CIS Forescout Network Access Control STIG Benchmark

v1.0.0 - 08-27-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

Target Technology Details

Forescout Network Access Control Secure Technical Implementation Guide (STIG)

Version: 2 Release: 4 Benchmark

Date: 02 Jul 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Forescout Network Access Control and are looking to comply with the STIG guidance

Recommendation Definitions

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

The Rule Title from the STIG.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Forescout Network Access Control

Recommendations

1 STIG RULES

Forescout Network Access Control

Forescout Network Access Control Secure Technical Implementation Guide (STIG)

Version: 2 Release: 4 Benchmark

Date: 02 Jul 2025

CLASSIFICATION unclassified

1.1 FORE-NC-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Forescout must enforce approved access by employing admissions assessment filters that include, at a minimum, device attributes such as type, IP address, resource group, and/or mission conditions as defined in Forescout System Security Plan (SSP). This is required for compliance with C2C Step 4.

```
GROUP ID: V-233309
RULE ID: SV-233309r811367
```

Rationale:

Successful authentication must not automatically give an entity access to an asset or security boundary. The lack of authorization-based access control could result in the immediate compromise and unauthorized access to sensitive information.

Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Many NACs include the ability to create network access control policies that include identity-based policies, role-based policies, and attribute-based policies.

It is recommended that Forescout have the capability to expose collected data on the assessed endpoints through an API that can be accessed externally, or the NAC solution must supply an SDK to allow customers to export data.

Admissions assessment filters should include, at a minimum, device attributes such as type, IP address, resource group, and/or mission conditions as defined in the Forescout SSP. Forescout should also track the following to facilitate security investigations: when each device was last admitted/readmitted to the network; owning organization; owning organization's organizational unit; geographic location or the nearest network switch; motherboard serial number and BIOS; globally unique ID; and which unique network access compliance policies each device passed or failed during the latest network admission/readmission.

The client may be denied admission based on a returned posture token. In most Forescout implementations, additional network access authorization policies can also be tied to the user's identity, but these features are out of scope for this STIG.

Audit:

If DoD is not at C2C Step 4 or higher, this is not a finding.

Use the Forescout Administrator UI to ensure that the endpoint compliance assessment policies have been implemented per the SSP and are functioning correctly.

If Forescout does not have compliance assessment policies configured this is a finding.

Remediation:

Use the Forescout Administrator UI to configure the endpoint compliance assessment policies per the SSP. Example only:

1. Log on to Forescout UI.
2. From the Policy tab, select the top most policy.
3. Select Add >> Classification >> Primary Classification, and then click "Next".
4. Give the policy a name, then click "Next".
5. If applicable, select the IP Address Range the policy will apply to, click "Ok", and then click "Next".
6. Select "Finish, then click "Apply".

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.2 FORE-NC-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Endpoint policy assessment must proceed after the endpoint attempting access has been identified using an approved identification method such as IP address. This is required for compliance with C2C Step 2.

```
GROUP ID: V-233310
RULE ID: SV-233310r811369
```

Rationale:

Automated policy assessments must reflect the organization's current security policy so entry control decisions will happen only where remote endpoints meet the organization's security requirements. If the remote endpoints are allowed to connect to the organization's network without passing minimum-security controls, they become a threat to the entire network.

Organizational policy must be established for what Forescout will check on the host for the agent and agentless. The Forescout system security plan (SSP) will be used to assess compliance with the requirement since each SSP item must be configured.

Examples include, but are not limited to:

- Verification that anti-virus software is authorized, running, and virus signatures are up to date.
- Host-based firewall installed and configured according to the organization's security policy.
- Host IDS/IPS is installed, operational, and up to date.
- Uses the result of malware, anti-virus, and IDS scans and status as part of the assessment decision process.
- Required BIOS, operating system, browser, and office application patch levels.
- Performs an assessment of the list of running services.
- Test for the presence of DoD-required software.
- Test for presence of peer-to-peer software (not allowed).

Audit:

If DoD is not at C2C Step 2 or higher, this is not a finding.

Use the Forescout Administrator UI to ensure that the endpoint compliance assessment policies have been implemented per the SSP and are functioning correctly.

1. Log on to the Forescout Administrator UI.
2. From the Home screen select the "Policy" tab.
3. Verify that policies exist that assess compliance in accordance with the SSP.

If Forescout does not have compliance assessment policies configured this is a finding.

Remediation:

Use the Forescout Administrator UI to configure the endpoint compliance assessment policies per the SSP.

1. From the console on the Enterprise Manager console, select the Policy tab.
2. In accordance with the SSP, ensure that the endpoint compliance assessment policies have been configured and are functioning properly.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.3 FORE-NC-000030 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

For endpoints that require automated remediation, Forescout must be configured to logically separate endpoints from the trusted network traffic during remediation. This is required for compliance with C2C Step 4.

```
GROUP ID: V-233311
RULE ID: SV-233311r1018659
```

Rationale:

Automated and manual procedures for remediation for critical security updates will be managed differently. Continuing to assess and remediate endpoints with risks that could endanger the network could impact network usage for all users. This isolation prevents traffic from flowing with traffic from endpoints that have been fully assessed and authorized.

This requirement does not mandate a remediation network be used, but rather requires that it be secured where used. For example, unauthenticated devices must not be allowed to connect to remediation networks.

Many sites block unauthorized traffic directly using the Forescout. Forescout accepts only endpoints with IP addresses that are in range. Configure Forescout to identify the endpoint. By default, the IP address is used as the endpoint identifier. The system can be configured to capture the following other endpoint unique identifiers if approved for use by the SSP as the identification method: BIOS Serial number and other hardcoded attributes, OS host name, etc.

Audit:

If DOD is not at C2C Step 4 or higher, this is not a finding.

If a separate remediation network is configured and isolated from the trusted network, this is not a finding.

Use the Forescout Administrator UI to verify that Forescout is configured to either redirect endpoints requiring automated remediation to a network segment that is isolated from trusted traffic or, if assessment is done on the Forescout, the endpoint traffic is logically separate during remediation.

