Cisco Start Firewall

Cisco ASA 5506-X アクセスリストと静的 NAT による公開サーバの設定

2016年2月12日 第1.0版









改訂履歴

1.0 2016年2月12日 ネットワールド ● 新規	版番号	改訂日	改訂者	改訂内容
	1.0	2016年2月12日	ネットワールド	● 新規





免責事項

- 本書のご利用は、お客様ご自身の責任において行われるものとします。本書に記載する情報については、株式会社ネットワールド(以下弊社)が慎重に作成および管理いたしますが、弊社がすべての情報の正確性および完全性を保証するものではございません。
- 弊社は、お客様が本書からご入手された情報により発生したあらゆる損害に関して、一切の責任を 負いません。また、本書および本書にリンクが設定されている他の情報元から取得された各種情報 のご利用によって生じたあらゆる損害に関しても、一切の責任を負いません。
- 弊社は、本書に記載する内容の全部または一部を、お客様への事前の告知なしに変更または廃 止する場合がございます。なお、弊社が本書を更新することをお約束するものではございません。





表記規則

表記	表記の意味
「」(括弧記号)	キー、テキストボックス、ラジオボタンなどのオブジェクト
	入力または選択するシステム定義値
<italic>(イタリック文字)</italic>	入力または選択するユーザー定義値
────────────────────────────────────	入力または選択するオブジェクト
""(二重引用符記号)	表示されるメッセージ
(蛍光マーカー)	確認するメッセージ
表記の例) ① → ExecJラジオボタンを選択 ② テキストボックスに以下の copy running-config < ③ 「コマンドを実行」ボタンをど Destination filename Building configuratio	代します。 マンドを入力します。 file name> PJックします。正常に実行されれば、画面に"[OK]"が表示されます。 [startup-config]? n
CLIIによる設定 CLI機能はルータのコマンドプロンプトで実行可能な設 CLI機能はルータのコマンドプロンプトで実行可能な設 Configure Copy running-config startup-config コマンドを実行 クリア Destination filename [startup-config]? Building configuration [OK]	をや、全ての105 (LIコマンドを入力できます





<u>目次</u>

1. はじめに	1
1.1 対象機器	1
1.2 アクセスリストと静的 NAT について	1
2. システム構成	2
2.1 システム構成	2
3. アクセスリストと静的 NAT の設定	3
3.1 DMZ インタフェースの設定	3
3.2 アクセスリストの設定	5
3.3 静的 NAT の設定	7





1. はじめに

本書は Cisco ASA 5506-X におけるアクセスリストと静的 NAT による公開サーバの設定手順につい て説明しています。

1.1 対象機器

本書で対象としている機器は以下になります。

表	1	本書の対象機器
15	÷.,	

ASA 5506-X	ASA 5506W-X	
(ASA5506-K9)	(ASA5506W-Q-K9)	
	V	

1.2 アクセスリストと静的 NAT について

アクセスリストは特定のホストやサービスに対してアクセスの許可もしくは不許可を定義する機能です。 デフォルトではインターネット側(outside)から内部へはアクセスできませんが、アクセスリストを使用する 事で、LAN 側の WEB サーバにインターネットからアクセスすることができます。また、LAN 側からインター ネットへのアクセスを制御する際にも利用することができます。

静的 NAT は、あるインタフェースから他のインタフェースを通るトラフィックに対して、IP アドレスを静的に 変換する機能です。 LAN にある WEB サーバのプライベート IP アドレスをインターネットに公開する IP ア ドレスに変換することで、インターネット側から WEB サーバにアクセスが行えるようになります。



Visco Start Firewall Cisco ASA 5506-X アクセスリストと静的 NAT による公開サーバの設定

2. システム構成

2.1 システム構成

本書での設定手順は以下のシステム構成に基づいて行われます。

別紙「Cisco ASA 5506-X クイックスタートガイド」の内容に基づいて初期設定が完了した状態となっています。GE1/1(outside)にはDHCPによりグローバルIPアドレスが払い出され、インターネットから アクセスできる状態を前提としています。



図1 システム構成図

表 2 本書で使用した機材およびそれらのシステム環境

機器	機器名	OS およびアプリケーション	インタフェース設定
Firewall	ASA 5506W-X	OS Version 9.5(2)	GE1/1
		ASDM Version 7.5(2)153	nameif:outside (デフォルト)
			IP アドレス:DHCP(デフォルト)
			security level:0(デフォルト)
			GE1/2
			nameif:inside (デフォルト)
			IP アドレス:172.16.1.254/24
			Security level:100(デフォルト)
			GE1/3
			nameif:dmz
			IP アドレス:10.1.1.254/24
			Security level:50(デフォルト)
管理用 PC		OS : Windows 7	インタフェース IP アドレス:172.16.1.1/24
		ターミナルアプリケーション (Tera Term)	
		Web ブラウザ(Internet Explorer11)	

