# Cisco Start Firewall

Cisco ASA 5506-X Network Object GroupとService Groupの設定

2016年2月5日 第1.0版



www.networld.co.jp







## 改訂履歴

版番号	改訂日	改訂者	改訂内容
1.0	2016年2月5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
Г	— <b>bold</b> (ボールド文字)	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
$\square$	— 🗌 (囲み線)	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 (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 Destination filename Building configuratio	択します。 コマンドを入力します。 <i>file name&gt;</i> だクリックします。正常に実行されれば、画面に"[OK]"が表示されます。 [startup-config]? on
	CLIIこよる設定 CLI編組はルータのコマンドブロンプトで実行可能な認 ・ Exec ・ Configure copy running-config startup-config コマンドを実行 クリア Destination filename [startup-config]? Building configuration [OK]	tzk+, 全てのIOS (Ц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 Network Object GroupとService Groupについて	1
2. システム構成	2
2.1 システム構成	2
3. Network Object GroupとService Groupの設定	3
3.1 Network Object Groupの設定	3
3.2 Service Groupsの設定	6





## 1. はじめに

本資料では、ASA 5506-X での Network Object Group と Service Group の設定手順について説明します。

### 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

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

### 1.2 Network Object Group と Service Group について

Network Object とは、IP アドレスに名前を付けてアクセスリストや NAT などのネットワーク設定に利用する機能となり、それをグループ化したものが Network Object Group となります。

Service Group は複数のプロトコルをグループしたものです。

Network Object Group や Service Group によって、複数の IP アドレスやプロトコルを、ネットワーク設定に一括で適用することができます。





# 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。設定状態は別紙「Cisco ASA 5506-X クイックスタートガイド」の設定完了後となり、管理 PCの ASDM から ASA に接続できる状態を 想定しています。

クライアント PC の IP アドレスに対して Network Object Group および Service Group の設定 を行います。



### 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	ネットワーク設定
Firewall	ASA 5506W-X	OS Version 9.5(2) ASDM Version 7.5(2)153	GE1/1 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)
L2 スイッチ	SG-110D		
管理用 PC		OS : Windows 7 ターミナルアプリケーション (Tera Term) Web ブラウザ(Internet Explorer11)	インタフェース IP アドレス:172.16.1.1/24

### 表 3 ASA 5506-X のネットワーク設定

ルーティング	DHCP によりインターネット側へのデフォルトルートを取得				
Object	Network Object	Sales-PC-01(172.16.1.10), Sale-PC-02(172.16.1.11)			
, , , , , , , , , , , , , , , , , , ,	Network Object Group	Sales-Group-1(Sales-PC-01, Sale-PC-02)			
	Service Group	Sales-Group-1-Service(http,https,imap4,smtp)			
NAT	any→outside への PAT(デフ	オルト)			





# 3. Network Object GroupとService Groupの設定

### 3.1 Network Object Groupの設定

す。

本節では Network Object Group の設定手順について説明します。

 管理 PC から ASDM により ASA にアクセスし、「Configuration」>「Firewall」>「Objects」>「N etwork Objects/Groups」を開き、「Add」をクリックして「Network Object Group」を開きま

Gisco ASDM 7.5 for ASA - 172	2.16.1.254		_			x
File View Tools Wizards V			ックします ***	Type topic to a	Go Go CI	sco
Device List   Bookmarks	Configuration > Firewall	> Objects > Network O	pjects/Groups			
Device List ☐ A × Add	Add      Edit      Dele     Add      Network Object	te 🔍 Where Jsed 🔍 No	・used Add」をクリ	Jックし、「Net	work Object	Group」を開きま
172.16.1.254	Network Object Gro	up	Netmask	Description	Object NAT Addre	22
192.108.1.1	- @ any - @ anyl					
irewall 🗗 🖓	- 🍑 any6	172 16 1.0	255 255 255 0			
Threat Detection	obj_any	1.0.0.0	0.0.0		outside (P)	
g <sup>9</sup> Identity Options	· · · · · · · · · · · · · · · · · · ·	192.168.10.0	255.255.255.0			
Scurig Group Diject Groups     Security Group Diject Groups     Class Maps     Charter Maps     Regular Expressions     Time Regular Expressions     Diffied Communications     Monance     devaced						
Levice Setup	<ol> <li>Firewall</li> </ol>	をクリックしま	व			
Remote Access VPN			-			
Site-to-Site VPN	-					
Device Management						
ž	2		Apply	Reset		
		1.png - ペイン	Kadmin>	15 🗔 🛃 🧕	16/02/04	2:29:38 UTC