If Forescout does not isolate endpoints during remediation, this is a finding.

Remediation:

Use the Forescout Administrator UI to configure a policy, per the SSP, that isolates endpoints requiring automated remediation from other endpoints on the trusted network. The following is an example only.

1. From the Policy tab, select the top most policy.
2. Select Add >> Classification >> Primary Classification, and then click Next.
3. Give the policy a name, then click Next.
4. Select the IP Address Range the policy will apply to, click "OK," and then click "Next".
5. Select "Finish", and then click "Apply".

This collects a series of attributes for each endpoint that can then be used in a policy as the unique identifier. However, by default the IP address is used, for example in the log records.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.4 FORE-NC-000040 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

If a device requesting access fails Forescout policy assessment, Forescout must communicate with other components and the switch to either terminate the session or isolate the device from the trusted network for remediation. This is required for compliance with C2C Step 3.

```
GROUP ID: V-233312
RULE ID: SV-233312r1113801
```

Rationale:

Endpoints with identified security flaws and weaknesses endanger the network and other devices on it. Isolation or termination prevents traffic from flowing with traffic from endpoints that have been fully assessed and authorized.

Audit:

If DOD is not at C2C Step 3 or higher, this is not a finding.

Use the Forescout Administrator UI to verify that policies are configured to filter the policy assessment devices based on risk and are remediated or isolated according to the SSP.

1. In the Forescout UI, go to the Policy Tab >> Compliance or Control Policies.
2. Verify the action within Compliance Policies is configured with one of the following actions:
    - Terminate the connection and place the device on a denylist to prevent future connection attempts until action is taken to remove the device from the denylist.
    - Redirect traffic from the remote endpoint to the automated remediation subnet for connection to the remediation server or segment the endpoint to a remediation VLAN. Use of ACLs or a VLAN solution is acceptable.
    - Allow the device access to limited network services such as public web servers in the protected DMZ (must be approved by the authorizing official [AO]).
    - Allow the device and user full entry into the protected networks, but flag it for future remediation. With this option, an automated reminder should be used to inform the user of the remediation status.

If Forescout does not communicate with the remote access gateway to implement a policy to either terminate the session or isolate the device from the trusted network this is a finding.

Remediation:

Use the Forescout Administrator UI to configure policies according to the SSP to filter assessed devices based on risk. Ensure the policies remediate or segment the at-risk devices according to the SSP.

1. In the Forescout UI, go to the Policy Tab >> Compliance or Control Policies.
2. Select a policy, then click “Edit”.
3. Configure the Compliance Policies to include any of the following actions:
    - Terminate the connection and place the device on a denylist to prevent future connection attempts until action is taken to remove the device from the denylist.
    - Redirect traffic from the remote endpoint to the automated remediation subnet for connection to the remediation server or segment the endpoint to a remediation VLAN. Use of ACLs or a VLAN solution is acceptable.
    - Allow the device access to limited network services such as public web servers in the protected DMZ (must be approved by the AO).
    - Allow the device and user full entry into the protected networks, but flag it for future remediation. With this option, an automated reminder must be used to inform the user of the remediation status.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.5 FORE-NC-000050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must be configured to notify the user before proceeding with remediation of the user's endpoint device when automated remediation is used. This is required for compliance with C2C Step 3.

```
GROUP ID: V-233313
RULE ID: SV-233313r1113802
```

Rationale:

Connections that bypass established security controls should be allowed only in cases of administrative need. These procedures and use cases must be approved by the information system security manager (ISSM).

Unless an exception is approved to not require notification of the user, the following configurations must be implemented:

- This setting may be sent from the assessment server, a central server, or from the remediation server.
- Verify the user is notified and accepts (e.g., using an accept button) that remediation is needed and is about to begin.

Audit:

If DOD is not at C2C Step 3 or higher, this is not a finding.

Check Forescout policy to ensure that exempt devices that are in need of remediation prompt the user to accept the remediation process, prior to conducting.

1. Log on to the Forescout UI.
2. Select the "Policy" tab.
3. Review the compliance policy identified by the site representation as the remediation policy, then click "Edit".
4. In the Sub-Rules section, select a policy and click "Edit".
5. From the Actions section, verify that the policy is configured to notify the user, prior to remediation, that user interaction is required.

If Forescout is not configured to notify the user before proceeding with remediation of the user's endpoint device when automated remediation is used, this is a finding.

Remediation:

Log on to the Forescout UI.

1. Select the "Policy" tab.
2. Select a compliance policy, then click "Edit".
3. In the Sub-Rules section, select a policy and click "Edit".
4. From the Actions section, click Add >> Notify >> and select a notification method.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.6 FORE-NC-000060 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Forescout must be configured so that all client machines are assessed by Forescout with exceptions that are allowed to bypass Forescout based on account or account type, as approved by the information system security manager (ISSM) and documented in the System Security Plan (SSP). This is required for compliance with C2C Step 1.

```
GROUP ID: V-233314
RULE ID: SV-233314r919219
```

Rationale:

The NAC gateway provides the policy enforcement allowing or denying the endpoint to the network. Unauthorized endpoints that bypass this control present a risk to the organization's data and network.

The focus of this requirement is on identification, documentation, and approval of devices that will bypass the NAC. This is not a requirement that all traffic flow through the NAC.

Audit:

If DOD is not at C2C Step 1 or higher, this is not a finding.

If traffic is not allowed to bypass the NAC policy, this is not a finding.

Use the Forescout Administrator UI to verify a policy exists that uses the exemption group configured so that all client machines are assessed by Forescout with exceptions that are allowed to bypass Forescout based on the account or account type, as approved by the ISSM and documented in the SSP.

1. In the filters pane under Groups, right-click the group editor. Pick the group indicated as compliance by the site representative.
2. Click "Scope" and review the Exemptions Group.

If Forescout is not configured to approve all instances where traffic is allowed to bypass the NAC as approved by the ISSM, this is a finding.

