ASA 7.x/PIX 6.x 이상: 포트 구성 열기/차단 예

목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>관련 제품</u> <u>표기 규칙</u> <u>구성</u> <u>네트워크 다이어그램</u> <u>포트 구성 차단</u> <u>포트 구성 추단</u> <u>포트 구성 열기</u> <u>ASDM을 통한 구성</u> <u>다음을 확인합니다.</u> <u>문제 해결</u> 관련 정보

<u>소개</u>

이 문서에서는 보안 어플라이언스에서 http 또는 ftp와 같은 다양한 유형의 트래픽에 대한 포트를 열 거나 차단하는 방법에 대한 샘플 컨피그레이션을 제공합니다.

참고: "포트 열기" 및 "포트 허용" 용어는 동일한 의미를 제공합니다. 마찬가지로 "포트 차단" 및 "포 트 제한"도 같은 의미를 제공합니다.

<u>사전 요구 사항</u>

<u>요구 사항</u>

이 문서에서는 PIX/ASA가 구성되어 제대로 작동한다고 가정합니다.

<u>사용되는 구성 요소</u>

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

• 버전 8.2(1)를 실행하는 Cisco 5500 Series ASA(Adaptive Security Appliance)

• Cisco ASDM(Adaptive Security Device Manager) 버전 6.3(5)

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>관련 제품</u>

이 컨피그레이션은 소프트웨어 버전 6.x 이상에서 Cisco 500 Series PIX Firewall Appliance와 함께 사용할 수도 있습니다.

<u>표기 규칙</u>

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

<u>구성</u>

각 인터페이스에는 0(최저)에서 100(최고)까지의 보안 레벨이 있어야 합니다. 예를 들어 내부 호스 트 네트워크와 같이 가장 안전한 네트워크를 레벨 100에 할당해야 합니다. 인터넷에 연결된 외부 네 트워크는 레벨 0이 될 수 있지만 DMZ와 같은 다른 네트워크는 그 사이에 배치될 수 있습니다. 동일 한 보안 레벨에 여러 인터페이스를 할당할 수 있습니다.

기본적으로 모든 포트는 외부 인터페이스(보안 레벨 0)에서 차단되며 모든 포트는 보안 어플라이언 스의 내부 인터페이스(보안 레벨 100)에서 열립니다. 이렇게 하면 모든 아웃바운드 트래픽이 컨피 그레이션 없이 보안 어플라이언스를 통과할 수 있지만, 보안 어플라이언스의 액세스 목록 및 고정 명령 컨피그레이션에서 인바운드 트래픽을 허용할 수 있습니다.

참고: 일반적으로 모든 포트는 Lower Security Zone에서 Higher Security Zone으로 차단되며, 모든 포트는 Higher Security Zone에서 Lower Security Zone으로 열려 있으므로 인바운드 및 아웃바운드 트래픽 모두에 대해 스테이트풀 검사가 활성화됩니다.

이 섹션은 다음과 같은 하위 섹션으로 구성됩니다.

- 네트워크 다이어그램
- <u>포트 구성 차단</u>
- <u>포트 구성 열기</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.

<u>네트워크 다이어그램</u>

이 문서에서는 다음 네트워크 설정을 사용합니다.



<u>포트 구성 차단</u>

보안 어플라이언스는 확장 액세스 목록에 의해 명시적으로 차단되지 않는 한 모든 아웃바운드 트래 픽을 허용합니다.

액세스 목록은 하나 이상의 액세스 제어 항목으로 구성됩니다. 액세스 목록 유형에 따라 소스 및 목 적지 주소, 프로토콜, 포트(TCP 또는 UDP용), ICMP 유형(ICMP용) 또는 이더 유형을 지정할 수 있 습니다.

참고: ICMP와 같은 연결 없는 프로토콜의 경우 보안 어플라이언스는 단방향 세션을 설정하므로 두 방향의 ICMP를 허용하려면(소스 및 대상 인터페이스에 대한 액세스 목록 응용 프로그램) 액세스 목 록이 필요하거나 ICMP 검사 엔진을 활성화해야 합니다. ICMP 검사 엔진은 ICMP 세션을 양방향 연 결로 취급합니다.

