IT RCSA - Infrastructure

Entity	Apple Bank
Test Name	IT Infrastructure
Test Date	4/9/2021
Process	IT-IFR-P11 Firewall Management
Sub-process	Firewall Security
Risk # and Description	IT-IFR-R11 - Access to firewalls, if not appropriately restricted, can lead to unauthorized changes.
Control # and Description	**IT-IFR-C27 Firewall Changes** Access to firewalls is restricted to designated IT professionals. All changes to the firewalls must follow the Bank's Change Management Policy
Level of Risk	High
Control Frequency	As Needed
Process Owner	Debi Gupta
Procedures Performed for Validating Population	Inquiry, Observation, Inspection
SII(s) or Exception(s) Number(s)	Self Reported by Information Security

Control Test Procedures

Test Step	Test Procedure
A	Determine that changes to firewalls must be appropriately approved Pg. 2, 7, 10, 13, 16
B	Determine that the change approver is not the change implementer Pg. 6, 8, 11, 14, 18
C	Determine that the change implementer is a designated IT professional Pg. 2, 7, 10, 13, 16

Page 2

Report Title:	Change Request Details
Run Date and Time:	2021-03-01 10:09:50 Eastern Standard Time
Run by:	Allen Lum
Table name:	change_request

Change Request

A

Number:	CHG0030415	Approval:	Approved
Requested by:	Michael Lamparello	Type:	Emergency
Category:	Network Infrastructure	State:	Canceled
Configuration item:		On hold:	false
Priority:	2 - High	Conflict status:	Not Run
Risk:	High	Conflict last run:	
Impact:	2 - Medium	Assignment group:	SN-NetworkInfrastructure
		Assigned to:	Michael Lamparello
		Project Name:	

B, C

Short description:

Chanin Cisco Firewalls/Firewall Management Center Software Upgrades

Description:

Upgrade the software running the Cisco Firepower Threat Defense (FTD) firewalls in Chanin, and the Cisco Firepower Management Center (FMC) virtual instance

On hold reason:

Planning

Location Affected by Change:

Justification:

Vulnerabilities have been identified by Qualys which require software upgrades to remediate

Implementation plan:

The Implementation Engineer (Mike Lamparello) will:
1. Download the new version of Cisco-recommended software for both FMC and the FTDs pre-change
2. Perform the software upgrade on the FMC first
3. Push the new code files to the individual firewalls (4) - will be done pre-change
4. Install the new software on the Chanin firewalls ONLY using FMC to facilitate the upgrades

Risk and impact analysis:

Moderate/Low - The firewalls are deployed in High-Availability (HA) pairs; one pair in Chanin, one pair in Scarsdale. We will fail the firewalls over to the secondary devices at both sites and upgrade the primary devices first. After successfully upgrade of the primary devices, we will upgrade the secondary devices. There should be no outage from this work.

Backout plan:

If there are issues, we have the option of reverting back to the original software version of code

Test plan:

Testers will be chosen who can test a majority subset of the firewall rules. Please see the attached document for testers and times.

Schedule

Planned start date:	2020-12-17 18:00:00

Planned end date:	2020-12-18 03:00:00
CAB (date):	2020-12-14

Conflicts

Notes

Watch list:		Work notes list:	

Additional comments:

2020-12-18 07:37:28 - Robert Celona (Additional comments)
reply from: rcelona@applebank.com

FYI - If you were not aware the maintenance was not completed and no
changes were made. Please let me know if anyone has questions. Thanks!

On Wed, Dec 16, 2020 at 3:58 PM Robert Celona <rcelona@applebank.com> wrote:

> Regarding tomorrow's maintenance alert. This is work being performed
> under CHG0030415. Please keep this in mind and escalate immediately if you
> observe anything unusual or we begin to spike calls to Service Desk. Please
> escalate to the leads or myself and do not contact additional support teams
> independently. As always please contact me with questions.
>
> ---------- Forwarded message ---------
> From: Service Desk <helpdesk@applebank.com>
> Date: Wed, Dec 16, 2020 at 3:27 PM
> Subject: *** SERVICE DESK ALERT *** MAINTENANCE ALERT - Chanin Firewall
> IOS Software Upgrades
> To:
>
>
>
>
>
>
> *The Network Infrastructure Team will be performing IOS software upgrades
> on the Firepower Management Center (FMC), as well as the Chanin Firepower
> Threat Defense (FTD) system firewall pair starting at 18:00 EST on
> Thursday, December 17th, and ending at 03:00 EST on Friday, December
> 18th.During this change time window, we do not anticipate any outages.We
> are conducting extensive User Acceptance Testing (UAT) at multiple points
> throughout the change window across many lines of businesses, and will
> report status at every stage of the upgrades.*
>
>
>
> *_________________*
>
> *Service Desk Team*
>
> Email: *servicedesk@applebank.com*
>
> Phone: 646-661-7770
>
> https://applebank.service-now.com/sp
>
>
> --
>
> Robert Celona
>
> AVP, Service Delivery Manager
>