Remediation:

Use the Forescout Administrator UI to configure an exception group that is defined in the SSP and ensure policy is applied to the group that allows NAC bypass.

Create a group based on the exemptions in the SSP.

1. In the filters pane under Groups, right-click the group editor. Pick or create an exemption group.
2. Add a name and then add the scope based on IP range or Subnet, or based on MAC Address.
3. Click "OK" and then click "OK" again. Click "Yes" for "Are you sure?".

Create a policy that uses the exemption group.

1. In the Views pane, click "Authentication & Authorization".
2. Select an existing policy and edit the Scope to add the Exemptions Group.
3. In Exceptions type, select "Group".
4. In the Policy screen, select the exceptions group created in the prior step, click "OK" several times, and then click "Apply".

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.7 FORE-NC-000090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

When devices fail the policy assessment, Forescout must create a record with sufficient detail suitable for forwarding to a remediation server for automated remediation or sending to the user for manual remediation. This is required for compliance with C2C Step 3.

```
GROUP ID: V-233317
RULE ID: SV-233317r811383
```

Rationale:

Notifications sent to the user and/or network administrator informing them of remediation requirements will ensure that action is taken.

Audit:

If DoD is not at C2C Step 3 or higher, this is not a finding.

Verify Forescout sends user and/or admin notification of remediation requirements, whether manual or automated.

If the NAC does not flag for future manual or automated remediation, devices failing policy assessment that are not automatically remediated either before or during the remote access session, this a finding.

Remediation:

Log on to the Forescout UI.

1. Within the Policy tab, locate the Compliance policies.
2. Within the policy Sub-Rule, ensure all policies that indicate remediation have been configured to notify the user and/or network administrator of required action.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.8 FORE-NC-000100 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Forescout must place client machines on a blacklist or terminate network communications on devices when critical security issues are found that put the network at risk. This is required for compliance with C2C Step 4.

```
GROUP ID: V-233318
RULE ID: SV-233318r811385
```

Rationale:

Devices that are found to have critical security issues place the network at risk if they are allowed to continue communications. Policy actions should be in place to terminate or restrict network communication or place the suspicious machine on a blacklist.

Audit:

If DoD is not at C2C Step 4 or higher, this is not a finding.

Check Forescout policy to ensure that any device with a critical security issue is checked through a security policy and an action is taken to either blacklist it or terminate communication with other network devices.

If the NAC does not immediately place the device on the blacklist and terminate the connection when critical security issues are found that put the network at immediate risk, this a finding.

Remediation:

Use the Forescout Administrator UI to configure compliance policies to ensure any device with critical security issues is added to a blacklist, had its network communication blocked, or isolated from trusted network traffic for remediation.

1. From the Policy tab, identify a Compliance policy.
2. Within the Compliance policy, under Sub-Rule for a device with critical security issues, ensure that an action that Adds Device to Blacklist and/or Disables Device is enabled.

If Forescout does not place client machines on a blacklist or terminate network communications on devices when critical security issues are found that put the network at risk, this is a finding.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.9 FORE-NC-000110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must be configured so client machines do not communicate with other network devices in the DMZ or subnet except as needed to perform an access client assessment or to identify themselves. This is required for compliance with C2C Step 2.

```
GROUP ID: V-233319
RULE ID: SV-233319r1111892
```

Rationale:

Devices not compliant with DOD secure configuration policies are vulnerable to attack. While endpoints are undergoing NAC authorization assessment, they must communicate only with the NAC. These devices should not communicate with other hosts in the DMZ or other network segments.

Audit:

If DOD is not at C2C Step 2 or higher, this is not a finding.

Verify ForeScout is configured so endpoints under assessment are isolated from peer communication.

1. Navigate to the Policy tab and examine the Compliance Assessment policy.
2. Verify either a Quarantine VLAN, ACL Enforcement Method, or Forescout Virtual Firewall is configured as part of the policy.

If Forescout allows endpoints under assessment to communicate with other endpoints in the DMZ or on other network segments, this is a finding.

Remediation:

Configure ForeScout so devices being assessed for compliance do not communicate with other devices in the DMZ or other network segments. There are different approaches; however, this typically involves isolating noncompliant devices into a quarantine or assessment zone until they meet compliance requirements.

The following are examples.

Create a Quarantine VLAN:

1. Set up a dedicated VLAN (e.g., "Quarantine_VLAN") for devices under assessment.
2. This VLAN should have restricted access, blocking communication to other devices or production network segments.
3. Allow traffic only to specific remediation servers (e.g., patch servers, ForeScout appliance for assessment).
4. Configure the switches to support dynamic VLAN assignment via CounterACT.
5. Enforce Network Isolation using a VLAN:

- Select the "Quarantine_VLAN".
- CounterACT will instruct the switch (via SNMP or CLI) to move the device to this VLAN upon detection.

Or
ACL Enforcement Method:

1. If VLANs are not feasible, use the **Apply ACL** action.
2. Configure an ACL on the switches or routers to block all traffic from the device's IP or MAC to other network devices, allowing only traffic to remediation servers (e.g., IP of patch server, DNS, or CounterACT appliance).
3. Example ACL (syntax depends on the switch/router):

```
deny ip <device_IP> 0.0.0.0 <network_range> <network_mask>
permit ip <device_IP> 0.0.0.0 <remediation_server_IP> 0.0.0.0
permit ip <device_IP> 0.0.0.0 <forescout_IP> 0.0.0.0
deny ip any any
```

Or

Virtual Firewall Method:

1. Use CounterACT's Virtual Firewall action to block all traffic from the device except to specific IPs/ports (e.g., remediation servers, CounterACT).
2. Configure rules in the action settings to allow only necessary outbound traffic.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.10 FORE-NC-000120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must enforce the revocation of endpoint access authorizations when devices are removed from an authorization group. This is required for compliance with C2C Step 4.

```
GROUP ID: V-233320
RULE ID: SV-233320r1001246
```

Rationale:

Ensuring the conditions that are configured in policy have proper time limits set to reflect changes will allow for proper access. This will help to validate that authorized individuals have proper access.