表 3 ASA 5506-X のネットワーク設定

ルーティング	・インターネット側ヘデフォルトルートを DHCP により取得
アクセスリスト	・outside から dmz のホスト 10.1.1.1 への HTTP アクセスを許可
NAT	・any→outside への PAT (デフォルト)
	・outsideとdmzのホスト10.1.1.1との静的 NAT





3. アクセスリストと静的 NAT の設定

3.1 DMZ インタフェースの設定

 管理 PC から ASDM により ASA にアクセスし、「Configuration」>「Device Setup」>「Interf ace Settings」>「Interfaces」を開き、「Gigabit Ethernet1/3」を選択して「Edit」を開きま



図 2 インタフェースの設定を開く

2) DMZ 用のインタフェースの設定を入力し、「OK」をクリックします。

Edit Interface	
General Advanced IPv6	
Hardware Port GigabitEthemet1/3 Configure Hardware Properties	
☑ Enable Interface	
IP Address	
IP Address 10.1.1.254 ③「IP Address」を設定します(例:10.1.1.254) Subnet Mask 05592552550 ④「Subnet Mask」を設定します(例:255.255.25	5.0)

図 3 DMZ 用インタフェースの設定





アクセスリストと静的 NAT による公開サーバの設定

3) Security Level の変更に対する警告文が表示されますが、「OK」をクリックして先に進みます。



図 4 Security Level 変更の警告文

4)「Apply」をクリックして ASA に設定を反映します。

Gisco ASDM 7.5(2)153 for ASA - 1	72.16.1.254								_ 0 <mark>_ X</mark> _
File View Tools Wizards Windo	w Help				-	Type topic t	o search	Go	de de
Home 🍕 Configuration 🔯 Monito	oring 🔚 Save 🔇 Refres	h 🔇 B	ack 🔘 Forward	🦓 Невр					cisco
Device List Bookmarks	onfiguration > Device Set	up > Inter	face Settings >	Interfaces					
Device List P ×									
🕈 Add 📋 Delete 🚿 Connect	Interface	Name	Zone	Route Map	State	Security Level	IP Address	Su Pre	Add 🔻
Find: Go	GigabitEthernet1/1	outside			Enabled	0	D D 199.	255	Edit
	GigabitEthernet1/2	inside			Enabled	100	172.16.1.254	255	
	GigabitEthernet 1/3	dmz			Enabled	50	10.1.1.254	255	Delete
	GigabitEthernet1/4				Disabled				
	GigabitEthernet1/5				Disabled				
	GigabitEthernet1/6				Disabled				
Device Setup 🗗 🖗	GigabitEthernet 1/7				Disabled				
Startup Warand	GigabitEthernet 1/8				Disabled				
Startup Wizard	GigabitEthernet 1/9	wifi			Enabled	100	192.168.10.1	255	
and the second	Management1/1				Enabled				
Envire Stern									
Franall								_	
Contraction of the second seco	<	_						F	
Remote Access VPN	Z Enable traffic between two	oor more in	nterfaces which are	configured with :	same security le	vels			
Site-to-Site VPN	Enable traffic between two	or more h	osts connected to t	ne same interfac	e				
Device Management	Enable jumbo frame reserv	ration	_						
, ,				Apply	Reset)			
				<admin></admin>	15	6		16	/02/09 2:51:32 UTC

