ASA/PIX - Cisco IOS 라우터 LAN-to-LAN IPsec 터널 구성

목차

소개 사전 요구 사항 요구 사항 사용되는 구성 요소 표기 규칙 배경 정보 구성 네트워크 다이어그램 구성 ASDM을 사용한 구성 다음을 확인합니다. 문제 해결 문제 해결 명령 관련 정보

<u>소개</u>

이 문서에서는 PIX Security Appliance 7.x 이상 또는 내부 네트워크 하나가 포함된 ASA(Adaptive Security Appliance)에서 암호화 이미지를 실행하는 2611 라우터에 IPsec 터널을 구성하는 방법을 설명합니다. 고정 경로는 간소화를 위해 사용됩니다.

라우터와 PIX 간의 LAN-to-LAN 터널 컨피그레이션에 대한 자세한 내용은 <u>IPSec - 라우터</u>에서 PIX로 구성 을 참조하십시오.

PIX <u>Firewall과</u> Cisco VPN 3000 Concentrator 간<u>의 LAN-to-LAN</u> 터널 컨피그레이션에 대한 자세한 내용은<u>Cisco VPN 3000 Concentrator</u>와 PIX 방화벽 컨피그레이션<u>사이</u>의 LAN-to-LAN IPSec 터널 을 참조하십시오.

PIX<u>와 VPN Concentrator</u> 사이에 LAN-to-LAN 터널이 있는 시나리오에 대한 자세한 내용은 PIX 7.x<u>와 VPN 3000 Concentrator</u> 간 IPsec 터널 구성 예를 참조하십시오.

PIX 간 LAN-to-LAN 터널을 통해 VPN 클라이언트가 허브 PIX를 통해 스포크 PIX에 액세스할 수 있 는 시나리오에 대한 자세한 내용은 PIX<u>/ASA 7.x Enhanced Spoke-to-Client VPN with TACACS+</u> <u>Authentication Configuration</u> 예를 참조하십시오.

SDM을 <u>참조하십시오. PIX/ASA Security Appliance에서</u> 소프트웨어 버전 8.x를 실행하는 동일한 시 나리오에 대해 자세히 알아보려면<u>ASA/PIX와 IOS 라우터</u> 간 Site-to-Site IPsec VPN 구성 예

Configuration Professional을 <u>참조하십시오. ASA/PIX와 IOS 라우터 간 Site-to-Site IPsec VPN</u>

ASDM GUI를 사용하여 ASA 관련 컨피그레이션이 표시되고 Cisco CP GUI를 사용하여 라우터 관 련 컨피그레이션이 표시되는 동일한 시나리오에 대해 자세히 알아보려면 <u>예</u>를 참조하십시오.

<u>사전 요구 사항</u>

<u>요구 사항</u>

이 문서에 대한 특정 요건이 없습니다.

<u>사용되는 구성 요소</u>

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

• PIX-525(PIX 소프트웨어 버전 7.0 포함)

• Cisco 2611 라우터(Cisco IOS® 소프트웨어 릴리스 12.2(15)T13 포함)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

<u>표기 규칙</u>

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 규칙</u>을 참조하십시오.

<u>배경 정보</u>

PIX에서 access-list 및 nat 0 명령이 함께 작동합니다. 10.1.1.0 네트워크의 사용자가 10.2.2.0 네트 워크로 이동하면 액세스 목록을 사용하여 10.1.1.0 네트워크 트래픽을 NAT(Network Address Translation) 없이 암호화할 수 있습니다. 라우터에서 route-map 및 access-list 명령은 10.2.2.0 네트 워크 트래픽이 NAT 없이 암호화되도록 허용하는 데 사용됩니다. 그러나 동일한 사용자가 다른 곳 으로 이동하면 PAT(Port Address Translation)를 통해 172.17.63.230 주소로 변환됩니다.

이는 PAT를 통해 터널을 통해 트래픽이 PAT를 통과하지 못하도록 PAT Security Appliance에서 필 요한 컨피그레이션 명령 및 PAT를 통해 실행하기 위해 인터넷에 대한 트래픽입니다.

access-list nonat permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 nat (inside) 0 access-list nonat nat (inside) 1 10.1.1.0 255.255.255.0 0 0

<u>구성</u>

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: <u>명령 조회 도구(등록된</u> 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램



<u>구성</u>

이러한 컨피그레이션 예는 명령줄 인터페이스를 위한 것입니다. ASDM을 사용하여 구성하려면 이 문서<u>의 Configuration using Adaptive Security Device Manager (ASDM)</u> 섹션을 참조하십시오.