Audit:

If DOD is not at C2C Step 4 or higher, this is not a finding.

Verify Forescout admission policy has been configured to revoke access to endpoints that have not met or are removed from the authorized group.

If Forescout is not configured with an admissions policy that enforces the revocation of endpoint access authorizations based on when devices are removed from an authorization group, this is a finding.

Remediation:

Use the Forescout Administrator UI to configure the authorization policy to take a control action on any devices that have not met authorization requirement or are no longer authorized.

1. Log on to the Forescout UI.
2. From the Policy tab, check that the authorization policy has a Block Action enabled on any devices that have not met or are removed from the authorized group.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.11 FORE-NC-000130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must enforce the revocation of endpoint access authorizations at the next compliance assessment interval based on changes to the compliance assessment security policy. This is required for compliance with C2C Step 4.

```
GROUP ID: V-233321
RULE ID: SV-233321r1001247
```

Rationale:

This requirement gives the option to configure for automated remediation and/or manual remediation. A detailed record must be passed to the remediation server for action. Alternatively, the details can be passed in a notice to the user for action. The device status will be updated on the network access server/authentication server so that further access attempts are denied. The NAC must have policy assessment mechanisms with granular control to distinguish between access restrictions based on the criticality of the software or setting failure.

Audit:

If DOD is not at C2C Step 4 or higher, this is not a finding.

Verify Forescout admission policy has been configured to revoke access to endpoints that have not met or are removed from the authorized group.

If Forescout is not configured with an admissions policy that enforces the revocation of endpoint access authorizations based on when devices are removed from an authorization group, this is a finding.

Remediation:

Use the Forescout Administrator UI to configure the authorization policy to configured to perform a control action on any devices that have not met authorization requirement or are no longer authorized.

1. Log on to the Forescout UI.
2. From the Policy tab, check that the authorization policy has a Block Action enabled on any devices that have not met or are removed from the authorized group.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.12 FORE-NC-000140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must deny or restrict access for endpoints that fail critical endpoint security checks. This is required for compliance with C2C Step 4.

```
GROUP ID: V-233322
RULE ID: SV-233322r1001248
```

Rationale:

Devices that do not meet minimum-security configuration requirements pose a risk to the DOD network and information assets.

Endpoint devices must be disconnected or given limited access as designated by the approval authority and system owner if the device fails the authentication or security assessment. The user will be presented with a limited portal, which does not include access options for sensitive resources. Required security checks must implement DOD policy requirements.

Audit:

If DOD is not at C2C Step 4 or higher, this is not a finding.

Verify Forescout has been configured to redirect filtered devices to a limited access network to include a remediation network or limited access network.

If a policy does not exist that redirects the failed device to an authorized network for remediation or limited access, this is not a finding.

If the NAC does not deny or restrict access for endpoints that fail critical endpoint security checks, this is a finding.

Remediation:

Use the Forescout Administrator UI to configure any pre-connect policies to ensure endpoints that fail the baseline security configuration requirements are set to either restrict access or isolate the endpoint.

1. Log on to the Forescout UI.
2. From the Policy tab, check any Pre-Connect policies to ensure devices that fail the baseline security configuration requirements are set to either restrict access to production network, are granted access to only remediation network, or are granted to a limited access network.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.13 FORE-NC-000160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must off-load log records onto a different system. This is required for compliance with C2C Step 1.

```
GROUP ID: V-233324
RULE ID: SV-233324r1113796
```

Rationale:

Having a separate, secure location for log records is essential to the preservation of logs as required by policy.

Satisfies: SRG-NET-000492-NAC-002110, SRG-NET-000334-NAC-001350

Audit:

If DOD is not at C2C Step 1 or higher, this is not a finding.

1. Go to Tools >> Options >> Syslog.
2. Verify a syslog server's IP address is configured.

Or

1. Go to Tools >> Options.
2. Navigate to the extended module (e.g., Splunk) that offloads log records to a separate device.
3. Verify the connection is successful.

If each Forescout device does not offload log records to a separate device, this is a finding.

Remediation:

Configure Syslog server with TCP, as well as configure Syslog to alert if the communication between the Syslog server and the Forescout appliance loses connectivity.

1. Go to Tools >> Options >> Syslog.
2. Click "Add/Edit".
3. Configure the Syslog:

- Navigate to Syslog Server IP address >> Server Port >> Server Protocol set to TCP.
- Check the Use TLS setting.
- Configure the Identity, Facility, and Severity.

4. Click "Ok".
5. Click "Apply".

Or
Configure external module (e.g., Splunk) per instructions to send appliance logs from each Forescout appliance to the separate destination.

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4::AU-4 (1)
- NIST SP 800-53 Revision 5::AU-4 (1)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

1.14 FORE-NC-000170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must generate a critical alert to be sent to the Information System Security Officer (ISSO) and Systems Administrator (SA) (at a minimum) in the event of an audit processing failure. This is required for compliance with C2C Step 1.

```
GROUP ID: V-233325
RULE ID: SV-233325r1113798
```

Rationale:

Ensuring that a security solution alerts in the event of misconfiguration or error is imperative to ensuring that proper auditing is being conducted. Having the ability to immediately notify an administrator when this auditing fails allows for a quick response and real-time remediation.

Audit:

If DOD is not at C2C Step 1 or higher, this is not a finding.

Verify Forescout sends an alert to the proper security personnel when an audit process failure occurs.

1. Log on to the Forescout UI.
2. Locate the audit process policies as identified by the site representative.
3. Verify a policy for "audit failure" exists.
4. Verify this policy includes notification of security personnel as follows.
5. a. Navigate to Options >> General >> Mail and DNS.
6. b. Verify the configuration of the appropriate Operator Email and mail relay information to ensure alerts and notifications are being sent to the appropriate people.
7. c. Verify that any policies that need notification actions have one of the following actions configured:

- Send Email.
- Send Email to User.
- Send Balloon Notification.
- HTTP Notification.
- Splunk: Send Update from CounterACT.

