ılıılı cısco

Cisco Adaptive Security Appliance Smart Tunnels Solution Brief

August 2012

Guide

Contents

Introduction	3
Smart Tunnel Applications Smart Tunnel Advantages over Port-Forwarding, Plug-ins Smart Tunnel Compared to AnyConnect Secure Mobility Client Smart Tunnel End-User Experience System Requirements	3 4 4
Configuration Examples	5
Native Client-Server Applications Web Applications Access Lists (web-type) Tunnel Policy for Smart Tunnel Single Sign-On (SSO) For Smart Tunnel External Portal Page	7 8 8 9
Deployment Considerations	.13
Security Implications Protected Mode for Windows Proxy Servers Customization Troubleshooting Common Problems	. 13 . 14 . 14
Conclusion	15
Appendix A1: Finding Application Process Names on Windows	.15
Appendix A2: Popular Applications	. 17
Appendix A3: Smart Tunnel for VMWare View Client	.18

Introduction

The Cisco[®] Adaptive Security Appliance (ASA) 5500 Series SSL VPN Edition offers flexible Client and Clientless SSL VPN capabilities. It supports highly secure connections across public networks to mobile users, contractors, and business partners.

Smart Tunnel is an advanced feature of Clientless SSL VPN¹ that provides seamless and highly secure remote access for native client-server applications. It also complements the clientless rewriter in support of proprietary applications or web pages that are technically difficult to rewrite.

Clientless SSL VPN with Smart Tunnel is the preferred solution for allowing access from non-corporate assets as it does not require the administrative rights, and it avoids the need to install a Full-Tunnel VPN Client on the endpoint. Smart Tunnel supports multiple configurable options to customize the security policy, while helping to ensure a simplified user experience.

This solution brief provides an overview, configuration examples, and best practices of using Smart Tunnel. The target audience includes security engineers and administrators. A basic working knowledge of Cisco ASA, Clientless SSL VPN, and AnyConnect is assumed.

After reading this document, you should have a good understanding of the components involved in the solution, and will be well equipped to review other detailed collateral.

Smart Tunnel Applications

Smart Tunnel allows any TCP-based client-server application to use ASA as a proxy gateway to the private side of a network. Examples of native applications that work through Smart Tunnel include Outlook, SharePoint, Telnet, Passive FTP, Lotus Sametime, Secure Shell (SSH), Remote Desktop Protocol (RDP), and Virtual Network Computing (VNC). Smart Tunnel does not support applications that use Universal Datagram Protocol (UDP). Using the Cisco ASA Device Manager (ASDM), an administrator can define which applications and networks are allowed access.

Smart Tunnel is also used to provide remote access to web applications that are difficult to rewrite, such as proprietary, non-standards-based Java, Java Script, or Flash animations. Smart Tunnel also supports Single Sign-On to web applications that require either form-based POST parameters, http basic, FTP, or NTLM authentication

Smart Tunnel can also co-exist with a Full-Tunnel VPN Client. For example, an employee can connect to the company network by using Full-Tunnel VPN Client, while simultaneously connecting to a vendor network by using Smart Tunnel.

Smart Tunnel Advantages over Port-Forwarding, Plug-ins

- Smart Tunnel offers better performance than browser plug-ins.
- Port forwarding is the legacy technology for supporting TCP-based applications over a Clientless SSL VPN connection. Unlike port forwarding, Smart Tunnel simplifies the user experience by not requiring the user connection of the local application to the local port.
- Smart Tunnel does not require users to have administrator privileges.
- Smart Tunnel does not require the administrator to know application port numbers in advance.

¹ Clientless SSL VPN:

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd80402e3f.html.

Smart Tunnel Compared to AnyConnect Secure Mobility Client²

Smart Tunnel is used with Clientless SSL VPN (also known as L7VPN, Browser-Based VPN or WebVPN) to provide remote access for specific administrator-approved native TCP-based client-server applications on Windows and Mac OS X. For Linux, iOS, and Android devices, AnyConnect is the preferred solution for native applications access to corporate resources.

Smart Tunnel is the preferred deployment method for assets that do not provide administrative privileges. It is also ideal for user communities, such as vendors and contractors, who should not have access to the Layer-3 Full-Tunnel AnyConnect VPN Client.

The following table highlights the major differences between Smart Tunnel and AnyConnect Secure Mobility Client:

Feature	Smart Tunnel	AnyConnect Secure Mobility Client
Type of VPN	L7 VPN	L3 VPN
Type of Asset	Trusted and untrusted assets	Trusted assets
Type of Users	Vendors, partners, contractors, and employees	Employees
Type of Applications	TCP ports	TCP and UDP ports
Admin Privileges on the End Point	Not required	Required for initial installation
Granular Application Access Control	Administrator defines the applications that are allowed access to the tunnel	All applications have access to the tunnel
Single Sign-On	Supported for Web Applications	Not supported
Access-List	Web-Type (L7) ACL	Network (L3) ACL
Split-Tunnel Policy	Supported	Supported
Stateful Failover	Not supported	Supported
OS Support	Windows, Mac OS X (Requires Active-X or Java)	Windows, Mac OS X, Linux, iOS, Android
License	AnyConnect Premium	AnyConnect Premium or AnyConnect Essentials
Server-Side Proxy	Not supported	Supported
Client-Side Proxy	Supported	Supported

 Table 1.
 Comparison: Smart Tunnel and AnyConnect

Smart Tunnel End-User Experience

Login

1. Authenticate with the Clientless SSL VPN (such as https://myasa.example.com).

Native Client-Server Applications

- 2. From the main portal page, navigate to the Application Access Panel³.
- 3. As soon as the page loads, the browser downloads the necessary software modules to launch Smart Tunnel.
- Launch any of the allowed native client-server applications to access remote corporate network using the Smart Tunnel.