> *Service Desk Team*
>
> Email: *servicedesk@applebank.com <servicedesk@applebank.com>*
>
> Phone: 646-661-7770
>
> ServiceNow Portal: https://applebank.service-now.com/sp
>
>
>

--

Robert Celona

AVP, Service Delivery Manager

Service Desk Team

Email: *servicedesk@applebank.com <servicedesk@applebank.com>*

Phone: 646-661-7770

ServiceNow Portal: https://applebank.service-now.com/sp

Work notes:

2020-12-18 09:08:31 - Joseph Armenti (Work notes)
The virtual server that hosts the FMC application was not configured to Cisco specifications and so we could not install the upgrade to the application.

Closure Information

Status of Change:

Close notes:

Related List Title:	Conflict List
Table name:	conflict
Query Condition:	Change = CHG0030415
Sort Order:	None

Value of property 'glide.pdf.max_rows' must be less or equal than 5,000. Default max row number applied (1,000)

1 Conflicts

Affected CI	Impacted Service	Type	Schedule	Conflicting change	Last checked
		Inside Blackout Window	Change Freeze		2020-12-17 19:00:00

Related List Title: CIs Affected List

Table name: task_ci

Query Condition: Task = CHG0030415

Sort Order: None

Value of property 'glide.pdf.max_rows' must be less or equal than 5,000. Default max row number applied (1,000)

1 CIs Affected

Configuration Item	Class	Discovery State	Discovery Last Updated

Related List Title: Approval List

Table name: sysapproval_approver

Query Condition: Approval for = CHG0030415

Sort Order: Order in ascending order

Value of property 'glide.pdf.max_rows' must be less or equal than 5,000. Default max row number applied (1,000)

3 Approvals

State	Approver	Assignment group	Comments	Created
No Longer Required	Maria Siegel	SN-CAB		2020-12-14 09:04:27
Approved	Joseph Armenti B	SN-CAB	2020-12-14 10:24:10 - Joseph Armenti (Comments) [code][/code]	2020-12-14 09:04:27
No Longer Required	Jose Mendez	SN-CAB		2020-12-14 09:04:27

Related List Title: CAB Agenda Item List

Table name: cab_agenda_item

Query Condition: Change Request = CHG0030415

Sort Order: Order in ascending order

Value of property 'glide.pdf.max_rows' must be less or equal than 5,000. Default max row number applied (1,000)

1 CAB Agenda Items

Meeting	Meeting start time	Meeting end time	Allotted time	State	Decision
Apple Bank - IT Change Advisory Board	2020-12-14 10:00:00	2020-12-14 11:00:00	7 Minutes	Complete	Approved

Report Title:	Change Request Details
Run Date and Time:	2021-03-01 10:13:09 Eastern Standard Time
Run by:	Allen Lum
Table name:	change_request

Change Request

A

Number:	CHG0030424	Approval:	Approved
Requested by:	Michael Lamparello	Type:	Emergency
Category:	Network Infrastructure	State:	Closed
Configuration item:		On hold:	false
Priority:	4 - Low	Conflict status:	Not Run
Risk:		Conflict last run:	
Impact:	3 - Low	Assignment group:	SN-NetworkInfrastructure
		Assigned to:	Michael Lamparello
		Project Name:	

B, C

Short description:

Configure Static Route on Cisco FTD Firewalls

Description:

Add a static route for the two VPN subnets on the Scarsdale FTD firewall pair

On hold reason:

Planning

Location Affected by Change:	Scarsdale - 1075 Central Park Ave

Justification:

This action was recommended by the Cisco TAC engineer who was engaged to solve a high utilization issue seen in the Scarsdale firewalls. The change was approved by the CTO (Debi Gupta) and implemented on 12/16 in the afternoon.