If Forescout does not send an alert when an audit processing failure occurs, this is a finding.

Remediation:

Log on to the Forescout UI.

1. Locate the audit process policies as identified by the site representative.
2. Configure a policy for audit failure to include the notification of security personnel. This could also include sending a balloon message, notification, or email as follows.
3. a. Navigate to Options >> General >> Mail and DNS.
4. b. Configure the appropriate Operator Email and mail relay information to ensure alerts and notifications are being sent to the appropriate people.
5. c. Additionally, ensure that any policies that need notification actions have one of the following actions configured:

- Send Email.
- Send Email to User.
- Send Balloon Notification.
- HTTP Notification.
- Splunk: Send Update from CounterACT.

Additional Information:

CCI-001858 Provide an alert in an organization-defined real-time-period to organization-defined personnel, roles, and/or locations when organization-defined audit failure events requiring real-time alerts occur.

- NIST SP 800-53 Revision 4::AU-5 (2)
- NIST SP 800-53 Revision 5::AU-5 (2)

1.15 FORE-NC-000180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must authenticate all endpoint devices before establishing a connection and proceeding with posture assessment. This is required for compliance with C2C Step 4.

```
GROUP ID: V-233326
RULE ID: SV-233326r856512
```

Rationale:

Authenticating all devices as they connect to the network is the baseline of a good security solution. This is especially important prior to posture assessment to ensure authorized devices are online and have the proper posture prior to accessing the production network.

Device authentication is a solution enabling an organization to manage devices. It is an additional layer of authentication ensuring that only specific preauthorized devices can access the system. Authentication methods for NAC include, but are not limited to, Kerberos, MAC, or other protocols.

The IP Assignment Forescout configuration ensures any IP addresses that should be managed by the configured network will go through the policies within Forescout. Forescout policy structure is applied in a "waterfall" like way that assures all IP addresses start with the top most policy and flow down the policy tree. This policy flow ensures that all endpoints are properly identified, classified, and authenticated prior to the posture assessment.

Audit:

If DoD is not at C2C Step 4 or higher, this is not a finding.

Use the Forescout Administrator UI to verify all IP addresses identified in the SSP are configured within the Appliance IP Assignments list.

1. Log on to the Forescout UI.
2. Select Tools >> Option >> Appliance >> IP Assignment.
3. Verify all IP addresses associated with the SSP are labeled within the IP Assignments list.

If Forescout does not authenticate all endpoints prior to establishing a connection and proceeding with posture assessment, this is a finding.

Remediation:

Use the Forescout Administrator UI to configure the Appliance IP Assignments list with all IP addresses identified within the SSP.

1. Log on to the Forescout UI.
2. Select Tools >> Option >> Appliance >> IP Assignment.
3. Configure IP addresses associated with the SSP and label within the IP Assignments list, and then select "Apply".

Additional Information:

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

1.16 FORE-NC-000190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must be configured to apply dynamic ACLs that restrict the use of ports when non-entity endpoints are connected using MAC Authentication Bypass (MAB). This is required for compliance with C2C Step 4.

```
GROUP ID: V-233327
RULE ID: SV-233327r1113800
```

Rationale:

MAB is only one way of connecting non-entity endpoints, and can be defeated by spoofing the MAC address of an assumed authorized device. By adding the device to the MAR, the device can then gain access to the network.

NPE devices that can support PKI or an allowed authentication type must use PKI. MAB may be used for NPE that cannot support an approved device authentication. Non-entity endpoints include Internet of Things (IoT) devices, VoIP phone, and printer.

Audit:

If DOD is not at C2C Step 4 or higher, this is not a finding.

Verify Forescout applies dynamic ACLs (or VLAN restrictions) that restrict the use of ports when nonentity endpoints are connected using MAC Address Repository (MAR).

If the NAC does not apply dynamic ACLs (or VLAN restrictions) that restrict the use of ports when nonentity endpoints are connected using MAR, this is a finding.

Remediation:

Use the Forescout Administrator UI to configure the policy which identifies nonentity endpoints to complete a control action when a device is added to the MAR.

1. Log on to Forescout UI.
2. In the Policy tab, locate the Authentication and Authorization policy set.
3. Select a policy that identifies nonentity endpoints. Highlight the policy, then select "Edit".
4. From the Sub-Rules section, ensure that when a device is added to the MAR, the policy also applies one of the following actions:
5. -Access Port ACL.
6. -Endpoint Address ACL.
7. -WLAN Role.
8. -VLAN Change.

Additional Information:

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

1.17 FORE-NC-000210 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must reveal error messages only to the Information System Security Officer (ISSO), Information System Security Manager (ISSM), and System Administrator (SA). This is required for compliance with C2C Step 1.

```
GROUP ID: V-233328
RULE ID: SV-233328r811406
```

Rationale:

Ensuring the proper amount of information is provided to the Security Management staff is imperative to ensure role based access control. Only those individuals that need to know about a security error of an application need to be notified of the error.

Audit:

If DoD is not at C2C Step 1 or higher, this is not a finding.

Use the Forescout Administrator UI to verify only individuals authorized by the SSP are configured to receive error messages.

1. Log on to the Forescout UI.
2. Within the highlighted policy, under the Actions section, select a configured action to view.
3. Find the Notify section and verify that only authorized individuals (IAW the SSP) are configured for the following:

- HTTP Notification
- Send Email
- Send Notification

If Forescout error messages can be viewed by unauthorized users other than the security personnel that have a need to know, this is a finding.

Remediation:

Use the Forescout Administrator UI to configure the individuals authorized by the SSP to receive error messages.

1. Log on to the Forescout UI.
2. Within the highlighted policy, under the Actions section, select "Add" or "Edit".
3. Find the Notify section and select from any one of the below options for notifying authorized (IAW SSP) personnel:

- HTTP Notification
- Send Email
- Send Notification

Additional Information:

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a
- NIST SP 800-53 Revision 5::SI-11 a

1.18 FORE-NC-000230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must configure TCP for the syslog protocol to allow for detection by the central event server if communications is lost. This is required for compliance with C2C Step 1.

```
GROUP ID: V-233329
RULE ID: SV-233329r811408
```

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability and system operation may be adversely affected.