- <u>본사 PIX</u>
- <u>브랜치 라우터</u>

본사 PIX
HQPIX(config)# show run
PIX Version 7.0(0)102
names
!
interface Ethernet0
description WAN interface
nameif outside
security-level 0
ip address 172.17.63.229 255.255.255.240
interface Ethernet1
nameifinside
security-level 100
1p address 10.1.1.1 255.255.255.0
interface Ethernet2
shutdown
no nameif
no security-level
no ip address

interface Ethernet3 shutdown no nameif no security-level no ip address ! interface Ethernet4 shutdown no nameif no security-level no ip address 1 interface Ethernet5 shutdown no nameif no security-level no ip address ! enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname HQPIX domain-name cisco.com ftp mode passive clock timezone AEST 10 access-list Ipsec-conn extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 access-list nonat extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 pager lines 24 logging enable logging buffered debugging mtu inside 1500 mtu outside 1500 no failover monitor-interface inside monitor-interface outside asdm image flash:/asdmfile.50073 no asdm history enable arp timeout 14400 nat-control global (outside) 1 interface nat (inside) 0 access-list nonat nat (inside) 1 10.1.1.0 255.255.255.0 access-group 100 in interface inside route outside 0.0.0.0 0.0.0.0 172.17.63.230 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS protocol radius aaa-server partner protocol tacacs+ username cisco password 3USUcOPFUiMCO4Jk encrypted http server enable http 10.1.1.2 255.255.255.255 inside no snmp-server location no snmp-server contact snmp-server community public snmp-server enable traps snmp

```
crypto ipsec transform-set avalanche esp-des esp-md5-
hmac
crypto ipsec security-association lifetime seconds 3600
crypto ipsec df-bit clear-df outside
crypto map forsberg 21 match address Ipsec-conn
crypto map forsberg 21 set peer 172.17.63.230
crypto map forsberg 21 set transform-set avalanche
crypto map forsberg interface outside
isakmp identity address
isakmp enable outside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash sha
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
tunnel-group 172.17.63.230 type ipsec-121
tunnel-group 172.17.63.230 ipsec-attributes
pre-shared-key *
1
class-map inspection_default
match default-inspection-traffic
!
policy-map asa_global_fw_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect http
!
service-policy asa_global_fw_policy global
Cryptochecksum: 3a5851f7310d14e82bdf17e64d638738
: end
SV-2-8#
브랜치 라우터
BranchRouter#show run
Building configuration ...
Current configuration : 1719 bytes
! Last configuration change at 13:03:25 AEST Tue Apr 5
2005
```

```
! NVRAM config last updated at 13:03:44 AEST Tue Apr 5
2005
1
version 12.2
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname BranchRouter
!
logging queue-limit 100
logging buffered 4096 debugging
1
username cisco privilege 15 password 0 cisco
memory-size iomem 15
clock timezone AEST 10
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 11
encr 3des
authentication pre-share
group 2
crypto isakmp key cisco123 address 172.17.63.229
crypto ipsec transform-set sharks esp-des esp-md5-hmac
1
crypto map nolan 11 ipsec-isakmp
set peer 172.17.63.229
set transform-set sharks
match address 120
!
!
1
1
1
1
1
!
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
1
mta receive maximum-recipients 0
!
1
1
interface Ethernet0/0
ip address 172.17.63.230 255.255.255.240
ip nat outside
no ip route-cache
no ip mroute-cache
half-duplex
crypto map nolan
```

```
interface Ethernet0/1
ip address 10.2.2.1 255.255.255.0
ip nat inside
half-duplex
ip nat pool branch 172.17.63.230 172.17.63.230 netmask
255.255.255.0
ip nat inside source route-map nonat pool branch
overload
no ip http server
no ip http secure-server
ip classless
ip route 10.1.1.0 255.255.255.0 172.17.63.229
1
1
access-list 120 permit ip 10.2.2.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 130 deny ip 10.2.2.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 130 permit ip 10.2.2.0 0.0.0.255 any
!
route-map nonat permit 10
match ip address 130
!
call rsvp-sync
!
!
mgcp profile default
1
dial-peer cor custom
!
1
!
!
!
line con 0
line aux 0
line vty 0 4
login
!
!
end
```

<u>ASDM을 사용한 구성</u>

이 예에서는 ASDM GUI를 사용하여 PIX를 구성하는 방법을 보여 줍니다. 브라우저 및 IP 주소가 10.1.1.2인 PC가 PIX의 내부 인터페이스 e1에 연결됩니다. PIX에서 http가 활성화되어 있는지 확인 합니다.

