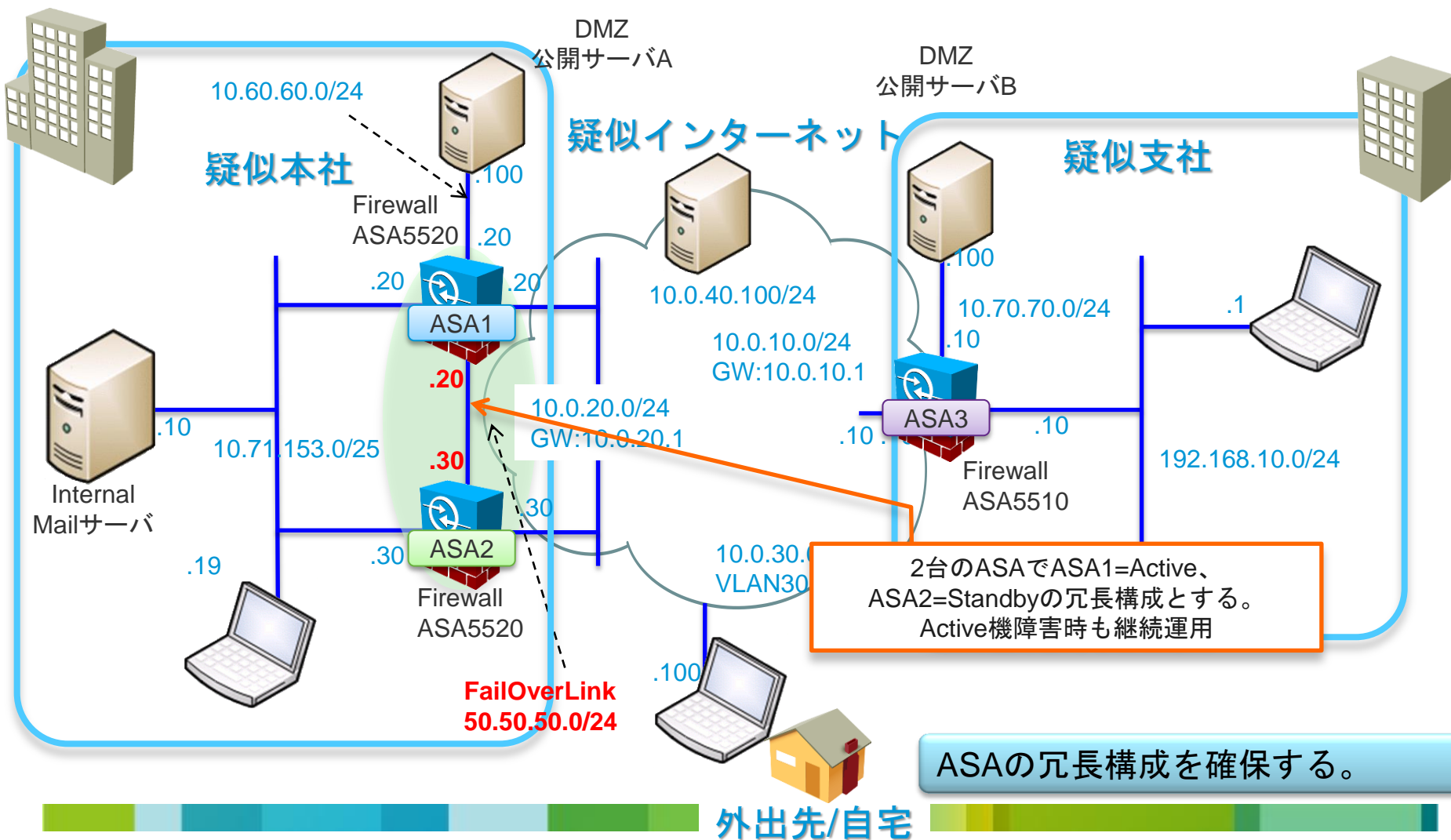


Cisco ASA5500 VPN Failoverの設定

Failoverの設定 ネットワーク構成



Failoverの設定 1

ASDM High Availability Scalability Wizard

Configuration Type (Step 1 of 6)

Use this wizard to configure Active/Active or Active/Standby failover, or VPN cluster load balancing. The following are the types of high scalability configurations available based on this firewall's software profile.

This Firewall's Hardware/Software Profile:

Hardware Mo...	ASA5520	Software Versi...	8.4(2)
Number of Interfa...	5	Failover Licen...	Active/Active
Additional Modu...	None	Firewall Mode:	Single Routed

Failover Configuration Type:

- Configure Active/Active failover
- Configure Active/Standby failover
- Configure VPN Cluster Load Balan...

Diagram: Internet cloud connected to two firewalls. Left: Primary Active, Right: Secondary Standby.

< Back Next > Finish Cancel Help

Active/Standby Failoverを選択

Peerアドレスを指定
(Failover後は設定が同期される。
その際もStandby機にASDMアクセスを可能にする)

Failover Peer Connectivity and Compatibility Check (Step 2 of 6)

Enter the IP address of the failover peer. When you click "Next", ASDM will perform several checks and report the pass/fail results. If any of the tests fail, you will need to resolve the cause of the failure before proceeding to the next step.

Peer IP Address:

- ✓ Connectivity test from this ASDM to the peer device passed.
- ✓ Connectivity test from this device to the peer device passed.
- ✓ Hardware compatibility test for platform, interfaces and modules pass...
- ✓ Software version compatibility test passed.
- ✓ Failover license compatibility test passed.
- ✓ Routed/Transparent firewall mode compatibility test passed.
- ✓ Single/Multiple firewall mode compatibility test passed.