図 2 Network Object Groupの設定画面へ移動

2) Network Object Group の「Group Name」を入力し、Network Object を作成して Group に追加します。

Add Network Object ( Group Name Sales-Group	-1	Group Nai	me」を入力	レます (例:Sales-Group-1)
Description				
Existing Network Object	ts/Groups:			Members in Group:
Name	IP Address	Netmask	Descriptio	Name IP Address NetmaskPrefix Length De
Network Objects				🔜 Sales-PC-01 172.16.1.10
- 🧼 any				() Notwark Object Crown b <sup>(</sup> ) Ωt0+10
- 🧇 any4				
- 🧼 any6				
- 🚜 inside-net	172.16.1.0	255.255.255.0		
- 🚜 wifi-netwo.	192.168.10.0	255.255.255.0		
🖳 🌺 obj_any	0.0.0	0.0.0		
Create new Network O     Name: (optional Sale:     Type: Host     IP Version: IF	viect memberi -PC-01	FCreate Network	new 'Net Object Ø	work Object member」をチェックします 名前を入力します(例:Sales-PC-01) 「ype」で「Host」を選択します。
IP Address: 172. Description:	6.1.10	5) IP Add	lress」を設	EU#9(199:172.16.1.10)

図 3 Network Object Groupの設定





Network Object GroupとService Groupの設定

3) 同じ手順で別の IP アドレスの Network Object を Group に追加します。

up Name: Sales	-Group-1				
cription:					
Existing Network	Objects/Groups:			Members in Group:	
Name	IP Address	Netmask	Description	Name IP Address Netmask F	refix Length De
- Network Obj	ects				
any 🧼				5 Sales-PO-02 172.16.1.11	
any4					
🧼 🥹 any6	170.10.10	055 055 055 0		①Network Object 名 Sale	es-PC-02 <b>] ,</b> IP ノ
inside	e-net 172.10.1.0	255.255.255.0			
ang win-r	192.100.10.0	0000		レス  172.16.1.11」の Object	を Group に追加
				sdd >>	
4				idd≫	
Create new Netw	III		ł	dd ≫ Remove	
Greate new Netw Name: ContinuaD	III vork Object member: Sales-PC-12		•	kd ≫ Remove	
Create new Netw Name: (optional) Type:	m work Object member: Sales-PC-02 Host			kd ≫ Remove	
✓ Create new Netw Name: (optional) Type: IP Version:	™ Sales-PC-02 Host ● IPv4 ○ IPv6		•	xd∂≫ Remove	
Create new Netw Name: (optional) Type: IP Version: IP Address:	m Sales-PC-02 Host ● IPv4 ● IPv6 172:18.11		,	dd ≫ Remove	
Create new Netw     Name: (optional)     Type:     IP Version:     IP Address:     Description:	™ Sales=PC=02 Host @ IPv4 ○ IPv6 172:16:1.11		•	ud >> Remove	
Create new Netw Name: (optional) Type: IP Version: IP Address: Description:	m Sales-PC-02 Host @ IPv4 @ IPv6 172.16.1.11			xd シ≥ Remove たクリックする	
<ul> <li>Create new Netr</li> <li>Name: (optional)</li> <li>Type:</li> <li>IP Version:</li> <li>IP Address:</li> <li>Description:</li> </ul>	m Sales-PO-62 Host @ IPv4 @ IPv6 172.16.1.11			id >> Remove たつリックする	

#### 図 4 Network Object の Group への追加

**4)** 作成した Network Object や Network Object Group が追加されていることを確認し、「Apply]をクリックして ASA に設定を反映させます。



図5設定の反映





Network Object Group と Service Group の設定

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。

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 Sales-PC-01 host 172.16.1.10 object network Sales-PC-02 host 172.16.1.11 object-proup network Sales-Group-1 network-object object Sales-PC-01 network-object object Sales-PC-02
Send Cancel Save To File

図 6 コマンドのプレビュー





### 3.2 Service Groupの設定

本節では Service Group の設定手順について説明します

 「Configuration」>「Firewall」>「Objects」>「Service Objects/Groups」を開き、「Add」 をクリックして「Service Group」を開きます。