이 절차에서는 본사 PIX의 ASDM 컨피그레이션을 설명합니다.

1. PC를 PIX에 연결하고 다운로드 방법을 선택합니다



ASDM은 PIX에서 기존 컨피그레이션을 로드합니다

			- Interface State	15		
General License			Interface	IP Address/Mask	Line Li	nk Current Kbps
Host Name:						
PD/ Version:	Device U	ptime:				
ASDM Version:	Device T	ype:				
Total Flash:	Status		_		×	
VPN Status	-				(a.)	
IKE Tunnels:	7	Please wait while ASDM is it device.	bading the current	configuration from yo	ur	
		Initializing Monitor modules.	•		Total	
Memory Memory Usa	1					
Memory Usa	•		input Kbps	. <mark>e</mark> c	Julput Kbpic	

이 창에서는 모니터링 기기 및 메뉴를 제공합니다

1 Cisco ASDM 5.0 for PIX - 10.1.1.1	
File Roles Bearch Options Tools Wizards Help	Refresh Save Help
- Device Information -	Interface Status
General License	Interface IP Address/Mask Line Link Current Kbps
Host Name: SV-2-8.cisco.com PIX Version: 7.0(0)102 Device Uptime: 0d 0h 24m 50s ASDM Version: 5.0(0)73 Device Type: PDK 525 Firewall Mode: Routed Context Mode: Single Tebl Fireb: 15 MP Tebl Memory 255 MP	inside 10.1.1.1/24 O up O up 1
LOGAL PERSIT. TO MIS LOGAL METTORY, 200 MES	Select an interface to view input and output Kbps
VPN Status IKE Tunnels: 0 IPSec Tunnels: 0	Traffic Status Connections Per Second Usage
System Resources Status CPU CPU Usage (percent) 01 02 04:57:46 CPU Usage (MB) 67:46 04:57:46 04:57:46 CPU Usage (MB) 04:57:46 04:56:36	0.5 0.5 0.5 0.5 0.5 0.5 0.5 0.5
- Latest ASDM Syslog Messages Syslog Disabled	Configure ASDM System Filter
Device configuration loaded successfully.	<admin> NA (15) 😡 🏭 🔒 4/5/05 4:57:46 AM UTC</admin>

2. Configuration > Features > Interfaces를 선택하고 Add for new interfaces 또는 Edit for an existing configuration을 선택합니다

Configuration + Feature	nes×interfaces) X Pa BA BA B	60					-	_	
Interfac	e Name	Enabled	Security	IP Address	Submet Mask	Management	MTU		D
Ethernett	inside	Yes	100	10.1.1.1	255.255.255.0	No.	1500		
Ethernet0	outside	Yes	0	172.17.63.229	255 255 255 240	No	1500	WAN interface	
Ethernet2		No			1	No			
Ethernet3		No				No			
Ethernet4		No.				No			
Ethernet5		No			1	No			-
Ethemet5		No				No			

3. 내부 인터페이스의 보안 옵션을 선택합니다

Cisco ASDM 5.	0 for PDX - 10.1.1.1	ante Halo						_10 X
Hone C	Configuration Monitoring	Back Ferward	Q Q Search Refresh	Save Help			Creat	e Systems
Features	Configuration > Features >	Security Policy > Access	Rules			_		
Piterfaces	Access Rules C A	4 配配配配码 AA Rules C Filter Ru AI Interfaces 王	les C Service Policy R; Show All	les				
Security Policy	# Rule Action	Source	Destination	Rule Applied	Interface	Service	Log Level	Add
245	1 2 4	any	any any	al incoming ins	side	D (p	Ingervas	Edit
NAT						Page 1	_	Delete
<u> 3</u>								
VPN								
Routing								
Building Blocks								
3. Device								
Administration								
Properties								
	1.1.							
	 Anow transc 	 Deny transc 	1	1		· show Summary	 Show Detail 	
Wizards 🕗		Apply	Reset	Advance	d			
				cisco	NA (2)		A 16/05 3 25:25	PM AEST