< Back Next > Finish Cancel Help

Failoverの設定 2

The image shows two screenshots from the ASDM High Availability and Scalability Wizard. The first screenshot is titled "LAN Link Configuration (Step 3 of 5)" and the second is "State Link Configuration (Step 4 of 6)".

LAN Link Configuration (Step 3 of 5):

- Interface: GigabitEthernet0/2
- Logical Name: FAILOVER
- Active IP Address: 50.50.50.20
- Standby IP Address: 50.50.50.30
- Subnet Mask: 255.255.255.0
- Communication Encryption: Use 32 hexadecimal characters
- Secret Key: *****

State Link Configuration (Step 4 of 6):

- Options:
 - Disable stateful failover
 - Use the LAN link as the State link
 - Configure separate stateful failover interfaces
- State Interface: (empty)
- Logical Name: FAILOVER
- Active IP Address: 50.50.50.20
- Standby IP Address: 50.50.50.30
- Subnet Mask: 255.255.255.0

FailoverInterfaceの設定

FailoverInterface (Fa0/2)を指定

Activeアドレス(ASA1のFO Linkアドレス)、Standbyアドレス(ASA2のFO Linkアドレス)を指定

StatefulFailoverInterfaceの設定

今回はFO Link/Stateful FO Link同一インターフェイスを使用

*ASA2には、予めFO Linkのアドレス50.50.50.30/24を設定してあります。

Failoverの設定 3

ASDM High Availability Scalability Wizard

High Availability and Scalability Wizard

Standby Address Configuration (Step 5 of 6)

Assign a standby IP address and a monitoring status to each of the interfaces with configured active IP addresses. Double-click on a standby address or click on a monitoring checkbox to edit it. Press the Tab or Enter key after editing an address.

Device/Interf...	Active IP Address	Subnet Mask/ Prefix Length	Standby IP Address
▼ ASA1			
dmz	10.60.60.20	255.255.255.0	10.60.60.30
inside	10.71.153.20	255.255.255.0	10.71.153.30
management	1.1.1.1	255.0.0.0	1.1.1.2
outside	10.0.20.20	255.255.255.0	10.0.20.30

切り替えのトリガとなる監視対象のインターフェイスを確認
StandbyInterfaceのアドレスを確認

< Back Next > Finish Cancel Help

Failoverの設定 4

High Availability and Scalability Wizard

ASDM High Availability Scalability Wizard

Summary (Step 6 of 6)

Click Finish to send the following failover configurations to the Primary and Secondary devices. Once the configurations are sent, the devices will start the failover synchronization. Failover synchronization might take a few minutes. To check the failover status, go to Monitoring -> Properties -> Failover -> Status.

Configuring Active/Standby failover

Peer IP Address: 10.71.153.30

LAN Link:

Interface: GigabitEthernet0/2
Logical Name: FAILOVER
Active IP Address: 50.50.50.20
Standby IP Address: 50.50.50.30
Subnet Mask: 255.255.255.0
Secret Key: *****

State Link:

Use LAN link (GigabitEthernet0/2)

Standby IP Address and Monitoring Status:

dmz	10.60.60.20	10.60.60.30	Monitored
inside	10.71.153.20	10.71.153.30	Monitored

< Back Next > **Finish** Cancel Help

設定を確認し、Finishをクリック

Failover同期の確認

Monitoring → Administration
→ Failover → Statusをクリック

Monitoring > Properties > Failover > Status

Failover state of the system:

```
Failover On
Failover unit Primary
Failover LAM Interface: F0 GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 160 maximum
failover replication http
Version: Ours 8.4(2), Mate 8.4(2)
Last Failover at: 07:38:28 UTC Jul 21 2011
This host: Primary - Active
Active time: 1731 (sec)
slot 0: ASA5520 hw/sw rev (2.0/8.4(2)) status (Up Sys)
Interface inside (10.71.153.20): Normal (Waiting)
```

Make Active Make Standby Reset Failover Reload Standby

一方の状態が'Active'、かつもう一方が'Standby Ready'であれば、フェイルオーバーの同期が正常に確立している。

Failover同期の切り替え、切り戻し

手動にてプライマリ/セカンダリユニットを切り替えることができる。

Cisco ASDM 6.4 for ASA - 10.71.132.170

File View Tools Wizards Window Help

Home Configuration **Monitoring** Save Refresh Back Forward Help

Device List

+ Add - Delete Connect

Find: 10.0.0.1 10.71.132.170 10.71.132.171 10.71.132.172 Go

Properties

- AAA Servers
- Device Access
- Connection Graphs
- CRL
- DNS Cache
- IP Addr
- System Resources Graphs
- WCCP
- Connections
- Per-Process CPU Usage

Interfaces

VPN

Routing

Properties

Logging

Monitoring > Properties > Failover > Status

Failover state of the system:

```
Failover On
Failover unit Primary
Failover LAN Interface: FO GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 160 maximum
failover replication http
Version: Durs 8.4(2), Mate 8.4(2)
Last Failover at: 07:36:26 UTC Jul 21 2011
  This host: Primary - Active
    Active time: 1731 (sec)
  slot 0: ASA5520 hw/sw rev (2.0/8.4(2)) status (Up sys)
    Interface inside (10.71.132.20): Normal (waiting)
```

Make Active Make Standby Reset Failover Reload Standby

Refresh

プライマリユニットを
セカンダリユニットに切り替える。

セカンダリユニットを
プライマリユニットに切り替える。