 ² AnyConnect Datasheet: <u>http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/data_sheet_c78-527494.pdf</u>.
 3 User-Experience:

http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy_files/deploy-72.jpg.

Web Pages Configured for Smart Tunnel

- 5. From the main portal page, navigate to the Web Applications Panel.
- 6. Click on the specific published web bookmark.
- 7. Browser downloads the necessary software modules to launch Smart Tunnel.
- 8. The bookmark is opened in a new browser window that uses Smart Tunnel to access remote corporate network.

Logoff

 After all the applications are closed, either log out of the Clientless SSL VPN session or close all the browser windows.

Note: From ASA Release 8.3.1 or later, administrators can choose to provide a logout icon⁴ so that the Smart Tunnel stays active, even when all the browser windows are closed.

System Requirements

Smart Tunnel requires AnyConnect Premium License to be installed on the ASA VPN Gateway. The ASA configuration guide⁵ lists the specific browsers supported on Mac OS X and Windows. Smart Tunnel requires the browser to enable either MS Active-X or Java or both.

Note: Smart Tunnel was introduced in ASA 8.0 release. However, please consult the respective administrator guide for specific functionality support.

Configuration Examples

Native Client-Server Applications

This procedure should only be used for supporting applications outside of the browser. The ASA administrator defines the approved list of applications, along with the processes used by each application. For example, Outlook 2010 uses "outlook.exe" on Windows; hence, a Smart Tunnel entry has to be created with that process name. Please refer to (Appendix A1) on how to find out the process names for an application. Also, (Appendix A2) has list of popular applications and their process names.

Note: From ASA Release 8.3 and later, administrators can also enter wild-card entries for the application path name (for example, out*.exe matches outlook.exe).

http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/vpn_clientless_ssl.html#wp1733488.

 ⁴ Logout Icon: <u>http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/vpn_clientless_ssl.html#wp1733488</u>.
 ⁵ ASA Administration Guide:



	uration > Rem	tote Access VPN	> Clientless	SSL VPN Access	> Portal > Smart Tunnels				
annin Access Four eccliKEV1) Connec trure Mobility Solur dress Assignmen ess SSL VPN Acce ↓ Click	table. to Log Off Smar off the smart-tu	t Tunnel Session unnel when its pa nel logoff icon in	rent process,	, such as a browse		group policy or u	ser policy	by clicking on the Assign button above	e the
Bookmarks & Add	🖬 Edit 📋 De	elete 💥 Assign	Find:		Match Case				
Client-Server Plu Customization List Name		Application ID		Process Name	≜ ¹ OS	Hash		Group Policies/User Policies Assigned to	
Help Customizat	0		Add	Smart Tunnel List					P
Port Forwarding List Smart Tunnels Web Contents	and the second	eering-Smart-Tu					F	Engineering	
pup Policies App namic Access Poli	plication ID	Process Name	OS	Hash Add Smart Tun	nel Entry	Add			
vanced PN Remote coal Users can Image Desktop Managy ate Management age Localization Server cced		Application OS: Process Na Hash (Opti	Win me: outlo (e.g. w	ook2010 dows ok.exe oord.exe)			'User Pol ed to	icies	
all							es/User	Policies	

After the Smart Tunnel list is defined, it should be associated with the group or user policy.

Figure 2. Associate Smart Tunnel list to group policy

$\Theta \cap \Theta$			Edit Internal Group Policy: Engineering	
General Portal	Bookmark List: URL Entry:	 ✓ Inherit ✓ Inherit 	C Enable O Disable	Manage
More Options	File Access Control	Innerit	C Enable O Disable	
	File Server Entry:	🗹 Inherit	O Enable O Disable	
	File Server Browsing:	Inherit	O Enable O Disable	
	Hidden Share Access:	Inherit	O Enable O Disable	
	Port Fowarding Control			
	Port Forwarding List:	🗹 Inherit	\$	Manage
			Auto Applet Download	
	Applet Name:	Inherit		
	Smart Tunnel			
	Smart Tunnel Policy:	🗌 Inherit	Network: Tunnel Option: Use tunnel for all network traffic	Manage
•	Smart Tunnel Application:	🗌 Inherit	Engineering-Smart-Tunnel-List	Manage
	Auto Sign-on Server:	🗹 Inherit	Smart Tunnel all Applications Auto Start	Manage
			Windows Domain Name (optional): Auto sign-on works only with Internet Explorer on Windows client or in Firefox on any platform.	
	ActiveX Relay	-		
	ActiveX Relay:	M Inherit	C Enable C Disable	
	More Options			¥
Find:		O Ne	xt O Previous	
			(Help) (Cancel) (OK)	

Note: Setting the above option to "auto-start" will automatically start Smart Tunnels upon logging into the Clientless SSL VPN portal page. Setting the option to "enable" requires starting Smart Tunnels manually from within the portal. Setting the option to "disables Smart Tunnels.

Note: Setting the option to "all applications" will tunnel all applications without choosing which executable an end user may invoke for external applications. This setting should be used only for debugging purposes.

Web Applications

Smart Tunnel can also be used to support remote access for complex web pages that are difficult to rewrite. The ASA administrator can edit the bookmark for the web application to enable Smart Tunnel option with a single checkbox (see Figure 3).