4. NAT 컨피그레이션에서 암호화된 트래픽은 NAT-exempt이며 다른 모든 트래픽은 외부 인터페 이스에 대한 NAT/PAT입니다

	arcia opposis ro	ors vecaros	пер	0			Č in	
Hone C	Configuration M	Initoring	Dack Forward d	Q Q Search Refresh :	Save Help			السط
eatures	Configuration - Fr	ratures > NAT	+ Translation Rules					
	🔹 🗄 🌾 🖬	1 2 2	66669					
serfaces	Enable traf	ic through the	firewall without address	translation				
6,	Translation	Rules	C Translation Exemp	tion Rules				
surity Policy	Show Rules f	or Interface: 🗍	NI Interfaces	Show All				
NAT	Rule		Original			Translated		Add
53	Type f	ntectace	Source Network	Destination Network	Interface	Address	DNS Rewrite	Edt
VPN	L insi	de d	10.1.1.0/24	🔹 any	outside	172.17.63.2290nterface PAT)	No	Delete
.7.	Ingi	te Lt	10.1.1.0024	any any	outstate	172.17.03.2230memaca PAU	NO	Longi
*35								
Routing								
20								
Contraction of the second								
ang biocks								
8								
Ch								
Device								
Device								
Device invistration								
Device inistration								
Device inistration operties								
operties								
operties								
operties								
operties	<u>.</u>							
operties	+ √+ Static NA ⁰	- III Dy	namic NAT 🖓 Stat	e Policy NAT 🖓 D	 ynamic Policy N	AT	Manage Pools	
operties	• Static NAT	r 📲 Dyr	namic NAT 🖓 Stat	e Policy NAT 🖓 D	J mamic Policy N	AT I	Manage Pools.,	

5. VPN > General(일반) > Tunnel Group(터널 그룹)을 선택하고 터널 그룹을 활성화합니다



6. VPN > IKE > Global Parameters를 선택하고 외부 인터페이스에서 IKE를 활성화합니다

Home	Configuration Montoring Back	Forward Search Retresh Save Heip	Cisco Syst
Features	Configuration > Features > VPN > 8/2	- Olobal Parameters 19 1 우리	
Interfaces Interf	General General Client Update Tunnel Group Group Policy - Default Tunnel Gateway KE - Default Connel Gateway - Policies - Policies - Policy - Policy	Global Parameters Enable IKE Interface Interface Dutside Yes Discipline Enable IPSec over NAT-T Nat Transparency Enable IPSec over NAT-T Nat Transparency Enable IPSec over NAT-T National IPSec over TCP Enable IPSec over TCP Enable IPSec over TCP Enable IPSec over TCP Identity to Be Sent to Peer Identity: Address Key Id String: Disable Inbound aggressive mode connections Alert peers before disconnecting Wait for all active sessions to voluntarily terminate before rebooting Apply: Reset	n l

7. VPN > IKE > Policies를 선택하고 IKE 정책을 선택합니다



8. VPN > IPsec > IPsec Rules를 선택하고 로컬 터널 및 원격 주소 지정을 위해 IPsec을 선택합 니다

Elie Rules	o for PEX - 10.1.1.1		-21					_ [D] ×
Hone C	Configuration Monitoring Back	Forward	Q	Refresh Save	? Help		E.	ste Statens dia ada
Features	Configuration = Features = VPN = IPSec =	IPSec Ru	es					
interfaces		IPSec Ru Use the	iles Rules menu,	the toolbar, or the right r	nouse button to add, edit or	felete rules.		
Security Policy	- Group Policy	*	Action	PD(Side Host/Network	Remote Side HostNetwork	Service	Tunnel Po	Add
品		1	protect	F 10.1.1.0/24	d ⁰ 10.2.2.0/24	💌 ip	outside:static-	Edž
Rouling Building Blocks Building Blocks Building Blocks Berkee Administration	Global Parameters Certificate Group Matching Project P							Delete
Wizards 🖉				Apply	Reset	now Summary	Show Detail	
				c	isco NA (2)	6	A 46/05 3 33:	35 PM AEST

9. VPN > IPsec > Tunnel Policy를 선택하고 터널 정책을 선택합니다

Ete Roles Be	ofer PIX = 10.1.1.1.1 erch Options Tools Wigards Help							_D×
Home	Configuration Montoring Eack	Porward Search	n Retresh	Save Help			C	SCO SYSTEMS
Features Interfaces Security Policy NAT Security Policy Security Policy Policy Policy Policy Policy Security Policy Policy Policy Security Policy P	Configuration > Features = VPN > IPSec General VPN System Options Client Update Tunnel Group Doup Policy Default Tunnel Gateway KE Global Parameters Policies Certricate Group Matching Policy Prolicy	Tunnel Policy Tunnel Policy Spacify Tunnel Policy Interface outside t	olicy Type & Priority Static - 21	Transform Set avalanche	Peer 172.17.63.230	Connection Type Bidirectional	SA 01.000.00 cr	Add Edtl Delete
Vicaros /	J			cisco	NA (2)	a 🔒 🔒 🔒	4/6/05 3:34:	45 PM AEST