일반적으로 내부(상위 보안 영역)에서 DMZ(하위 보안 영역) 또는 외부에 대한 DMZ로 시작되는 트 래픽에 적용되는 포트를 차단하려면 다음 단계를 완료하십시오.

1. 지정된 포트 트래픽을 차단하는 방식으로 액세스 제어 목록을 생성합니다.

access-list

2. 그런 다음 access-list를 access-group 명령으로 바인딩하여 활성화합니다.

access-group

예:

1. HTTP 포트 트래픽을 차단합니다. DMZ 네트워크에 IP 172.16.1.1이 배치된 내부 네트워크 10.1.1.0에 대한 http(웹 서버) 액세스를 차단하려면 다음과 같이 ACL을 생성합니다. ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0 host 172.16.1.1 eq 80 ciscoasa(config)#access-list 100 extended permit ip any any ciscoasa(config)#access-group 100 in interface inside

참고: no와 access list 명령을 차례로 사용하여 포트 차단을 제거합니다.

2. FTP 포트 트래픽을 차단합니다. DMZ 네트워크에 IP 172.16.1.2이 배치된 내부 네트워크 10.1.1.0이 FTP(파일 서버)에 대한 액세스를 차단하려면 다음과 같이 ACL을 생성합니다. ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0 host 172.16.1.2 eq 21 ciscoasa(config)#access-list 100 extended permit ip any any ciscoasa(config)#access-group 100 in interface inside

참고: 포트 할당에 대한 자세한 내용은 IANA <u>포트</u>를 참조하십시오.

- 이 섹션에서는 ASDM을 통해 이를 수행하는 단계별 컨피그레이션을 설명합니다.
 - 1. Configuration(컨피그레이션) > Firewall(방화벽) > Access Rules(액세스 규칙)로 이동합니다. Add Access Rule을 클릭하여 access-list를 생성합니다

4 A	Add 👻 🗹 Edit	💼 Delete	+ + 3	6 🐚 💼 - 🔍 Find
÷	Add Access Ru	le		Destination
~ [~	Insert Insert After		.10.100	any
	sinside (2 outg	oing rules)		See Shirty
1		🖳 172.3	16.10.50	🏟 any
2		🏈 any		🏟 any

이 액세스 규칙이 연결될 인터페이스와 함께 액세스 규칙의 소스 및 대상 및 작업을 정의합니다. 차단할 특정 포트를 선택하려면 세부 정보를 선택합니다

🚰 Add Acc	ess Rule
Interface:	inside 💌
Action: O	Permit ③ Deny
Source:	10.1.1.0
Destination	172,16.1.1
Service:	ip 🔲
Description:	
💽 Enable L	ogging
Logging l	evel: Default 💌
More Opt	ons
	OK Cancel Help
·용 가능한 포	트 목록에서 http를 선택한 다음 OK를 클릭하여 Add Access Rule 창으로

Ner	te	Protocal	Source Ports	Destination Ports	ICMP Type	Description	
and the second	18 dscard	top	default (1-65535)	9	od of the second se		
	11 daman	top	default (1-65535)	53			
	- me echo	top	default (1-65535)	7			
	18 0xec	top	default (1-65535)	512			
	tte finger	top	default (1-65535)	79			
	an fip	top	default (1-65535)	21			
	12- ftp-data	top	default (1-65535)	20			
	-18-gopher	top	default (1-65535)	70			
1 1	10 h323	top	default (1-65535)	1720			
1	38 hostname	top	default (1-65535)	101			
	ap http	top	default (1-65535)	80	S. 4	E.	
	Mt https	top	default (1-65535)	443			
1.13	- 12- ident	top	default (1-65535)	113			
	- 18 inap4	top	default (1-65535)	143			
	me irc.	top	default (1-65535)	194			
	12 iterberos	top.	default (1-65535)	750			
	tte-slogn	top	default (1-65535)	543			
	m Juhel	top	default (1-65535)	544			
	- 312- Idap	top	default (1-65835)	389			
	- 118- Idaps	top	defauk (1-65535)	636			
Selec	ted Service						
C	Senice						