Note: Once a user has clicked on a bookmark link with Smart Tunnel enabled, other links in the browser windows (that are not rewritten) will go through the tunnel as well. If an administrator only wants traffic to the internal network to go through the tunnel, the administrator needs to configure a tunnel policy. This requires at least ASA Release 8.3, and the administrator is warned in ASDM every time a bookmark link with Smart Tunnel is enabled.

00	Add Bookmark
Bookmark Title:	Web Bookmarks
URL:	http :// wwwin-example.com
Preload Page (Optio	onal)
Preload URL:	http 🛟 ://
Wait Time:	(seconds)
Other Settings (Op	tional)
Subtitle:	
Thumbnail:	None 🗘 (Manage)
✓ Place this bo	ookmark on the VPN home page
Enable Smar	t Tunnel 🔞
000	Smart Tunnel Policy
if t cor are is s pol	abling smart tunnel for a URL may send all browser traffic er smart tunnel to the Security Appliance. he Security Appliance does not have full network nnectivity, the user may not able to browse web sites that r not reachable from the Security Appliance. In such cases, it suggested to use a explicit smart tunnel policy at the group licy or user level to control what traffic is sent through art tunnel.
	ОК

Figure 3. Smart Tunnel for Web Applications

Note: Smart Tunnel is associated with web bookmarks using either http or https. Other protocols such as CIFS, FTP, and the Java plug-ins such as RDP and VNC cannot use the Smart Tunnel.

Access Lists (web-type)

The ASA allows administrators to apply web-type access lists to permit or restrict access to specific web pages. The Web-Type ACL can include Access Control Entry (ACE) for Smart Tunnel.

In the example below, Smart Tunnel is allowed for any web site that ends with a google.com domain suffix (for example, <u>http://images.google.com</u>). Remaining webpages are denied access through Smart Tunnel, due to an implicit deny at the end of the ACL. The Web-Type ACL can also include ACE for TCP traffic. In the example below, TCP traffic from SSH native application will be allowed access to 192.168.100.0 subnet through the Smart Tunnel, and traffic to any other server will be denied.



General Portal	Name: Engineering						
 More Options 	Banner: 🗹 Inherit						
	More Options						
	Tunneling Protocols:	🗌 Inherit	Clientless SSL VPN	SL VPN Client	t 🗌 IPsec IKEv1	I IPsec IKE	/2 🗌 L2TP/IPsec
	Web ACL:	🗌 Inherit	Smart-Tunnel-ACL				* Manage
	Access Hours:	000		ACL Man	nager		
	Simultaneous Logins:	🗣 Add	• 🗹 Edit 📋 Delete 🕈 🗲	1 mm -	Q Find 🔀 Ass	ign	
	Restrict access to VLAN:	No	Address -Tunnel-ACL	Service	Action		Logging
	Connection Profile (Tunnel Group) Lock:	1 2	smart-tunnel://*.google.com	10 ssh	 Permit Permit 		_
	Maximum Connect Time:	3	<u>异</u> 2001:2000::/64	😰 ssh	🖌 Permit		
	Idle Timeout:						
	Timeout Alerts						
	Session Alert Interval:						
	Idle Alert Interval:						
	Configure alert text messages and visual	1					rt
			Help	Canc	el OK	2	
			Спер	Cane			

Tunnel Policy for Smart Tunnel

A tunnel policy for Smart Tunnel governs whether a connection is to be tunneled through the VPN gateway or goes directly to the destination. Similar to Split-Tunnel policy for Full-Tunnel VPN Client, there are three tunnel policies available:

Tunnel All: Default policy to tunnel traffic to all destination networks.

Tunnel Specified: Tunnels only networks specified by the network name.

Exclude Specified: Tunnels only networks that are outside the networks specified by the network name.

Note: When configuring the network for Tunnel Policy for Smart Tunnel, both the IP address and host name of the network must be entered.



General	Bookmark List:	🗹 Inherit					\$	Manage
More Options	URL Entry:	🗹 Inherit	🔘 Enable 🤇) Disable				
	File Access Control							
	File Server Entry:	🗹 Inherit	🔘 Enable 🤇) Disable				
	File Server Browsing:	🗹 Inherit	🔿 Enable 🔇) Disable				
	Hidden Share Access:	🗹 Inherit	🔿 Enable 🤇	Disable				
	Port Fowarding Control							
	Port Forwarding List:	🗹 Inherit					\$	Manage
			Auto Apple	t Download				
	Applet Name:	🗹 Inherit						
	Smart Tunnel							
	Smart runner		Network:	engineering	servers		:	1
	Smart Tunnel Policy:	🗌 Inherit	Tunnel Option:			ecified network	•	Manage
		-		Use smart to		Manage Smart Tunnel L		J
	Smart Tunnel Application:	🗌 Inherit				,		
	Auto Sign-on Server:	🗌 Inherit	Smart Tu Smart Tu	o Log Off Smart nnel Application nnel Auto Sign-	List			
				nnel Networks				
	ActiveX Relay		Add	Edit 📋 Del	ete 🛃 Assign	Find:	0 0 🗆 Ma	tch Case
	ActiveX Relay:	🗹 Inherit	Network	Name	Network IP	/ Host	Group Policies/User Policies Assigned to	
	More Options	_	engineer	ing-servers		100.0/255.255.255.0 ample.com	Engineering	
ind:		O Ne	×					
					Help	Cancel	ОК	

Note: Unlike Full-Tunnel VPN Client, the Tunnel Policy for Smart Tunnel can be specified using host names. This drastically reduces the Split-Tunnel list that needs to be configured. For example, administrator can enter *.example.com, instead of entering the list of all the IP subnets that belong to example.com.

