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password lab
!
ntp clock-period 17179864
!
webvpn gateway ssl-gw1
 ip address 172.18.143.193 port 443
```

```
 ssl trustpoint win2k3
 inservice
 !
webvpn install svc disk0:/webvpn/svc.pkg
webvpn install csd disk0:/webvpn/sdesktop.pkg
 !
webvpn context vpn1
title "SSLVPN Cisco"
 logo file disk0:/nsitelogo.gif
 title-color #4186BE
 secondary-color #9ABEDC
 ssl authenticate verify all
 !
 url-list "nsite"
   heading "NSITE Links"
   url-text "NSITE" url-value "http://nsite.cisco.com"
   url-text "ASWAN" url-
value "http://nsite/groups/ST5/content/aswan/aswan-main.htm"
 !
 url-list "eng"
   url-text "wwwin-eng" url-value "http://wwwin-eng.cisco.com"
 !
 policy group vpn1
   url-list "eng"
 !
 policy group aswan
   url-list "nsite"
 !
 default-group-policy aswan
 aaa authentication list ssl_global
 aaa authentication domain @cisco
 gateway ssl-gw1 domain cisco
 inservice
!
webvpn context vpn2
 title "Linksys SSLVPN"
 title-color #601080
 secondary-color #E1A0FF
 ssl authenticate verify all
 !
 policy group vpn2
   functions svc-required
   svc address-pool "ssl_addr_pool2"
   svc split exclude local-lans
   svc split exclude 172.18.0.0 255.255.0.0
 !
 default-group-policy vpn2tunnel
 aaa authentication list ssl_global
 aaa authentication domain @linksys
 gateway ssl-gw1 domain linksys
```

```
 inservice
!
end
```

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

Printed in USA C11-362464-01 02/08