4. OK(**확인)**를 클릭하여 액세스 규칙의 컨피그레이션을 완료합니다

🖆 Add Acce	ss Rule		
Interface:	nside 🔽		
Action: OPe	ermit 💿 Deny		
Source:	10.1.1.0		
Destination	172.16.1.1		Ξ
Service:	cp/http		
Description:			
Enable Log	gging		
Logging Le	vel: Default	~	
More Optio	ns		
	1	ОК	Cancel Help
Insert After 를 클	릭하여 동일한 액서	╢스 목록에 액세₂	스 규칙을 추가합니다
Configuration	> Firewall > Acce	ess Rules	
🔂 🛧 🔁	🕇 Edit <u> </u> Delete	* + ằ 🖻	1 💼 - 🔍 Fi
🔂 Add Ac	cess Rule	[Destination
💠 Insert.			
🐺 Insert /	After	• E	172.16.1.1
	any any	<u>י</u> ע) any
🖃 🦃 manag	e (2 implicit incoming	rules)	
1	🧼 any	9	Any less secur
- S 40	any	Sec. 19	

6. "any"에서 "any"로 트래픽을 허용하여 "암시적 거부"를 방지합니다. 그런 다음 OK(확인)를 클 릭하여 이 액세스 규칙 추가를 완료합니다

insert A	fter Access Rule
Interface:	inside 🔽
Action: 💿 I	Permit 🔿 Deny
Source:	any
Destination	any
Service:	ip
Description:	
💌 Enable L	ogging
Logging I	.evel: Default 💙
More Opt	ions
	OK Cancel Help

7. 구성된 액세스 목록은 Access Rules(액세스 규칙) 탭에서 확인할 수 있습니다. Apply(**적용**)를 클릭하여 이 컨피그레이션을 보안 어플라이언스에 전송합니다

#	Enabled	Source	Destination	Service	Action	Hits
i 🥵 i	side (3 incom	ing rules)				
1			🖳 172.16.1.1	10 http	😮 Deny	0
2		📌 any	🗌 any	tte> ip	🧹 Permit	0
3		🌍 any	any	<u>⊥</u> vip	😆 Deny	
n 👯 I	hanage (2 imp	licit incoming rules)				
1		🏟 any	Any less secure ne	💷 ip	🖌 Permit	
2		🏟 any	any	1e/ip	😮 Deny	
9 0	utside (1 impl	licit incoming rule)		-		
1		🌍 any	any	IP ip	8 Deny	
			JJJC]

ASDM에서 전송된 컨피그레이션을 통해 ASA의 CLI(Command Line Interface)에서 이 명령

집합이 생성됩니다.

access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq www access-list inside_access_in extended permit ip any any access-group inside_access_in in interface inside

이 단계를 통해 예 1은 ASDM을 통해 수행되어 10.1.1.0 네트워크가 웹 서버 172.16.1.1에 액 세스하지 못하도록 차단되었습니다. 예 2도 동일한 방법으로 전체 10.1.1.0 네트워크가 FTP 서버 172.16.1.2에 액세스하지 못하도록 차단할 수 있습니다. 유일한 차이점은 포트를 선택하 는 단계입니다.**참고:** 예 2에 대한 이 액세스 규칙 컨피그레이션은 새로운 컨피그레이션으로 간 주됩니다.

8. FTP 트래픽 차단을 위한 액세스 규칙을 정의한 다음 Details 탭을 클릭하여 대상 포트를 선택

🗯 Add Acc	ess Rule
Interface:	inside 🛛 🖌
Action: 🚫 P	Permit 💿 Deny
Source:	10.1.1.0
Destination	172.16.1.1
Service:	ip 💮
Description:	
💌 Enable Lo	ogging
Logging L	evel: Default 💟
More Opti	ons
-L	OK Cancel Help
니나. 	K를 클릭하여 Add Access Rule 창으로 돌아갑니다