Note that this configuration allows for the central log server to be configured with a critical alert to be sent to the System Security Officer (ISSO) and Systems Administrator (SA) (at a minimum) if it is unable to communicate the Forescout or stops receiving log updates. The alert requirement is in the Syslog STIG.

Audit:

If DoD is not at C2C Step 1 or higher, this is not a finding.

1. Go to Tools >> Options >> Syslog.
2. Verify the Server Protocol is set to TCP.
3. Verify "Use TLS" setting is set.
4. Verify the "Identity, Facility, and Severity" setting is configured.

If Forescout does not use TCP for the syslog protocol, this is a finding.

Remediation:

Configure Syslog server with TCP, as well as configure Syslog to alert if the communication between the Syslog server and the Forescout appliance loses connectivity.

1. Go to Tools >> Options >> Syslog.
2. Click Add/Edit.
3. Configure the Syslog:

- Syslog Server IP address
- Server Port
- Server Protocol set to TCP
- Check the Use TLS setting
- Configure the Identity, Facility, and Severity.

4. Click "OK".
5. Click "Apply".

Additional Information:

CCI-000139 Alert organization-defined personnel or roles within an organization-defined time period in the event of an audit logging process failure.

- NIST SP 800-53::AU-5 a
- NIST SP 800-53A::AU-5.1 (ii)
- NIST SP 800-53 Revision 4::AU-5 a
- NIST SP 800-53 Revision 5::AU-5 a

1.19 FORE-NC-000240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout switch module must only allow a maximum of one registered MAC address per access port. This is required for compliance with C2C Step 4.

```
GROUP ID: V-233330
RULE ID: SV-233330r1113804
```

Rationale:

Limiting the number of MAC addresses that can access from the same switch access port can help prevent a CAM table overflow attack. This type of attack lets an attacker exploit the hardware and memory limitations of a switch. If there are enough entries stored in a CAM table before the expiration of other entries, no new entries can be accepted into the CAM table. An attacker will be able to flood the switch with mostly invalid MAC addresses until the CAM table's resources have been depleted. When there are no more resources, the switch has no choice but to flood all ports within the VLAN with all incoming traffic. This happens because the switch cannot find the switch port number for a corresponding MAC address within the CAM table, allowing the switch to become a hub and traffic to be monitored.

Some technologies are exempt from requiring a single MAC address per access port; however, restrictions still apply. VoIP or VTC endpoints may provide a PC port so a PC can be connected. Each of the devices will need to be statically assigned to each access port.

Hot-desking is where several people are assigned to work at the same desk at different times, each user with their own PC. In this case, a different MAC address needs to be permitted for each PC that is connecting to the LAN drop in the workspace. Additionally, this workspace could contain a single phone (and possibly desktop VTC endpoint) used by all assignees, and the PC port on it might be the connection for their laptop. In this case, it is best not to use sticky port security but to use a static mapping of authorized devices.

Note: For Forescout, setting the "Maximum connected endpoints per port" to "1" does not prevent multiple MAC addresses from being connected. This setting will cause Forescout to ignore any switch port that has more than "1" MAC address connected. Enable this option to detect endpoints that are connected to the trunk ports of a managed switch. The plugin resolves and displays in the Console the switch properties of these connected endpoints, including the VLAN-related properties Switch Port VLAN, Switch Port VLAN Name, and Switch Port VLAN Change. To use this option, add the uplink port names of the managed switch in the "Don’t learn on port names" field. The plugin ignores learn events for those uplink ports. If needed for use of this option, modify the "Maximum connected endpoints per port" field to increase its value to allow plugin detection of multiple endpoints concurrently connected to the same switch port. The field’s default value is 10 (endpoints). The updated value must reflect the maximum number of endpoints that can be concurrently connected to the same port. This setting may hinder visibility for larger switches.

Audit:

If DOD is not at C2C Step 4 or higher, this is not a finding.

Review the switch configuration to verify each access port is configured for a single registered MAC address.

1. Log on to the Forescout UI.
2. Go to Tools >> Options >> Switch >> Permissions >> Advanced.
3. Verify the "Maximum connected endpoints per port" is set to "1".

If Forescout switch is not configured to permit a maximum of one registered MAC address per access port, this is a finding.

Remediation:

Forescout has the ability to configure the amount of maximum connected endpoints per port. Allowing only one MAC address per port will break VOIP. Function is handled by the switch.

1. Log on to the Forescout UI.
2. Go to Tools >> Options >> Switch >> Permissions >> Advanced.
3. Set the Maximum connected endpoints per port to one.

Additional Information:

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

1.20 FORE-NC-000260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

For TLS connections, Forescout must automatically terminate the session when a client certificate is requested and the client does not have a suitable certificate. This is required for compliance with C2C Step 1.

```
GROUP ID: V-233331
RULE ID: SV-233331r856515
```

Rationale:

In accordance with NIST SP 800-52, the TLS server must terminate the connection with a fatal “handshake failure” alert when a client certificate is requested and the client does not have a suitable certificate.

During the TLS handshake negotiation, a "client certificate request" that includes a list of the types of certificates supported and the Distinguished Names of acceptable Certification Authorities (CAs) is sent to the client.

TLS handshake enables the SSL or TLS client and server to establish the secret keys with which they communicate.

Audit:

If DoD is not at C2C Step 1 or higher, this is not a finding.

Verify Forescout is configured to a list of DoD-approved certificate types and CAs.

Verify the TLS session is configured to automatically terminate any session if the client does not have a suitable certificate.

For TLS connections, if Forescout is not configured to automatically terminate the session when the client does not have a suitable certificate, this is a finding.

Remediation:

Use the Forescout Administrator UI to configure the certificate options to require the Re-verify TLS Sessions is set to every 1 day, or in accordance with the SSP.