Implementation plan:

Add the static route to the Scarsdale Cisco FTD firewall pair

Risk and impact analysis:

Low/Low - Firewall pushes by nature are a low-risk activity. This change is to add a static route, and will not affect the operation of the firewall nor its rules.

Backout plan:

Remove the route nd push the changes to the firewalls

Test plan:

Observe utilization returning to nominal levels

Schedule

Planned start date:	2020-12-17 15:00:00
Planned end date:	2020-12-17 16:00:00
CAB (date):	

Conflicts

Notes

Watch list:	Work notes list:

Additional comments:

2020-12-17 12:37:55 - Michael Lamparello (Additional comments)
This Emergency Change is being implemented by the request and approval by the CTO, Debi Gupta.

Work notes:

Closure Information

Status of Change:	Successful
Close notes:	With Cisco guidance, Added a static route for the two VPN subnets on the Scarsdale FTD firewall pair to address performance issue

Related List Title:	Conflict List
Table name:	conflict
Query Condition:	Change = CHG0030424
Sort Order:	None

None

Related List Title:	Approval List
Table name:	sysapproval_approver
Query Condition:	Approval for = CHG0030424
Sort Order:	Order in ascending order

Value of property 'glide.pdf.max_rows' must be less or equal than 5,000. Default max row number applied (1,000)

3 Approvals

State	Approver	Assignment group	Comments	Created
No Longer Required	Maria Siegel	SN-CAB		2020-12-17 12:43:11
Approved	Joseph Armenti	SN-CAB		2020-12-17 12:43:11
No Longer Required	Jose Mendez	SN-CAB		2020-12-17 12:43:11

B

Related List Title: Change Task List

Table name: change_task

Query Condition: Change request = CHG0030424

Sort Order: Number in ascending order

Value of property 'glide.pdf.max_rows' must be less or equal than 5,000. Default max row number applied (1,000)

2 Change Tasks

▲ Number	Short description	Type	State	Planned start date	Planned end date	Assignment group	Assigned to
CTASK0010374	Implement	Planning	Closed			SN-NetworkInfrastructure	
CTASK0010375	Post implementation testing	Planning	Closed			SN-NetworkInfrastructure	

Page 10

Report Title:	Change Request Details
Run Date and Time:	2021-03-01 10:13:42 Eastern Standard Time
Run by:	Allen Lum
Table name:	change_request

Change Request

A

Number:	CHG0030441	Approval:	Approved
Requested by:	Michael Lamparello	Type:	Normal
Category:	Network Infrastructure	State:	Closed
Configuration item:	10.254.11.9	On hold:	false
Priority:	4 - Low	Conflict status:	Not Run
Risk:	High	Conflict last run:	
Impact:	3 - Low	Assignment group:	SN-NetworkInfrastructure
		Assigned to:	Michael Lamparello
		Project Name:	

B, C

Short description:

Firewall Rule Push for Upstart Application File Transfer

Description:

Firewall Push to enable file transfer access to Upstart application

On hold reason:

Planning

Location Affected by Change:	NA

Justification:

This change is to provide access from the Apple Bank MoveIt Server to the URL partners-sftp.aws.upstart.com for file transfer services. This will be implemented and tested with the vendor via conference call on January 11th. This new service will be used to issue unsecured loans to consumers by Apple Bank, and is being requested by the Consumer Banking Project Manager. (Gordon Levy)

Implementation plan:

The Implementation Engineer (Mike Lamparello) will:
1. Using FMC, add the requested ip addresses (see attached Firewall Request form) to the existing firewall rule.
2. Push the changes to the firewalls.

Risk and impact analysis:

Low/Low - This is a firewall push which will permit access, not block it.

Backout plan:

The Implementation Engineer (Mike Lamparello) will:
1. Remove the ip addresses from the existing rule using FMC
2. Push the change to the firewalls

Test plan:

Testing will be performed by John Bernstein and the vendor after the rule push has completed

Schedule

Planned start date:	2021-01-11 18:00:00

Planned end date:	2021-01-12 00:00:00
CAB (date):	2021-01-11

Conflicts

Notes

Watch list:		Work notes list:	

Additional comments:

Work notes:

Closure Information

Status of Change:	Successful
Close notes:	Firewall rule pushed but not successfully tested.