ter:					
Name	Protocol	Source Ports	Destination Ports	ICMP Type	Description
ter citrix-ica	top	default (1-65535)	1494		
tiqbe	tcp	default (1-65535)	2748		
- 100 daytime	tcp	default (1-65535)	13		
tte discard	top	default (1-65535)	9		
tte domain	tcp	default (1-65535)	53		
ray echo	top	default (1-65535)	7		
to exec	tcp	default (1-65535)	512		
10 finger	tcp	default (1-65535)	79		
- 🔞 ftp	top	default (1-65535)	21		—
ftp-data	top	default (1-65535)	20		
copher	top	default (1-65535)	70		
10 h323	tcp	default (1-65535)	1720		
- 💷 hostname	tcp	default (1-65535)	101		
ter http	top	default (1-65535)	60		
- 100 https	top	default (1-65535)	443		
ident	top	default (1-65535)	113		
imap4	tcp	default (1-65535)	143		
TO IC	tcp	default (1-65535)	194		
- 100 kerberos	tcp	default (1-65535)	750		
an Islamia	hen.	dofout (1 ceeses	E40		
lected Service	_				

10. OK(**확인)**를 클릭하여 액세스 규칙의 컨피그레이션을 완료합니다

📬 Add Acc	ess Rule
Interface:	inside 🔽
Action: 🚫 I	Permit 💿 Deny
Source:	10.1.1.0
Destination	172,16.1.1
Service:	tcp/ftp
Description:	
💽 Enable L	ogging
Logging I	Level: Default 💙
More Opt	ions
	OK Cancel Help

11. 다른 트래픽을 허용하려면 다른 액세스 규칙을 추가합니다. 그렇지 않으면 Implicit Deny 규 칙은 이 인터페이스의 모든 트래픽을 차단합니다

🚰 Insert A	fter Access Rule
Interface:	inside 😽 😽
Action: 💿	Permit 🔿 Deny
Source:	any 🛄
Destination	any 🔄
Service:	ip 📰
Description:	
💽 Enable L	ogging
Logging	Level: Default 💙
More Opt	ions
	OK Cancel

.

... 12. 전체 액세스 목록 컨피그레이션은 Access Rules(액세스 규칙) 탭 아래에서 이와 같습니다

#	Enabled	Source	Destination	Service	Action
🗄 🦊 in	iside (3 incom	ning rules)			
4	V	a 10.1.1.0	172.16.1.1	100 ftp	3 Deny
2		🐔 any	🔿 any 👘	IP) ip	🖌 Perm
3		🥥 any	🥥 any	🗶 ip	3 Deny
8 🦊 m	ianage (2 imp	olicit incoming rules)			
1		🧼 any	Any less secure ne	JP> ip	💞 Perm
2		🌍 any	🌍 any	10 ip	🕴 Deng
- 5 o	utside (1 impl	licit incoming rule)			
1		any	any	12 ip	🔕 Den

13. Apply(**적용**)를 클릭하여 컨피그레이션을 ASA로 전송합니다. 동일한 CLI 컨피그레이션은 다 음과 같습니다.

access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq ftp access-list inside_access_in extended permit ip any any access-group inside_access_in in interface inside

<u>포트 구성 열기</u>

보안 어플라이언스는 확장 액세스 목록에서 명시적으로 허용하지 않는 한 인바운드 트래픽을 허용 하지 않습니다.

외부 호스트가 내부 호스트에 액세스하도록 허용하려면 외부 인터페이스에 인바운드 액세스 목록 을 적용할 수 있습니다. 변환된 주소는 외부 네트워크에서 사용할 수 있는 주소이므로 액세스 목록 에서 내부 호스트의 변환된 주소를 지정해야 합니다. 하위 보안 영역에서 상위 보안 영역으로 포트 를 열려면 다음 단계를 완료하십시오. 예를 들어 외부(하위 보안 영역)에서 내부 인터페이스(상위 보안 영역)로 또는 DMZ에서 내부 인터페이스로 이동하는 트래픽을 허용합니다.