Cisco ASDM 7.5 for ASA - 172.10	16.1.254					OX
File View Tools Wizards	onitorine 🔚 Save 🐼 Refresh 🗿 Baci		lelp	Type topic to search	Go	cisco
Device List Bookmarks	Configuration > Firewall > Objects > S	ervice Objects/Grou	<u>DS</u>			
Device List 🗗 🕂 🗡						
🗣 Add 📋 Delete 🚿 Connect	THOU . M COIL Delete & Wiere	seu				
Find Go	Service Object					Filter Clear
	Bervice Group	Source Ports	Destination Ports	ICMP	Description	
	B TCP Service Group		マクリックし、	[Service	Groun	を思きます
	W UDP Service Group	Uniduji			Group	
Firmual	TCP-UDP Service Group					
B Breat Detection	ICMP Group					
Identity Options	Protocol Group					
- St Identity by TrustSec						
Herror Coperts/Targe     Borror Colorts/Targe     Social User Grups     Social User	〕「Objects」>「Serv	vice Obje	cts/Grou	ps」をクリッ <sup>,</sup>	クします	
Firewall	②「Firewall」をクリック	します				
Remote Access VPN						
Site-to-Site VPN						
Device Management						
×		App	k Reset			
Configuration changes saved successful	ily.	Kad	min>  15	D 🛃 🔂	1	6/02/04 2:47:58 UTC

図 7 Service Groupを開く

**2)** 「Group Name」に Service Group の名前を入力します。「Existing Service/Serice Group」から、Group に含めるプロトコルを選択し、「Add」をクリックして Group のメンバーとします。

N		Name	
Name Pare discussion of the second of the	● ● ● ● ● ● ● ● ● ●	Name ③「Add」をクリックします )	

図 8 Service Groupの設定



Cisco Start Firewall Cisco ASA 5506-X



Network Object Group と Service Group の設定

**3)** 同様の手順で複数のプロトコルを Group のメンバーにすることができます。追加し終えたら、「OK」をク リックして完了します。

roup Name: Sales-Group1-Serv	ice		
Existing Service/Service Gro	m		Members in Group:
Name 100 lotusnotes 100 nebios-ssn 100 nfs 100 nrtp 100 pointywhere-data 100 pim-suto-rp 100 pop2		•	Name ************************************
100         pop3           100         pop4           100         stp           100         stp           100         stp           100         stp           100         sth           100         sth           100         sth           100         sth           100         sth           100         sth		Add >>	
Create new member: Name: Service Type: Destination Port/Range: Source Port/Range: defi Description:	top sult		
	(	②「OK」をクリ	ックします
	ОК	Cancel	Help

### 図9 複数のプロトコルの Group への追加

**4)** 作成した Serice Group が追加されていることを確認し、「Apply」をクリックして ASA に設定を反映 します。

	C 1 051					1	
File View Tools Wizards Wit	dow Help				Type topic to search	Go	
Home 🍓 Configuration 🔯 Mo	mitoring 🔚 Save 🌘	🔖 Refresh 🚺 Ba	ck 🔘 Forward 🧖	Help			CISCO
Device List Bookmarks	Configuration > Fire	ewall > Objects >	Service Objects/Gro	ups			
Device List ☐ ₽ ×	da Add y 177 page 11		Head				
🏶 Add 📋 Delete 🚿 Connect		Delete   📽 where	oseu				511 01
Find Go	Name Service Objects	Protocol	Source Ports	Destination Ports	ICMP	Description	[Filter]Oilear]
Frewall Threat Detection	Sales-Group	les.] D作成した	Service C	aroup が追加	加されています	す	
definition of the second							
Device Setup     Firewall     Gemote Access VPN     Site-to-Site VPN				②[Apply]	をクリックします	す	
Device Management			Ap	ply Reset		-	
Configuration changes saved successful	ly.		Ka	dmin> 15	6	16	/02/04 2:52:48 UTC

### 図 10 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。

The following CLI Co to the ASA, click S	commands commands are generated b Send. To not send the com	based on the change mands and continue	es you made in ASDM. T making changes in AS	o send the commands DM, click Cancel.
object-group service-obj service-obj service-obj service-obj	service Sales-Group I-Se ect top destination eq http ect top destination eq http ect top destination eq an ect top destination eq smt	vice is p4 P		
	Send	Cancel	Save To File	

図 11 コマンドのプレビュー

# 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。

www.networld.co.jp