図5 設定の反映

5) ASA に投入されるコマンドのプレビューが表示されますので、「Send」をクリックして実行します。



図 6 コマンドのプレビュー





3.2 アクセスリストの設定

本節では、インターネットから DMZ の WEB サーバへのアクセスを許可するためのアクセスリストの設定 手順について説明します。

6)「Configuration」>「Firewall」>「Access Rules」を開き、「Add」>「Add Access Rule」 を開きます。

Cisco ASDM 7.5(2)153 for ASA - 172.16.1.254			- 0 - X -
File View Tools Wizards Window Help		Type topic to search G	° dhalu cisco
Device List Bookmarks Configuration > Firewall > Access Rules		Addresses Services Time Rar	iges
Device List 🗗 🕂 🙀 Add 🗸 🗹 Edit 📋 Delete 🛧 🗲 👗 🐚 📾	- 🔍 Find 🖭 Diagram 調 Export	Addresses	67 9 ×
Add Delete & Connect Add Access Rule		Add - C Edit Delete , Whe	re Used 🔍 Not Used
Find Go 47TADD		Silikule」を用きしま	9 Filter Clear
172.16.1.254	decarty croop	Name	
insert Arter		Network Objects	
Inside (1 implicit incoming rule)		- I any	
Firewall 0 0 0		any4	
Access Bules		ariyo	
	します	inside-network/24	
Q Service Policy Rules		- 🙀 outside-network/16	
Filter Rules		- 🖷 wifi-network/24	
Public Servers		- 🗷 NAT	
URL Filtering Servers		- 👼 obj_any	
Threat Detection			
Lentity Options			
🕀 🕼 Objects			
Communications			
m. 69 Movancen			
A. Device Setup			
	±		
CIFICEWall CIFICEWall」をクリックし	15 9		
Remote Access VPN			
Site-to-Site VPN			
Device Management	t i		
* Apply Reset	Advanced		
Configuration changes saved successfully.	<admin> 15</admin>	🕞 🛃 🔂	16/02/09 5:18:55 UTC
図 フ マクセ	7月7トの設定な	2問/	
四 / パンピ	ヘノヘトのみたて	/ 1751 -	

7) アクセスリストの条件を入力し、「OK」をクリックします。

Add Access Rule
Interface: outside 🖵
Action: Permit Deny ① Permit を選択します
Source Oriteria
Source: any 辺送信元 IP アドレスを入力します(例):any)
User:
Security Group:
Destination Oriteria
Destination: 10.1.1.1 回③許可する宛先 IP アドレスを入力します(例:10.1.1.1)
Security Group:
Service: [tcp/http] ④許可するサービスを入力します(例:tcp/http)
Description:
☑ Enable Logging
Logging Level Default
More Options ⑤ 「OK はなり」いのします ×

図8 アクセスリストの設定





8) アクセスリストが作成されている事を確認し、「Apply」をクリックして ASA に設定を反映します。



9) ASA に投入されるコマンドのプレビューが表示されますので、「Send」をクリックして実行します。

Preview CLI Commands
The following CLI commands are generated based on the changes you made in ASDM. To send the commands to the ASA, click Send. To not send the commands and continue making changes in ASDM, click Cancel.
access-list outside_access_in line 1 extended permit top any host 10.1.1.1 eq http access-group outside_access_in in interface outside
Send Cancel Save To File

図 10 コマンドのプレビュー





3.3 静的 NAT の設定

 Configuration」>「Firewall>「NAT Rules」を開き、「Add」>「Add "Network Objec t" NAT Rule」を開きます。

Gisco ASDM 7.5(2)153 for ASA	172.16.1.254		and the second secon	_ 0 _ X
File View Tools Wizards			Type topic to search Go	cisco
Device List Bookmarks	Configuration > Firewall > NAT Rules		Addresses Services	
Device List ⊡ ₽ ×	🗣 Add - 🛒 Edit 🏦 Delete 🛧 🗲 👗 🗎	💁 Find 🖼 Diagram 💷 Packet	Addresses	9 ¢ ×
🗣 Add 📋 Delete 🖋 Connect	Add NAT Pula Refere "Network Obje t" NA	T Rulas	💠 Add - 🛒 Edit 🏢 Delete 🔍 When	e Used 🔍 Not Used
Find: Go		in Kules	Filter:	Filter Clear
172.16.1.254	Add Network Object NAT Rule	Service	Name	
	Add NAT Rule After "Network Object" NAT	Rules	Network Objects	
Firmerall 2010	Insert After SADD "N	letwork Obje	ct" NAT Rule]&	開きします
			- Sanyti	
NAT Rules (3)	AT Rules をクリックします	す	- Miniside-network/24	
C AAA Dules			📸 obj_any	
Filter Rules			- M outside-network/16	
- Public Servers			- an wifi-network/24	
Identity Options				
Hand Objects				
🐵 🙀 Unified Communications				
⊞-13 Advanced				
A Device Setup				
🖏 Firewall 🛛 🚺	「Firewall」をクリックしま	व		
Bemote Access VPN		-		
Site-to-Site VPN				
Device Management	<	•		
»	Apply Res	et		
		≺admin> 15	🔊 🛃 🔂 🔹 🔒	16/02/09 3:00:12 UTC

図 11 NAT ルールの設定を開く

2) NAT の設定を入力後、「Advanced」をクリックします。



図 12 NAT ルールの設定





3) 公開するポートを設定し、「OK」をクリックします。

advanced NAT Sett	ings 🛛 🗙	
Translate DNS rep	olies for rule	
Disable Proxy ARP on egress interface		
Lookup route table	e to locate egress interface	
Interface	①dmzを選択します	
Source Interface:	dmz 🗸	
Destination Interface	outside 🗸 🗸	
	②outside を選択します	
Service		
Protocol:	🏧 🗐変換前のプロトコルを入力します(例: http)	
Real Port:	http	
Mapped Port:		
⑤クリックします のк	(4) 変換使のノロトコルを入力しよ9 (例:http) Cancel Help	