1. 고정 NAT는 실제 주소의 고정 변환을 매핑된 주소로 생성합니다. 이 매핑된 주소는 인터넷에 서 호스트하는 주소이며 서버의 실제 주소를 알 필요 없이 DMZ의 애플리케이션 서버에 액세 스하는 데 사용할 수 있습니다.

static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask] |
 access-list access_list_name | interface}

자세한 내용은 <u>PIX/ASA</u>에 <u>대한 명령 참조</u>의 <u>Static NAT</u> 섹션을 참조하십시오. 2. 특정 포트 트래픽을 허용하도록 ACL을 생성합니다.

access-list

3. access-list를 access-group 명령으로 바인딩하여 활성화합니다.

access-group

예:

1. SMTP 포트 트래픽을 엽니다. 외부(인터넷)의 호스트가 DMZ 네트워크에 위치한 메일 서버에 액세스할 수 있도록 포트 tcp 25를 엽니다.Static 명령은 외부 주소 192.168.5.3을 실제 DMZ 주소 172.16.1.3에 매핑합니다. ciscoasa(config)#static (DMZ,Outside) 192.168.5.3 172.16.1.3 netmask 255.255.255.255 ciscoasa(config)#access-list 100 extended permit tcp any host 192.168.5.3 eq 25 ciscoasa(config)#access-group 100 in interface outside

2. HTTPS 포트 트래픽을 엽니다. 외부(인터넷)의 호스트가 DMZ 네트워크에 있는 웹 서버(보안

```
)에 액세스하도록 허용하려면 포트 tcp 443을 엽니다.
ciscoasa(config)#static (DMZ,Outside) 192.168.5.5 172.16.1.5
netmask 255.255.255
ciscoasa(config)#access-list 100 extended permit tcp
any host 192.168.5.5 eq 443
ciscoasa(config)#access-group 100 in interface outside
```

3. DNS 트래픽 허용: 외부(인터넷)의 호스트가 DMZ 네트워크에 있는 DNS 서버(보안)에 액세스 하도록 허용하려면 포트 udp 53을 엽니다. ciscoasa(config)#static (DMZ,Outside) 192.168.5.4 172.16.1.4 netmask 255.255.255.255 ciscoasa(config)#access-list 100 extended permit udp any host 192.168.5.4 eq 53 ciscoasa(config)#access-group 100 in interface outside

참고: 포트 할당에 대한 자세한 내용은 IANA <u>포트</u>를 참조하십시오.

<u>ASDM을 통한 구성</u>

이 섹션에서는 ASDM을 통해 위에서 언급한 작업을 수행하는 단계별 접근 방식을 설명합니다.

1. 192.168.5.3 서버에 대한 smtp 트래픽을 허용하도록 액세스 규칙을 생성합니다



 액세스 규칙의 소스 및 목적지와 이 규칙이 바인딩하는 인터페이스를 정의합니다. 또한 작업 을 허용으로 정의합니다

Interface:	outside		
Action: 🧿	Permit) O Deny		
Source:	any		
Destination	192.168.5.3		
Service:	ip)
Description			
🗹 Enable	Logging		
Logging	Level: Default		
More Op	tions		
	6	OK Canad	Lista

3. SMTP**를** 포트로 선택한 다음 OK를 클릭합니다

Nan	10	Protocol	Source Ports	Destination Ports	ICMP Type	Descripti
	ne pop	ten	default (1-65535)	514		
	and sheep	tro	default (1-65535)	554		
	sin in	top	default (1-65535)	5060		
	EQ state	ltco	default (1-65535)	25	6	
	- set salhet	top	default (1-65535)	1521		
	ssh	top	default (1-65535)	22		
	Star Sunrpc	top	default (1-65535)	111		
1	100 tacacs	top	default (1-65535)	49		
	- 😥 talk	top	default (1-65535)	517		
-	teinet	tcp	default (1-65535)	23		
	No. Unto	top	default (1-65535)	540		
	10 whois	top	default (1-65535)	43		
- 1	ww biff	udp	default (0-65535)	512		
	we bootpc	udp	default (0-65535)	68		
	inty bootps	udp	default (0-65535)	67		
	in cfs	udp	default (0-65535)	3020		
	www.discard	udp	default (0-65535)	9		
	- inter dissist	udp	default (0-65535)	195		
-	👷 domain	udp	default (0-65535)	53		
-		1.1.2.	L.f. A. In Amonth		1	