Single Sign-On (SSO) For Smart Tunnel

Single Sign-On is supported when Smart Tunnel is enabled for web bookmarks. SSO is not supported when using the native client-server applications. ASA allows multiple SSO options for Clientless SSL VPN users. Please consult the [Ref-TBD] ASA SSO Solution Guide for a detailed overview and examples.

Auto Sign-On Servers for Basic/NTLM/FTP Authentication

Administrators can specify the server lists to which the Smart Tunnel will perform Auto Sign-On. ASA submits the Clientless SSL VPN username and passwords to the internal servers.

Note: When configuring network for Auto Sign-On server list for Smart Tunnel, both the IP address and hostname of the network must be entered.

00			Edit Internal Group Policy: Engineering
General	Bookmark List:	✓ Inherit	Anage
Portal More Options	URL Entry:	🗹 Inherit	O Enable O Disable
	File Access Control		
	File Server Entry:	✓ Inherit	O Enable O Disable
	File Server Browsing:	✓ Inherit	O Enable O Disable
	Hidden Share Access:	✓ Inherit	O Enable O Disable
	Port Fowarding Control		
	Port Forwarding List:	✓ Inherit	\$ Manage
			Auto Applet Download
	Applet Name:	✓ Inherit	
	Applet Name.	U innent	
	Smart Tunnel		
	Smart Tunnel Policy:	🗌 Inherit	Network: engineering-servers
		0	Tunnel Option: Use smart tunnel for the specified network
	Smart Tunnel Application:	🗌 Inherit	Engineering-Smart-Tunnel-List 🗘 Manage
			Smart Tunnel all Applications
	Auto Sign-on Server:	🗌 Inherit	Engineering-Auto-Sign-On 🗘 Manage
		_	Anage Smart Tunnel Lists
	ActiveX Relay ActiveX Relay:	✓ Inherit	Method to Log Off Smart Tunnel Session & Smart Tunnel Application List &
	More Options		Smart Tunnel Auto Sign-on Server List
	Inore options		Add Edit Delete Assign Find:
ind:		O Ne	Server List Name Server v1 Group Policies/User Policies Assigned to
ges saved success	- fully		Engineering-Auto-Sign-On wwwin-example.com
iges saved succes:		-	Smart Tunnel Networks *
			(Help) (Cancel) (OK)

Figure 6. Auto Sign-On Server List for Smart Tunnel

Form-Based Single Sign-On and Macro Substitution

Web bookmarks that require Form-based POST parameters can be configured to use Smart Tunnel. In addition, ASA Release 8.3 introduced the support of macro substitution as part of the POST parameters.

Figure 7. Form-Based Single-Sign-On with Smart Tunnel and Macro Substitution

		Add Bo	okmark
Bookmark Title:	Exchange 2003 with Smart Tunnel		
URL:	https :// mail.example.com	n/exchweb/bin/auth/	owaauth.dll
eload Page (Opti	onal)		
Preload URL:	http 🛟 ://		
Wait Time:	(seconds)		
wait Time:	(seconds)		
her Settings (Op	otional)		
Subtitle:			
Thumbnail:	None	Manage	\supset
Place this b	ookmark on the VPN home page		
Enable Sma			
e chable shia			
Advanced Opti	ons		
A second s			
A second s	ons 🔾 Get 🛛 💿 Post ←	_	
A second s	🔾 Get 🛛 💿 Post 🔶		
URL Method:	🔾 Get 🛛 90st ←		
URL Method: Post Paramete	🔾 Get 🛛 90st ←	V	ilue
URL Method: Post Paramete Add Z Ec	🔾 Get 🛛 90st ←		ilue tps://mail.example.com/exchang
URL Method: Post Paramete Add 2 Ed Name	🔾 Get 🛛 90st ←	ht EX	tps://mail.example.com/exchang (AMPLE\CSCO_WEBVPN_USERNAM
URL Method: Post Paramete Add 2 Ed Name destination username password	🔾 Get 🛛 90st ←	ht EX	tps://mail.example.com/exchang (AMPLE\CSCO_WEBVPN_USERNAM SCO_WEBVPN_PASSWORD
URL Method: Post Paramete Add 2 Ec Name destination username password SubmitGrade	⊖ Get	ht EX	tps://mail.example.com/exchang (AMPLE\CSCO_WEBVPN_USERNAM
URL Method: Post Paramete Add 2 Ed Name destination username password	🔾 Get 🛛 90st ←	ht EX	tps://mail.example.com/exchang (AMPLE\CSCO_WEBVPN_USERNAM SCO_WEBVPN_PASSWORD
URL Method: Post Paramete Add 2 Ec Name destination username password SubmitGrade	⊖ Get	ht EX	tps://mail.example.com/exchang (AMPLE\CSCO_WEBVPN_USERNAM SCO_WEBVPN_PASSWORD
URL Method: Post Paramete Add 2 Ec Name destination username password SubmitGrade	⊖ Get	ht EX	tps://mail.example.com/exchang (AMPLE\CSCO_WEBVPN_USERNAM SCO_WEBVPN_PASSWORD
URL Method: Post Paramete Add 2 Ec Name destination username password SubmitGrade	⊖ Get	ht EX	tps://mail.example.com/exchang (AMPLE\CSCO_WEBVPN_USERNAM SCO_WEBVPN_PASSWORD
URL Method: Post Paramete Add 2 Ec Name destination username password SubmitGrade	⊖ Get	ht EX	tps://mail.example.com/exchang (AMPLE\CSCO_WEBVPN_USERNAM SCO_WEBVPN_PASSWORD
URL Method: Post Paramete Add 2 Ec Name destination username password SubmitGrade	⊖ Get	ht EX	tps://mail.example.com/exchang (AMPLE\CSCO_WEBVPN_USERNAM SCO_WEBVPN_PASSWORD
URL Method: Post Paramete Add 2 Ec Name destination username password SubmitGrade	⊖ Get	ht EX	tps://mail.example.com/exchang (AMPLE\CSCO_WEBVPN_USERNAM SCO_WEBVPN_PASSWORD
URL Method: Post Paramete Add 2 Ec Name destination username password SubmitGrade	⊖ Get	ht EX	tps://mail.example.com/exchang (AMPLE\CSCO_WEBVPN_USERNAM SCO_WEBVPN_PASSWORD
URL Method: Post Paramete Add 2 Ec Name destination username password SubmitGrade	⊖ Get	ht EX	tps://mail.example.com/exchang (AMPLE\CSCO_WEBVPN_USERNAM SCO_WEBVPN_PASSWORD
URL Method: Post Paramete Add 2 Ec Name destination username password SubmitGrade	⊖ Get	ht EX	tps://mail.example.com/exchang (AMPLE\CSCO_WEBVPN_USERNAM SCO_WEBVPN_PASSWORD
URL Method: Post Paramete Add 2 Ec Name destination username password SubmitGrade	⊖ Get	ht EX	tps://mail.example.com/exchang (AMPLE\CSCO_WEBVPN_USERNAM SCO_WEBVPN_PASSWORD
URL Method: Post Paramete Add 2 Ec Name destination username password SubmitGrade	⊖ Get	ht EX	tps://mail.example.com/exchang (AMPLE\CSCO_WEBVPN_USERNAM SCO_WEBVPN_PASSWORD
URL Method: Post Paramete Add 2 Ec Name destination username password SubmitGrade	⊖ Get	ht ED	tps://mail.example.com/exchang (AMPLE\CSCO_WEBVPN_USERNAM SCO_WEBVPN_PASSWORD