図 13 NAT ルールの設定(advanced)

4) 「OK」をクリックして NAT ルールの設定を完了します。

G Add Network	c Object
Name:	NAT
Туре:	Host
IP Version:	
IP Address:	10.1.1.1
Description:	
NAT	\$
Add Autom	natic Address Translation Rules
Type:	Static 🗸
Translated A	Addr: outside
📃 Use one-	-to-one address translation
PAT Poo	I Translated Address:
Round	Robin
Extend	d PAT uniqueness to per destination instead of per interface
Transl	ate TCP and UDP ports into flat range 1024-65535 📃 Include range 1-1023
Enable	e Block Allocation
Block To ch	size of 512 and maximum block allocation per host 4 has been configured.
Fall thro	ugh to interface PAT(dest intf): dmz
📃 Use IPv6	ò for interface PAT
	Advanced
	OK Cancel Help

図 14 NAT ルール設定の完了





5) NAT ルールが追加されている事を確認し、「Apply」をクリックして ASA に設定を反映します。

Cisco ASDM 7.5(2)153 for ASA	- 172.16.1.254						- 0 ×
File View Tools Wizards Wi	ndow Help					Type topic to search Go	ababa
🚮 Home 🦓 Configuration 📴 M	onitoring 🔲 🔜 Sav	re 💽 Refres	ah 🔇 Back 🤅	Forward 💡 Help			cisco
Device List Bookmarks	Configuration >	Firewall >	NAT Rules			Addresses Services	
Device List 🗗 🗜 🗡	🔹 Add 🗸 🜠 Er	Gt 🏦 Dalata	*	III O First Find Diag	ram 🝘 Packat	Addresses	리 무 ×
🕈 Add 📋 Delete 🚿 Connect			> + 00 -m			💠 Add 👻 🎬 Edit 🏢 Delete 🔍 Where	Used 🔍 Not Used
Find: Go	# Match C	riteria: Origi	nal Packet				Filter Clear
	Source Int	f Dest Intf		ルーシルの追	加きれて	いることを唯認します	
						Name Natural Objects	
	I dmz	outside	A NAT	🕲 any	100 http	E-Network Objects	
	ourside	um2	any any	utside	12 http	any and	
Firewall D P	2 Any	outside	📲 obj_any	🧼 any	🂝 any	any any	
Access Bules						- all dmz-network /24	
- E NAT Bules						- m inside-network /24	
- Q Service Policy Rules						- A NAT	
AAA Rules						- 👼 obi anv	
Public Services						- A outside-network/16	
URL Eiltering Servers						wifi-network/24	
Threat Detection							
- Julentity Options							
Identity by TrustSec							
Dijects							
Unified Communications							
W US Huvanceu							
0							
Device Setup							
🚯 Firewall							
Remote Access VPN							
Site-to-Site VPN			ைபிய	カレキオ			
🗾 Device Management	4		2799	JUA 9	÷		
»			Apply	Reset			
•					1.0		/00/00 5.00 50 1770
				<admin></admin>	10	Leg 🔛 🛄 💽	1/02/09 0:06:62 UTC

図 15 設定の反映

6) ASA に投入されるコマンドのプレビューが表示されますので、「Send」をクリックして実行します。

Preview CLI Commands
The following CLI commands are generated based on the changes you made in ASDM. To send the commands to the ASA, click Send. To not send the commands and continue making changes in ASDM, click Cancel.
object network NAT host 10.1.1.1 nat (dmz.outside) static interface service tcp http http
Send Cancel Save To File

図 16 コマンドのプレビュー

7) ここまでで、DMZのWEBサーバを、アクセスリストと静的NATによりインターネットに公開する設定が 完了となります。インターネットよりASAのGE1/1(outside)のIPアドレスにHTTPアクセスし、WEB サーバにアクセスできるか確認して下さい。

お問い合わせ

Q 製品のご購入に関するお問い合わせ

https://info-networld.smartseminar.jp/public/application/add/152

Q ご購入後の製品導入に関するお問い合わせ

弊社担当営業にご連絡ください。

Q 製品の保守に関するお問い合わせ

保守開始案内に記載されている連絡先にご連絡ください。

本書に記載されているロゴ、会社名、製品名、サービ ス名は、一般に各社の登録商標または商標です。 本書では、®、™、©マークを省略しています。