1. Log on to the Forescout UI.
2. Select Tools >> Options >> Certificates.
3. Check that in the Ongoing TLS Sessions section, view the Re-verify TLS Sessions.
4. Change the Re-verify TLS Sessions to Every 1 Day or in accordance with the site's SSP, then click "Apply".
5. Next, select the HPS Inspection Engine >> SecureConnector.
6. In the Client-Server Connection, ensure the Minimum Supported TLS Version is set to TLS version 1.2.

Additional Information:

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

1.21 FORE-NC-000270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must use TLS 1.2, at a minimum, to protect the confidentiality of information passed between the endpoint agent and Forescout for the purposes of client posture assessment. This is required for compliance with C2C Step 1.

```
GROUP ID: V-233332
RULE ID: SV-233332r811414
```

Rationale:

Using older unauthorized versions or incorrectly configuring protocol negotiation makes the gateway vulnerable to known and unknown attacks that exploit vulnerabilities in this protocol.

Audit:

If DoD is not at C2C Step 1 or higher, this is not a finding.

Verify Forescout is configured to a list of DoD-approved certificate types and CAs.

Verify the TLS session is configured to automatically terminate any session if the client does not have a suitable certificate.

For TLS connections, if Forescout is not configured to use TLS 1.2 at a minimum, this is a finding.

Remediation:

Configure the SecureConnector to ensure the minimum supported TLS version is set to TLS 1.2.

Log on to the Forescout UI.

1. Select Tools >> Options >> Certificates.
2. Check the Ongoing TLS Sessions section, view the Re-verify TLS Sessions.
3. Change the Re-verify TLS Sessions to Every 1 Day or in accordance with the site's SSP, then click "Apply".
4. Next, select the HPS Inspection Engine >> SecureConnector.
5. In the Client-Server Connection, ensure the Minimum Supported TLS Version is set to TLS version 1.2.

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.22 FORE-NC-000290 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Communications between Forescout endpoint agent and the switch must transmit access authorization information via a protected path using a cryptographic mechanism. This is required for compliance with C2C Step 1.

```
GROUP ID: V-233334
RULE ID: SV-233334r1001245
```

Rationale:

Forescout solution assesses the compliance posture of each client and returns an access decision based on configured security policy. The communications associated with this traffic must be protected from alteration and spoofing attacks so unauthorized devices do not gain access to the network.

Audit:

If DOD is not at C2C Step 1 or higher, this is not a finding.

Verify both ends are configured for secure communications between the NAC and NAC agent.

If communication between the NAC and NAC agent does not use an encrypted method for protecting posture information transmitted between the devices, this is a finding.

Remediation:

Log on to the Forescout UI.

1. Select Tools >> Option >> HPS Inspection Engine >> SecureConnector.
2. In the Client-Server Connection, check the Minimum Supported TLS Version is set to TLS version 1.2.

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.23 FORE-NC-000440 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must perform continuous detection and tracking of endpoint devices attached to the network. This is required for compliance with C2C Step 1.

```
GROUP ID: V-233337
RULE ID: SV-233337r811425
```

Rationale:

Continuous scanning capabilities on the NAC provide visibility of devices that are connected to the switch ports. The NAC continuously scans networks and monitors the activity of managed and unmanaged devices, which can be personally owned or rogue endpoints. Because many of today's small devices do not include agents, an agentless discovery is often combined to cover more types of equipment.

Audit:

If DoD is not at C2C Step 1 or higher, this is not a finding.

Verify the NAC performs continuous detection and tracking of endpoint devices attached to the network.

1. Log on to the Forescout UI.
2. Go to Tools >> Options >> Appliance >> IP Assignment.
3. Check that all IP addresses that should be managed are within the IP Assignments as required by the SSP.

If the NAC does not perform continuous detection and tracking of endpoint devices attached to the network, this is a finding.

Remediation:

Log on to the Forescout UI.

1. Go to Tools >> Options >> Appliance >> IP Assignment.
2. Enter all IP addresses to be managed in the IP Assignment to enable the continuous monitoring capabilities of Forescout.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.24 FORE-NC-000450 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must deny network connection for endpoints that cannot be authenticated using an approved method. This is required for compliance with C2C Step 4.

```
GROUP ID: V-233338
RULE ID: SV-233338r811427
```

Rationale:

Without identifying devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity. Identification failure does not need to result in connection termination or preclude compliance assessment. This is particularly true for unmanaged systems or when the NAC is performing network discovery.

Audit:

If DoD is not at C2C Step 4 or higher, this is not a finding.

Use the Forescout Administrator UI to verify that a policy exists to deny network connections for endpoints that cannot be authenticated using an approved method and that the authentication failure is logged.

1. Log on to Forescout UI.
2. From the Policy tab, select the Authentication and Authorization policy.
3. Find the 802.1x Authorization policy.

If NAC does not have an authorization policy that denies network connection for endpoints that cannot be authenticated using an approved method and log authentication failures, this is a finding.

Remediation:

Use the Forescout Administrator UI to configure a policy to deny network access using a control action for any endpoints that cannot be authenticated using an approved method as defined in the SSP.

1. Log on to Forescout UI.
2. From the Policy tab, select the Authentication and Authorization policy.
3. Find the 802.1x Authorization policy and click Edit.
4. From the Sub-Rules section, check that all of the options for authentication are selected including the following:
5. -Machine Authenticated
6. -User+Machine Authenticated
7. -User+Managed Machine
8. -User+NotMachine Authenticated

If these are all configured, check that the final step is not authorized by one of the previous steps, and block traffic in accordance with the SSP by selecting "Add>".

1. Give the policy a name like "Deny Access".
2. In the Condition box, click "Add" and select "802.1x RADIUS Authentication State".
3. Check the box labeled "RADIUS-Rejected", and then click "OK".
4. In the Actions box, click "Add" and select a block action in accordance with the SSP.