External Portal Page

The External Portal Page feature on the ASA allows the administrator to bypass the main Clientless portal and redirect the user to a custom URL. ASA Release 8.3 introduced the feature to enable Smart Tunnel for this external portal page.

Figure 8. Smart Tunnel for External Portal Page

Configuration > Remo	te Access VPN > Clientless SSL VI	PN Access > Portal > Customization
Customization Objects	000	Edit Customization Object
Configure Customization		
This parameter is enforce	General	✓ Enable External Portal
customization of the Logi	▼ Logon Page	
	Title Panel	
🕈 Add 🗹 Edit 📋 Delet	Language Logon Form	Portal URL: http://wwwin-example.com
Customization	Logon Form Fields Order	
Template	Informational Panel	Edit Bookmark
DfltCustomization	Copyright Panel	
Doctors_Customization Engineering_Customization	▼ Portal Page	
Chymeenne costomzadon	Title Panel	To create a new bookmark, select an option from the following:
	Toolbar	• URL with GET or POST method
	Applications Custom Panes	This is the traditional bookmark using the GET method, or the POST method with par
	Home Page	
	Timeout Alerts	O Predefined application templates (Microsoft OWA, Citrix XenApp)
	Logout Page	This option simplifies bookmark creation with users selecting a predefined ASDM ter
	External Portal Page	values for certain well-defined applications like Microsoft OWA 2010 and Citrix XenA
	~	O HTML form auto-submit
		This option lets you create bookmark for any complex auto sign-on application. It w
		1- Define the bookmark with some basic initial data and without the post parameter
		group policy or user.
		2- Edit the bookmark in ASDM again. Use the capture function to capture the SSL VP
		Create Bookmark
	00	Add Bookmark
Find:		
OnScreen Keyboard	100	
Specify when OnScreen Ke	URL: http 🗘	:// wwwin-example.com
Do not show OnScree	Preload Page (Optional)	
O Show only for the log		
	Preload URL: http 🛟	Ĵ ://
Show for all portal pa	Wait Time: (se	econds)
	🔶 🗹 Enable Smart Tunnel	0
cessfully.		
cessiuny.		Help Cancel OK

Note: The VPN Group-Policy also has an attribute, "Home-page URL," under the Customization panel. This option should be used only when a unified homepage is needed for both the AnyConnect Client and Clientless SSL VPN. If the homepage is used exclusively for Clientless SSL VPN, the External Portal Page (Figure 4 above) is preferred. The External Portal Page also supports Form-Based Single Sign-On.

Figure 9. Smart Tunnel for Homepage URL

000			Edit Internal Group Policy: Engineering	
General Portal More Options Customization Login Setting Single Signon VDI Access Session Settings	Portal Customization: Homepage URL (optional): Use Smart Tunnel for Homepage:	 ✓ Inherit ☐ Inherit ☐ Inherit 	http :// wwwin-example.com/internal-page.htm Image: Assistance Image: Disable Image: Disable Image: Disable	
	Access Deny Message:	🗹 Inherit		

Deployment Considerations

Security Implications

Legacy port forwarding technology required the administrator to manually enter local and remote port information for each application. The user was then instructed to connect to the local port using the application. Some administrators considered this a security risk, because any other malicious application could misuse that open port to connect to the private network.