10. VPN > IPsec > Transform Sets를 선택하고 Transform set를 선택합니다

Cisco ASDM S File Roles Bi	to for PDX-10.11.1.1 earth: Options: Tools: Wizards: Help						<u>_ 0 ×</u>
Home	Configuration Monitoring Back	Forward Search	Refresh	Save Help			Cisco Systems
Features	Centriputation - Features - VFN - Place Centriputation - Features - VFN - Place Centriputation - Client Update - Client U	Transform Sets Transform Sets Specify Transform Sets Name esp-DES-MD5 ESP-DES-MD5 ESP-AES-128-MA ESP-AES-128-MA ESP-AES-128-MA ESP-AES-256-MD5	Node Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel	ESP Encryption DES DES 3DES 3DES AES-128 AES-128 AES-128 AES-128 AES-128 AES-128 AES-128 AES-128 AES-256 AES-256	ESP Authentication MD5 SHA MD5 SHA MD5 SHA MD5 SHA MD5 SHA MD5 SHA MD5	AH Authentication None None None None None None None No	Add Edt Delete
Wizards /							

11. Routing(**라우팅) > Routing(라우팅) > Static Route(고정 경로)를** 선택하고 게이트웨이 라우 터에 대한 고정 경로를 선택합니다. 이 예에서 고정 경로는 간소화를 위해 원격 VPN 피어를 가리킵니다

🖆 Cisco ASDM 5.0) for PIX - 10.1.1.1							
File Rules Sea	onfiguration Montoring	nds Help	Q Search R	etresh Save	З			Cesco Systems
Features	Configuration = Features = 5 Configuration = Features = 5 Reuting - RIP - Provy ARPs B - CoSPF B - COSPF	Routing - Routing - Sis Ref & S & C & C Static Route Specify static rout Interface outside	bc Route es. IP Address 0.0.0.0	Netmask 0.0.0.0	Gateway IP 172.17.63.230	Metric 1	Tunneled No	Add Edit Delete
	,				cisco NA	(2)	AR	105 3:39:36 PM AEST

<u>다음을 확인합니다.</u>

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 show 명령을 지원합니다. OIT를 사용하여 show 명령 출력의 분석을 봅니다.

- show crypto ipsec sa 2단계 보안 연결을 표시합니다.
- show crypto isakmp sa 1단계 보안 연결을 표시합니다.

<u>문제 해결</u>

ASDM을 사용하여 로깅을 활성화하고 로그를 볼 수 있습니다.

- Configuration(구성) > Properties(속성) > Logging(로깅) > Logging Setup(로깅 설정)을 선택하 고 Enable Logging(로깅 활성화)을 **선택한** 다음 Apply(적용)를 클릭하여 로깅을 활성화합니다.
- Monitoring(모니터링) > Logging(로깅) > Log Buffer(로그 버퍼) > On Logging Level(로깅 레벨)을 선택하고 Logging Buffer(로깅 버퍼)를 선택한 다음 View(보기)를 클릭하여 로그를 확인합니다.

<u>문제 해결 명령</u>

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 show 명령을 지원합니다. OIT를 사용하여 show 명령 출력의 분석을 봅니다.

참고: debug 명령을 사용하기 전에 디버그 <u>명령에 대한 중요 정보</u>를 참조하십시오.

- debug crypto ipsec 2단계의 IPsec 협상을 표시합니다.
- debug crypto isakmp 1단계의 ISAKMP 협상을 표시합니다.
- debug crypto engine 암호화된 트래픽을 표시합니다.
- clear crypto isakmp 1단계와 관련된 보안 연결을 지웁니다.
- clear crypto sa 2단계와 관련된 보안 연결을 지웁니다.
- debug icmp trace 호스트의 ICMP 요청이 PIX에 도달하는지 여부를 표시합니다. 이 디버그를 실행하려면 컨피그레이션에서 ICMP를 허용하려면 access-list 명령을 추가해야 합니다.
- logging buffer debugging(로깅 버퍼 디버깅) PIX를 통과하는 호스트에 대해 설정 및 거부된 연 결을 표시합니다. 정보는 PIX 로그 버퍼에 저장되며 show log 명령을 사용하여 출력을 볼 수 있 습니다.

<u>관련 정보</u>

- <u>가장 일반적인 L2L 및 원격 액세스 IPSec VPN 문제 해결 솔루션</u>
- <u>Cisco PIX 방화벽 소프트웨어</u>
- <u>Cisco Secure PIX Firewall 명령 참조</u>
- <u>보안 제품 필드 알림(PIX 포함)</u>
- <u>RFC(Request for Comments)</u>