Additional Information:

CCI-000778 Uniquely identify organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53::IA-3
- NIST SP 800-53A::IA-3.1 (ii)
- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

1.25 FORE-NC-000460 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must use a bidirectional authentication mechanism configured with a FIPS-validated Advanced Encryption Standard (AES) cipher block algorithm to authenticate with the endpoint device. This is required for compliance with C2C Step 1.

```
GROUP ID: V-233339
RULE ID: SV-233339r971529
```

Rationale:

Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk. Currently, DoD requires the use of AES for bidirectional authentication since it is the only FIPS-validated AES cipher block algorithm.

Because of the challenges of applying this requirement on a large scale, organizations are encouraged to apply the requirement only to those limited number (and type) of devices that truly need to support this capability.

Audit:

If DoD is not at C2C Step 1 or higher, this is not a finding.

Use the Forescout CLI credentials to verify FIPS mode is set by running the "fstool version" command and look for the "FIPS enabled" setting.

Log on using the CLIAdmin credentials established upon initial configuration.

Verify FIPS mode by typing the command "fstool version".

If Forescout does not use AES, this is a finding.

Remediation:

To enable FIPS mode, log in to the CLI account a use the "fstool fips" command.

Note that use of FIPS mode is not mandatory in DoD. However, it is the primary method for mitigation of this requirement and ensuring FIPS compliance.

Log on using the CLIAdmin credentials established upon initial configuration.

To enable FIPS mode, type "fstool fips". A prompt alerting the user that FIPS 140-2 will be enabled will be displayed. Type "Yes" for FIPS to accept this prompt.

Note: Use of FIPS mode is not mandatory in DoD. However, it is the primary method for mitigation of this requirement and ensuring FIPS compliance.

Additional Information:

CCI-001967 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

- NIST SP 800-53 Revision 4::IA-3 (1)
- NIST SP 800-53 Revision 5::IA-3 (1)

1.26 FORE-NC-000470 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

When connecting with endpoints, Forescout must be configured to use FIPS 140-2/3 validated algorithms for encryption processes and communications. This is required for compliance with C2C Step 1.

```
GROUP ID: V-233340
RULE ID: SV-233340r1018668
```

Rationale:

A certificate's certification path is the path from the end entity certificate to a trusted root certification authority (CA). Certification path validation is necessary for a relying party to make an informed decision regarding acceptance of an end entity certificate.

NAC must be configured for only Certificate Signing. The NAC must interact with TLS-compliant lookups and verification in exchange with endpoints in Extensible Authentication Protocol (EAP) transactions where TLS is supported within the EAP type.

Certification path validation includes checks such as certificate issuer trust, time validity, and revocation status for each certificate in the certification path. Revocation status information for CA and subject certificates in a certification path is commonly provided via certificate revocation lists (CRLs) or online certificate status protocol (OCSP) responses.

Audit:

If DoD is not at C2C Step 1 or higher, this is not a finding.

Use the Forescout CLI credentials to verify FIPS mode is set by running the "fstool version" command and look for the "FIPS enabled" setting. Use the Forescout Administrator UI to verify SecureConnector is set to use TLS version 1.2 or higher for Client-Server Connections.

1. Log on using the CLIAdmin credentials established upon initial configuration.
2. Verify FIPS mode by typing the command "fstool version".

To configure TLS:

1. Log on to the Forescout UI.
2. Select Tools >> Option >> HPS Inspection Engine >> SecureConnector.
3. In the Client-Server Connection, check the Minimum Supported TLS Version is set to TLS version 1.2.

If the NAC is not configured to use FIPS 140-2/3 validated algorithms when connecting with endpoints, this is a finding.

Remediation:

To enable FIPS mode log into the CLI account a use the "fstool fips" command. Use the Forescout Administrator UI to set SecureConnector to use TLS version 1.2 or higher for Client-Server Connections.

To configure FIPS Mode:

1. Log on using the CLIAdmin credentials established upon initial configuration.
2. To enable FIPS mode, type "fstool fips". A prompt will be generated alerting the user FIPS 140-2 will be enabled. Type "Yes" for FIPS to accept this prompt.

To configure TLS:

1. Log on to the Forescout management tool.
2. Select Tools >> Option >> HPS Inspection Engine >> SecureConnector.
3. In the Client-Server Connection, set the Minimum Supported TLS Version to TLS version 1.3.

Additional Information:

CCI-000185 For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (a)
- NIST SP 800-53 Revision 5::IA-5 (2) (b) (1)

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	FORE-NC-000010 (Manual)	☐	☐
1.2	FORE-NC-000020 (Manual)	☐	☐
1.3	FORE-NC-000030 (Manual)	☐	☐
1.4	FORE-NC-000040 (Manual)	☐	☐
1.5	FORE-NC-000050 (Manual)	☐	☐
1.6	FORE-NC-000060 (Manual)	☐	☐
1.7	FORE-NC-000090 (Manual)	☐	☐
1.8	FORE-NC-000100 (Manual)	☐	☐
1.9	FORE-NC-000110 (Manual)	☐	☐
1.10	FORE-NC-000120 (Manual)	☐	☐
1.11	FORE-NC-000130 (Manual)	☐	☐
1.12	FORE-NC-000140 (Manual)	☐	☐
1.13	FORE-NC-000160 (Manual)	☐	☐
1.14	FORE-NC-000170 (Manual)	☐	☐
1.15	FORE-NC-000180 (Manual)	☐	☐
1.16	FORE-NC-000190 (Manual)	☐	☐
1.17	FORE-NC-000210 (Manual)	☐	☐
1.18	FORE-NC-000230 (Manual)	☐	☐
1.19	FORE-NC-000240 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	FORE-NC-000260 (Manual)	☐	☐
1.21	FORE-NC-000270 (Manual)	☐	☐
1.22	FORE-NC-000290 (Manual)	☐	☐
1.23	FORE-NC-000440 (Manual)	☐	☐
1.24	FORE-NC-000450 (Manual)	☐	☐
1.25	FORE-NC-000460 (Manual)	☐	☐
1.26	FORE-NC-000470 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 22, 2025	1.0.0	Initial CIS Release