With the implementation of a Smart Tunnel, the administrator enters the process name and path, instead of the port numbers. Smart Tunnel does not allow any other application traffic.

A malicious program would have to determine the specific process that is allowed to use the Smart Tunnel, and then masquerade as that process. This is more complicated compared to scanning for open ports. Additionally, there is an option to validate the checksum of the executable before allowing access to the Smart Tunnel.

In addition, the introduction of a Tunnel Policy and Web-Type ACLs for Smart Tunnel further reduces the attack vector by limiting the internal networks available for the Smart Tunnel. Hence, the security risk associated with Port Forwarding technology does not apply to the Smart Tunnel.

Note: It is recommended to enable cache-cleaner when using Smart Tunnels. It will erase any sensitive content that might be saved in the browser cache, and will also log out the user when all browser windows are closed.

Protected Mode for Windows

When using Windows, it is recommended to add the ASA to the trusted zone. Starting from ASA 8.3, the users will receive a prompt to accept Smart Tunnel start if the ASA is not in the trusted zone. Only when the user responds positively, Smart Tunnel will operate correctly.

By default, Internet Explorer runs in protected mode when it is not in a trusted Internet zone. This is to make sure that software spawned from the browser (malicious or otherwise) cannot affect the behavior of other applications with higher privileges.

For example, if the ASA resides in a non-trusted zone, a Smart Tunnel started from it cannot change the behavior of the Lotus Sametime (because the Lotus Sametime is likely running at a higher integrity level). This is not a design flaw or defect, but helps ensure the protection of the user. The user has the option of turning off protected mode if he or she does not want to use this feature.

Proxy Servers

Proxy Server Between the End Point and the ASA

Smart Tunnel honors the proxy settings in the browser when the endpoint accesses the ASA through a proxy server. However, Proxy Automatic Configuration (PAC) files are not supported. In the case of proxies that require authentication, only basic digest authentication is supported.



Proxy Server Behind the ASA

In some deployments, the administrator may choose to place a proxy server between the ASA and the remote destination network. These proxies sit behind the ASA. Only the Clientless SSL VPN content rewriter honors the proxy configuration. The ASA will not relay non-http based traffic, such as those from Java applets, plug-ins, and Smart Tunnels.



Customization

Group Policy and User Policy

The Smart Tunnel application list and Web bookmarks can be applied per Group Policy or User Policy. For example, it is possible to have one set of Smart Tunnel applications for Engineering, and have entirely different set of applications for Marketing.

Dynamic Access Policy (DAP)

Dynamic Access Policy on the ASA applies customized security policy based on user identity and device posture status. However, the DAP only includes web bookmarks that have Smart Tunnel enabled. Currently, it is not possible to apply different Smart Tunnel application list or Tunnel policy based on DAP record.

Troubleshooting Common Problems

Smart Tunnel does not work with Internet Explorer.

"Failed to start Smart Tunnels."

- 1. Add the ASA to the list of Trusted Sites⁶
- 2. Allow Active-X controls:

When this problem appears, the browser displays a new window with the message:

"To protect your security, Internet Explorer has restricted this webpage from running scripts or ActiveX controls that could access your computer. Click here for options..."

⁶ Trusted Sites: http://www.microsoft.com/windows/ie/ie6/using/howto/security/settings.mspx

You may check the option "Do not show this message again," then click OK. The page will then display without ActiveX content.

To view the JavaScript or the ActiveX content on the page and see your menus working, you will have to rightclick the Information Bar that appeared at the top of the page, and select "Allow Blocked Content." After this, you will be prompted with a message box that reads "Are you sure you want to let the file run active content?"

Smart Tunnel does not work with Firefox or Java.

"Failed to start Smart Tunnels": Please consult the respective ASA configuration guide to ensure that the version of Firefox is supported and that you have the required Java JRE version. Also, try disabling add-ons within Firefox and retry.

Smart Tunnel is started, but could not connect to the corporate resources.

Recheck the web-type ACL. There is an implicit deny-all at the end of your ACLs. Remember that Smart Tunnel is governed by the ACE that starts as: smart-tunnel://, not http://.

Get additional help.

You can contact Cisco Technical Assistance Center (TAC) for additional help.

- Please note the nature of the problem when reporting issues. How did it not work? Did it crash? Did it fail to start? Did the Web browser show an error message that says XXX?
- Please provide detail steps to reproduce, including what has been configured, and more.
- Please provide any error message seen anywhere.
- Please examine logs, which can be found at the local machine's event viewer (Windows) or /tmp (other platforms).
- For Smart Tunnel bookmarks, please note whether any external process is spawned as a result of bringing up the page.

Conclusion

Smart Tunnel helps enable highly secure remote access for native client-server applications and complex web pages. It is the preferred solution for allowing access from non-corporate assets, as it does not require the administrative rights, and it avoids the installation of a Full-Tunnel VPN Client on the endpoint.

Smart Tunnel supports multiple configurable options to customize the security policy, while supporting a simplified user experience.

Appendix A1: Finding Application Process Names on Windows

When trying to determine the process names that are required for the smart tunnel to work properly, it is important to understand how a process is spawned, as the parent process of each process must be allowed access to the tunnel. For example, to allow telnet.exe access to the tunnel, if a user opens a Command prompt (cmd.exe) and then types "telnet," both cmd.exe and telnet.exe have to be allowed access to Smart Tunnel.