Related List Title:	Conflict List
Table name:	conflict
Query Condition:	Change = CHG0030441
Sort Order:	None

None

Related List Title:	Approval List
Table name:	sysapproval_approver
Query Condition:	Approval for = CHG0030441
Sort Order:	Order in ascending order

Value of property 'glide.pdf.max_rows' must be less or equal than 5,000. Default max row number applied (1,000)

4 Approvals

State	Approver	Assignment group	Comments	Created
No Longer Required	Jose Mendez	SN-CAB		2021-01-07 12:53:26
No Longer Required	Maria Siegel	SN-CAB		2021-01-07 12:53:26
Approved	Adolfo Giannasi			2021-01-07 11:36:47
Approved	Joseph Armenti	SN-CAB	2021-01-11 10:15:49 - Joseph Armenti (Comments) [code]<p>Approved</p>[/code]	2021-01-07 12:53:26

B

Related List Title: Change Task List

Table name: change_task

Query Condition: Change request = CHG0030441

Sort Order: Number in ascending order

Value of property 'glide.pdf.max_rows' must be less or equal than 5,000. Default max row number applied (1,000)

2 Change Tasks

▲ Number	Short description	Type	State	Planned start date	Planned end date	Assignment group	Assigned to
CTASK0010400	Post implementation testing	Planning	Closed			SN-NetworkInfrastructure	
CTASK0010401	Implement	Planning	Closed			SN-NetworkInfrastructure	Michael Lamparello

B, C

Related List Title: CAB Agenda Item List

Table name: cab_agenda_item

Query Condition: Change Request = CHG0030441

Sort Order: Order in ascending order

Value of property 'glide.pdf.max_rows' must be less or equal than 5,000. Default max row number applied (1,000)

1 CAB Agenda Items

Meeting	Meeting start time	Meeting end time	Allotted time	State	Decision
Apple Bank - IT Change Advisory Board	2021-01-11 10:00:00	2021-01-11 11:00:00	7 Minutes	Complete	Approved

Report Title:	Change Request Details
Run Date and Time:	2021-03-01 10:14:22 Eastern Standard Time
Run by:	Allen Lum
Table name:	change_request

Change Request

A

Number:	CHG0030584	Approval:	Approved
Requested by:	Ignacio Sanchez	Type:	Normal
Category:	Network Infrastructure	State:	Scheduled
Configuration item:	CI not Listed	On hold:	false
Priority:	4 - Low	Conflict status:	Not Run
Risk:	High	Conflict last run:	
Impact:	3 - Low	Assignment group:	SN-NetworkInfrastructure
		Assigned to:	Ignacio Sanchez
		Project Name:	

B, C

Short description:

Visa firewall rules cleanup on cisco FTD firewalls in Scarsdale

Description:

Adjust visa ATM firewall rules to match ports allowed list provided by Visa and Robert Sovatsky

On hold reason:

Planning

Location Affected by Change:	All

Justification:

Visa ATM fw rules are too permissive allow traffic to more than just the dps host they are expected to connect with

Implementation plan:

Log into FMC, adjust the fw rules to allow access to the port specified by Visa .

Risk and impact analysis:

Possible interruption of visa ATM traffic

Backout plan:

Revert firewall rules to current state

Test plan:

Visa DPS and ATM team will be on the bridge call, at the deployment of the rule change will be able to determine which , if any atm is not communicating properly with Visa

Schedule

Planned start date:	2021-02-25 21:00:37
Planned end date:	2021-02-26 01:00:53
CAB (date):	2021-02-22

Conflicts

Notes

Watch list:	Work notes list:

Additional comments:

Work notes:

Closure Information

Status of Change:

Close notes:

Related List Title: Conflict List

Table name: conflict

Query Condition: Change = CHG0030584

Sort Order: None

None

Related List Title: Approval List

Table name: sysapproval_approver

Query Condition: Approval for = CHG0030584

Sort Order: Order in ascending order

Value of property 'glide.pdf.max_rows' must be less or equal than 5,000. Default max row number applied (1,000)

5 Approvals

B

State	Approver	Assignment group	Comments	Created
Approved	Adolfo Giannasi			2021-02-18 09:09:58
Approved	Joseph Armenti	SN-CAB	2021-02-22 10:32:12 - Joseph Armenti (Comments) [code]<p>Request for Change has been approved by the CAB</p>[/code]	2021-02-19 16:09:18
No Longer Required	Jose Mendez	SN-CAB		2021-02-19 16:09:18
No Longer Required	Michael Lamparello	SN-CAB		2021-02-19 16:09:18
No Longer Required	Maria Siegel	SN-CAB		2021-02-19 16:09:18