4. OK(**확인**)를 클릭하여 액세스 규칙 구성을 완료합니다

🖆 Add Aco	ess Rule
Interface:	outside 🔽
Action: 💿	^p ermit O Deny
Source:	any 💮
Destination	192.168.5.3
Service: (tcp/smtp
Description:	
💽 Enable L	ogging
Logging	Level: Default
More Opt	ions
	OK Cancel

5. 172.16.1.3을 192.168.5.3으로 변환하려면 고정 NAT를 구성합니다.고정 NAT **항목을** 추가하 려면 Configuration > Firewall > NAT Rules > Add Static NAT Rule으로 이동합니다



Original Source 및 Translated IP 주소를 관

련 인터페이스와 함께 선택한 다음 OK를 클릭하여 Static NAT 규칙 구성을 완료합니다

🖆 Add Static NAT	Rule	
Original		
Interface:	DMZ	~
Source:	172.16.1.3	
Translated		
Interface: (outside	~
💿 Use IP Address:	192.168.5.3	···
🚫 Use Interface IP	Address	
Port Address Translatio	on (PAT)	
Enable Port A	ddress Translation (PAT)	
Protocol:		
Original Port:		
Translated Po	t)	
Connection Settin		*
	27	
	OK Cancel Help	
xample 섹션에 나열된	세 가지 고정 규칙을 모두 <u>보여줍니다</u>	

🗣 Ad	id 🕶 🕝 Edit 📋	Delete 🕈 🐇 🛛	🔄 🎆 🕘 🔍 Find	🔛 Diagram 🕯	🯹 Packet Trace	
#	Туре	Original		Translated		
		Source	Destination	Service	Interface	Address
DMZ	:					
1	• Static	3 172.16.1.3			outside	3 192.168.5.
2	• Static	172.16.1.5			outside	192.168.5.
3	Static	172.16.1.4			outside	. 192.168.5.

이 이미지는 Examples(예) 섹션에 나열된 세 가지 액세스 규칙 모두를 <u>나타냅니다</u>

.

#	Enabled	Source	Destination	Service	Action
. "S	OMZ (2 implicit	incoming rules)	Paste		
1		🏟 any	Any less secure ne	. 💶 ip	🖌 Permit
2		🏟 any	🏟 any	IP> ip	🕴 Deny
1.59	nside (2 implic	it incoming rules)			
1		🏟 any	Any less secure ne	. ⊥P∕ip	🖌 Permi
2		🏟 any	🏟 any	💶 ip	🕴 Deny
- 5	manage (2 imp	licit incoming rules)			
1		🏟 any	Any less secure ne	, 💴 ip	🖋 Permit
2		🏟 any	🏟 any	<u>.∎</u> ∕ip	😢 Deny
	outside (4 inco	ming rules)			
1	¥	🧼 any	192.168.5.3	₩ smtp	🖌 Permit
2		🏟 any	192.168.5.5	10 https	🖌 Permit
3	V	🥌 any	192.168.5.4	CCP domain	🧹 Permit
4		any	 any 	IP ip	🔞 Deny

<u>다음을 확인합니다.</u>

다음과 같이 특정 show 명령으로 확인할 수 있습니다.

- show xlate 현재 변환 정보를 표시합니다.
- show access-list—액세스 정책에 대한 적중 카운터를 표시합니다.
- show logging 버퍼의 로그를 표시합니다.

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

<u>문제 해결</u>

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

<u>관련 정보</u>

- <u>PIX/ASA 7.x: 인터페이스 간 통신 활성화/비활성화</u>
- <u>PIX 7.0 및 Adaptive Security Appliance Port Redirection(Forwarding) with nat, global, static,</u> patoral 및 access-list 명령
- PIX에서 nat, global, static, pattern, access-list 명령 및 포트 리디렉션(전달) 사용
- PIX/ASA 7.x: Enable FTP/TFTP Services 컨피그레이션 예
- <u>PIX/ASA 7.x: VoIP(SIP,MGCP,H323,SCCP) 서비스 구성 사용 예</u>
- <u>PIX/ASA 7.x: DMZ 구성의 메일 서버 액세스 예</u>
- <u>기술 지원 및 문서 Cisco Systems</u>