Process Explorer can be used to determine what processes are involved in launching of an executable. In the following example, cmd.exe and telnet.exe are involved in launching of telnet. Double-clicking an entry also shows the information for a process, including its parent process. Note that Process Explorer updates dynamically, and you can watch the sequence of process launch events in real time as well.

Process	PID	CPU	Description	Company Name
🕢 tedit.exe	4384		TEdit	Captain Lion
🐼 devenv.exe	5736		Microsoft Visual Studio 2005	Microsoft Corporation
WINWORD.EXE	5888		Microsoft Office Word	Microsoft Corporation
EXCEL.EXE	1360		Microsoft Office Excel	Microsoft Corporation
📿 tedit.exe	2916		TEdit	Captain Lion
wireshark.exe	4336		Wireshark	The Wireshark develop
🔪 📿 procexp.exe	4504	2.21	Sysinternals Process Explorer	Sysinternals - www.sys
🔫 🖃 📷 cmd.exe	2100		Windows Command Processor	Microsoft Corporation
🛃 telnet.exe	5508		Microsoft Telnet Client	Microsoft Corporation
🖉 tedit.exe	5948		TEdit	Captain Lion
MpCmdRun.exe	5852		Microsoft Malware Protection Comm	Microsoft Corporation
CSISS EXE	4984		Client Server Buntime Process	Microsoft Cornoration

telnet.exe:550	18 Properties		_0
TCP/IP	Security	Environment	Strings
Image File - Version: Time: Path: C:\Windo Command telnet Current dir		oft Corporation	Threads
User: Started: Comment: Data Execut	cmd.exe(2100) PIGLET\lion 10:42:38 PM 2/8/201	tatus: DEP (permanent)	Verify Bring to Front Kill Process
		ŌK	Cancel

- Cisco does not decide what process a customer should allow access to the Smart Tunnel. To determine the processes that are involved in an application, the administrator needs to contact the vendor of the application, as Cisco has no knowledge regarding how those applications work.
- One implementation tip that can be employed is to allow all executables access. Start the application and use Process Explorer to identify each process that has the Smart Tunnel dynamic link library loaded.

Appendix A2: Popular Applications

Application	os	Process/Path
Command Prompt	Windows	cmd.exe
Lotus Notes	Windows	Nfileret: nfileret.exe LotusnInotes: nInotes.exe Lotusntaskldr: ntaskldr.exe
Lotus Sametime	Windows	connect.exe
Outlook Express	Windows	msimn.exe
Outlook	Windows	outlook.exe
PerForce	Windows	p4v.exe
RDP	Windows	mstsc.exe
VMWare View Client	Windows	VMViewClient - wswc.exe VM_WSNM_USB - wsnm_usbctrl.exe VM_WSNM - wsnm.exe
Firefox	Mac	/Applications/Firefox.app/Contents/MacOS/firef ox-bin
Safari	Мас	/Applications/Safari
Terminal	Мас	"terminal open -a MacTelnet"
VNC	Мас	~/bin/vnc

CLI:

smart-tunnel list Engineering-List VNC ~/bin/vnc platform mac smart-tunnel list Engineering-List CommandPrompt cmd.exe platform windows smart-tunnel list Engineering-List OutlookExpress msimn.exe platform windows smart-tunnel list Engineering-List Firefox/Applications/Firefox.app/Contents/MacOS/firefox-bin platform mac smart-tunnel list Engineering-List Lotusntaskldr ntaskldr.exe platform windows smart-tunnel list Engineering-List LotusnInotes nInotes.exe platform windows smart-tunnel list Engineering-List Lotusnfileret nfileret.exe platform windows smart-tunnel list Engineering-List Outlook2010 outlook.exe platform windows smart-tunnel list Engineering-List Terminal "terminal open -a MacTelnet" platform mac smart-tunnel list Engineering-List PerForce p4v.exe platform windows smart-tunnel list Engineering-List RDP mstsc.exe platform windows smart-tunnel list Engineering-List Safari/Applications/Safari platform mac smart-tunnel list Engineering-List LotusSametime connect.exe platform windows smart-tunnel list Engineering-List VMViewClient wswc.exe platform windows smart-tunnel list Engineering-List VM_WSNM_USB wsnm_usbctrl.exe platform windows smart-tunnel list Engineering-List VM_WSNM wsnm.exe platform windows

Appendix A3: Smart Tunnel for VMWare View Client

Step 1. Enable Clientless SSL VPN on the outside interface.

Home 🖧 Configuration 🔯 Monit	oring 🔚 Save 🔇 Refre	sh 🔇 Back 🚫 Forward 🢡 Help		
Remote Access VPN 🗗 🕂 🗙	Configuration > Remote	Access VPN > Clientless SSL VPN Access > Co	nnection Profiles	
Introduction Network (Client) Access AnyConnect Connection Profiles	Access Interfaces	tless SSL VPN access.		
IPsec Connection Profiles	Interface	Allow Access		
Group Policies	outside			
Dynamic Access Policies	inside			
AnyConnect Customization/Local	Access Port: 443			
AnyConnect Client Profile				
AnyConnect Client Settings				
Address Assignment				
Advanced Glentless SSL VPN Access	Click here to Assign Certificate to Interface.			
Connection Profiles	Login Page Setting			
Portal	Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWeb/			
Group Policies	Anow user to select connection prome, identified by its alias, on the login page, otherwise, berautweb			
D. Dumania Assass Delisian	Allow upor to optor int	ornal paceword on the login page		

Step 2. Configure Connection Profile for Clientless Access.

Select appropriate authentication server, DNS server and enable Clientless SSL VPN.