Related List Title: CAB Agenda Item List

Table name: cab_agenda_item

Query Condition: Change Request = CHG0030584

Sort Order: Order in ascending order

Value of property 'glide.pdf.max_rows' must be less or equal than 5,000. Default max row number applied (1,000)

1 CAB Agenda Items

Meeting	Meeting start time	Meeting end time	Allotted time	State	Decision
Apple Bank - IT Change Advisory Board	2021-02-22 10:00:00	2021-02-22 11:00:00	7 Minutes	Complete	Approved

Report Title:	Change Request Details
Run Date and Time:	2021-03-01 10:15:24 Eastern Standard Time
Run by:	Allen Lum
Table name:	change_request

Change Request

A

Number:	CHG0030243	Approval:	Approved
Requested by:	Ignacio Sanchez	Type:	Normal
Category:	Network	State:	Closed
Configuration item:	CI not Listed	On hold:	false
Priority:	4 - Low	Conflict status:	No Conflict
Risk:	Moderate	Conflict last run:	2020-11-23 09:49:53
Impact:	3 - Low	Assignment group:	SN-NetworkInfrastructure
		Assigned to:	Ignacio Sanchez
		Project Name:	

Short description:

Upgrade Panorama appliances and Paloalto firewalls to remediate vulnerabilities

Description:

Upgrade Panorama virtual appliances and Palo Alto firewalls from os verson 9.0.9h to version 9.0.10 to remediate vulnerabilites prior to Go live next weekend

On hold reason:

Planning

Location Affected by Change:	All

Justification:

Remediate os vulnerabilities on new firewalls prior to Go live date

Implementation plan:

Backup configuration , fail over, upgrade Scarsdale Panorama appliance, fail over , upgrade Chanin Panorama appliance. Upgrade Paloalto firewalls at Chanin and Scarsdale, upgrading scondary, fail over and upgrade primary

Risk and impact analysis:

There is no expected impact nor outage from this upgrade

Backout plan:

Revert firewalls and Panorama to current OS

Test plan:

Continue using GRE tunnel for test pilot of servers verify firewall operation is working as current , in preparation for go live on 11/20/20

Schedule

Planned start date:	2020-11-12 19:01:09
Planned end date:	2020-11-13 01:01:20
CAB (date):	

Conflicts

Notes

Watch list:		Work notes list:	

Additional comments:

Work notes:

Closure Information

Status of Change:	Successful
Close notes:	Panorama and firewalls updated to version 9.0.10

Related List Title:	Conflict List
Table name:	conflict
Query Condition:	Change = CHG0030243
Sort Order:	None

None

Related List Title:	CIs Affected List
Table name:	task_ci
Query Condition:	Task = CHG0030243
Sort Order:	None

Value of property 'glide.pdf.max_rows' must be less or equal than 5,000. Default max row number applied (1,000)

1 CIs Affected

Configuration Item	Class	Discovery State	Discovery Last Updated
CI not Listed	Configuration Item		

Related List Title:	Approval List
Table name:	sysapproval_approver
Query Condition:	Approval for = CHG0030243
Sort Order:	Order in ascending order

Value of property 'glide.pdf.max_rows' must be less or equal than 5,000. Default max row number applied (1,000)

4 Approvals

B

State	Approver	Assignment group	Comments	Created
Approved	Adolfo Giannasi			2020-11-12 09:02:31
Approved	Joseph Armenti	SN-CAB		2020-11-12 09:48:05
No Longer Required	Maria Siegel	SN-CAB		2020-11-12 09:48:05
No Longer Required	Jose Mendez	SN-CAB		2020-11-12 09:48:05

Related List Title: Change Task List

Table name: change_task

Query Condition: Change request = CHG0030243

Sort Order: Number in ascending order

Value of property 'glide.pdf.max_rows' must be less or equal than 5,000. Default max row number applied (1,000)

2 Change Tasks

▲ Number	Short description	Type	State	Planned start date	Planned end date	Assignment group	Assigned to
CTASK0010271	Post implementation testing	Planning	Closed			SN-NetworkInfrastructure	Ignacio Sanchez
CTASK0010272	Implement	Planning	Closed			SN-NetworkInfrastructure	Ignacio Sanchez

B, C