Home Configuration Monit	oring 🕞 Save 📿 Refresh			
Remote Access V/M D1 4 X Introduction Introduction Introduction Introduction Profiles Introduction Profiles Introduction Profiles	Advanced Advanced	Name: Alases: Authentication Method: AAA Server Group: DNS Server Group:	OefaultWEBVP O AAA O MicrosoftAD Use LOCAL DefaultDNS	
Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Advanced Source Desitop Manager Destroate Management Destroate Management DHCP Server MOS		Default Group Policy Group Policy:		demo.local Manage is an attribute of the group policy selected above.) ntless SSL VPN protocol

Step 3. Configure the Group Policy to apply a Smart Tunnel List for VMWare View Client:

The VMware View Client spawns processes wswc.exe, wsnm_usbctrl.exe, wsnm.exe. We create a Smart Tunnel List "VMWare_Apps" with all three processes. Check the "Auto-Start" option.

File View Tools Wizards Window Help		~ ~					Look For:
Home Cor Edit Internal Group	Policy: DfltGrpPolicy		🖆 Manage Smart	Tunnel Lists			
Britoduction Draw (Clent AryConnec More Options Draw (Clent AryConnec More Options Draw (Clent Draw (Clen	Boolmark List: URL Entry: File Access Control File Server Entry: File Server Browsing:	None O Enable O Enable O Enable O Disable O Enable O Disable	Method to log off sm	r, i.e. logoff the smart-t -tunnel logoff icon in the stion List	unnel when its parent pr	ocess, such as a	browser, terminates
AnyConnec AnyConnec AnyConnec AnyConnec Concel Concel Concel Connection	Hidden Share Access: Port Fowarding Control Port Forwarding List:	Enable Disable Insable Auto Applet Downlose	List Name VMWare_Apps	Application ID MM/ewClent M_WSNM_Usb M_WSNM	Process Name wowc.exe worm_usbctrl.exe worm.exe	05 Windows Windows Windows	Hash
	Applet Name: Smart Tunnel	Application Access	Edit Smar List Name: V	t Tunnel List MWare_Apps			
AAA/Local User Secure Desktop Certificate Man	Smart Tunnel Policy:	Network: Tunnel Option: Use tun	Application VMVIewCler VM_WSNM	t wswc.exe	e Window		Hash
경 Language Local 화 DHCP Server 해 DNS 경 Advanced	Smart Tunnel Application	VMWare_Apps	WI_WSNM	wsrm.ex	e Window	6	

Test: Clientless User Experience

From any web browser, the user navigates to the VPN gateway outside (Public) interface (for example, https://170.0.0.1). After authentication, Smart Tunnels will be automatically started and actively listening for the processes spawned by VMware View Client.

🖉 https://170.0.0.1/+CSCOE+/portal.	html - Windows Internet E				
C + https://170.0.0.1/+CSCOE+/p	ortal.html	V 😧 Cert	ificate Error 49 X Live Sear	ch	
2 Attps://170.0.0.1/+CSCOE+/portal	.html		⊡ • ⊠	🖶 • 🔂 Page •	
CISCO SSL VPN Service					
Home	Address http://]	Browse	
Web Applications					
Rowse Networks	Application Ac	ccess	Application Access Requirements and Recommendations		
Replication Access	These applications are auth Smart Tunnel:	norized to access			
2 AnyConnect	VMViewClient		To access applications remotely, you need the following prerequisites:		
NC VNC Connections	 VM_WSNM_Usb VM_WSNM 		 The corresponding links configured on the Application Access page. Remote servers configured for your use. 		
MetaFrame Access	Smart Tunnel has b	een started			
Telnet/SSH Servers	Per tunnel policy, all your browser traffic will		The client applications installed locally on your system.		
Post Plugin to post with preloaded page	be tunnele	d	* Each client application properly configured to communicate remotely with the server.		
Terminal Servers (Vista)	Gateway:	170.0.0.1	* Sun Microsystems J		
Servers	KBytes Sent: 0 Environment version 1.4 KBytes Received: 1 installed on your system				

After establishing the Clientless VPN with Smart Tunnels, the user manually launches the VMware View client, and authenticates with the VMware View Manager. They can then connect to the authorized desktops, using Microsoft RDP display protocol.

	ware View Client	
	Bayscribe Double-click to connect. Right-click for options. HIMSS_ThinApp_Demo Double-click to connect. Right-click for options.	
Ę	FollowMeDesktop Double-click to connect. Right-click for options.	Connect
	Display: Full Screen	Display Protocol PCoIP Logoff Vicrosoft RDP (default)
	<u>Connect</u> E <u>xi</u> t	Reset Desktop

Note: VMware View Manager also supports PC over Internet Protocal (PCoIP) display protocol. However, since the PCoIP protocol uses UDP for transport, it is not supported by the Smart Tunnel solution.

CLI:

dns server-group DefaultDNS

name-server 192.168.13.252

domain-name demo.local

webvpn

enable outside

smart-tunnel list VMWare_Apps VMViewClient wswc.exe platform windows

smart-tunnel list VMWare_Apps VM_WSNM_Usb wsnm_usbctrl.exe platform windows

smart-tunnel list VMWare_Apps VM_WSNM wsnm.exe platform windows

group-policy DfltGrpPolicy attributes

vpn-tunnel-protocol IPSec l2tp-ipsec svc webvpn

webvpn

smart-tunnel enable VMWare_Apps

tunnel-group DefaultWEBVPNGroup general-attributes

authentication-server-group MicrosoftAD



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA

C07-713780-00 09/12