

(Cisco Secure Access) Tectorial from Zero to Hero

Index

1. Connect

1. End User Connectivity
2. Network Connections
3. Users and Groups

2. Resources

1. Private Resources
2. Internet and SaaS Resources

3. Secure

1. Data Classification
2. Endpoint Posture Profiles
3. Web Profiles
4. Data Loss Prevention Policy
5. Access Policy

4. Tests

1. Posture for VPN and ZTNA
2. VPN on
3. Web Access

5. Monitor

1. ZTNA Client-Based
2. ZTNA Browser-based
3. Web access

Secure Access

1. Connect

1. End User Connectivity
 - Virtual Private Network: VPN Pools: **172.31.33.0/24** and **172.31.34.0/24**
 - Create new VPN

VPN Profile

A VPN profile allows for configuration of remote user connections through a VPN. [Help](#)

VPN Profile name
Fagioli1_VPN

- 1 General settings**
Default Domain: fagioli1.local | DNS Server: - | Protocol: TLS / DTLS
- 2 Authentication**
- 3 Traffic Steering (Split Tunnel)**
- 4 Cisco Secure Client Configuration**

General settings

Select and configure the network, protocol and posture that this VPN profile will use. [Help](#)

Default Domain

fagioli1.local

DNS Server

Use region configuration

+ New

Protocol

TLS / DTLS

IKEv2

Connect time posture (optional)

None

Multiple VPN postures can be created in Posture.

VPN Profile name
Fagioli1_VPN

- General settings
Default Domain: fagioli1.local | DNS Server: - | Protocol: TLS / DTLS
- Authentication
- Traffic Steering (Split Tunnel)
- Cisco Secure Client Configuration

Authentication Method

SAML

SAML Configuration

SAML Metadata XML Configuration

1. Download Service Provider XML file

This XML file contains metadata required to configure your IdP.

[Download service provider XML file](#)

2. Generate IP Security Metadata XML File

a. Upload the Service Provider XML file to your IdP.

b. From your IdP, create and download an IP Security Metadata XML file.

3. Upload IP security metadata XML file

Drag and drop file here or click to select it

(Security Metadata XML file)

Manual Configuration

Cancel

Back Next

Create a new app integration

Sign-in method

[Learn More](#)

OIDC - OpenID Connect

Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

SAML 2.0

XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

SWA - Secure Web Authentication

Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

API Services

Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Create SAML Integration

1 General Settings

2 Configure SAML

3 Feedback

1 General Settings

App name Fagioli1_VPN

App logo (optional) 

App visibility Do not display application icon to users

[Cancel](#) [Next](#)

- Picture name: **IMG_7160.jpg**
- Single sign-on URL: **<< AssertionConsumeService >>**
- Audience URI (SP Entity ID): **<< EntityDescriptor >>**

A SAML Settings

General

Single sign-on URL <https://29d8.vpn.sse.cisco.com/+CSCOEV/saml/sp/acs> Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) https://29d8.vpn.sse.cisco.com/saml/sp/metadata/Fagioli1_VPN

Default RelayState [?](#) If no value is set, a blank RelayState is sent

Name ID format [?](#) EmailAddress

Application username [?](#) Email

Update application username on Create and update

[Show Advanced Settings](#)

• Now you can configure the app to trust Okta as an IdP.

[View SAML setup instructions](#)

- XML > save to a file Fagioli1_VPN_Okta.xml

- Select which groups

Fagioli1_VPN

Active View Logs Monitor Imports

General Sign On Import Assignments

Priority	Assignment		
1	Security-Team No description	Edit	X

Authentication

Choose a configuration method to complete the SAML authentication process for this VPN profile.[Help](#)

Authentication Method

SAML

SAML Configuration

SAML Metadata XML Configuration

1. Download Service Provider XML file

This XML file contains metadata required to configure your IdP.

[Download service provider XML file](#)

2. Generate IdP Security Metadata XML File

- Upload the Service Provider XML file to your IdP.
- From your IdP, create and download an IdP Security Metadata XML file.

3. Upload IdP security metadata XML file

File 'Fagioli1_VPN_Okta.xml' uploaded. [Replace](#) [Delete](#)

General settings
Default Domain: fagioli1.local | DNS Server: - | Protocol: TLS / DTLS

Authentication
SAML

3 Traffic Steering (Split Tunnel)
Bypass Secure Access | 1 Exceptions

4 Cisco Secure Client Configuration

Traffic Steering (Split Tunnel)

Configure how VPN traffic traverses your network.[Help](#)

Tunnel Mode

Bypass Secure Access

All traffic is steered outside the tunnel.



Add Exceptions

Destinations specified here will be steered INSIDE the tunnel.

Destinations

10.1.1.0/24

DNS Mode

Default DNS

Cisco Secure Client Configuration

Select various settings to configure how Cisco Secure Client operates.[Help](#)

Session Settings **3** Client Settings **13** Client Certificate Settings **4**

[Download XML](#)

Edit

Pre Selected Settings

Use Start before Logon	Enabled
Minimize on connect	Enabled
Autoreconnect	Enabled
RSA Secure ID Integration	Automatic
Windows Logon Enforcement	Single Local Logon
Linux Logon Enforcement	Single Local Logon
Windows VPN Establishment	Local Users Only
Linux VPN Establishment	Local Users Only
Clear SmartCard PIN	Enabled
IP Protocol Supported	IPv4
Proxy Settings	Native
Allow local proxy connections	Enabled
Authentication Timeout	30

Cancel

[Back](#) [Save](#)

General

Use Start before Logon [i](#)

User controllable

Minimize on connect

User controllable

Local lan access [i](#)

User controllable

Autoreconnect [i](#)

User controllable

Auto reconnect behavior

Connect and resume

Suspend Secure Client during suspended standby

User controllable

User controllable

User controllable

Administrator Settings

Windows Logon Enforcement

Single Local Logon

Windows VPN Establishment

Local Users Only

Linux Logon Enforcement

Single Local Logon

Local Users Only

All Remote Users

All Remote Users

Clear SmartCard PIN

User controllable

Add IP Pool

X

Edit this IP pool that is used to manage a set of IP addresses for your VPN profile.

Parameters

Configure parameters for this IP pool by mapping it to a region and adding IP addresses for both Endpoint and Management IP pools.

Region

US (Pacific Northwest)

(

Display name

Fagioli_Pool

(

DNS Servers

Cisco Umbrella

(

+ Add

Endpoint IP pools

172.31.33.0/24

256 user connections

Management IP pools

172.31.34.0/24

256 management connections

- Download Cisco Secure Client and Profiles
 - Open Secure Access console inside Win10-TPM

Download Cisco Secure Client

X

The Cisco Secure Client protects computers, on and off the network. View detailed deployment instructions in [Help](#)



Version 5.1.2.42



Version 5.1.2.42



Version 5.1.2.42

Download Profiles

For Internet Security module: [orgInfo.json](#)

For VPN module: [FagioliVPN](#)

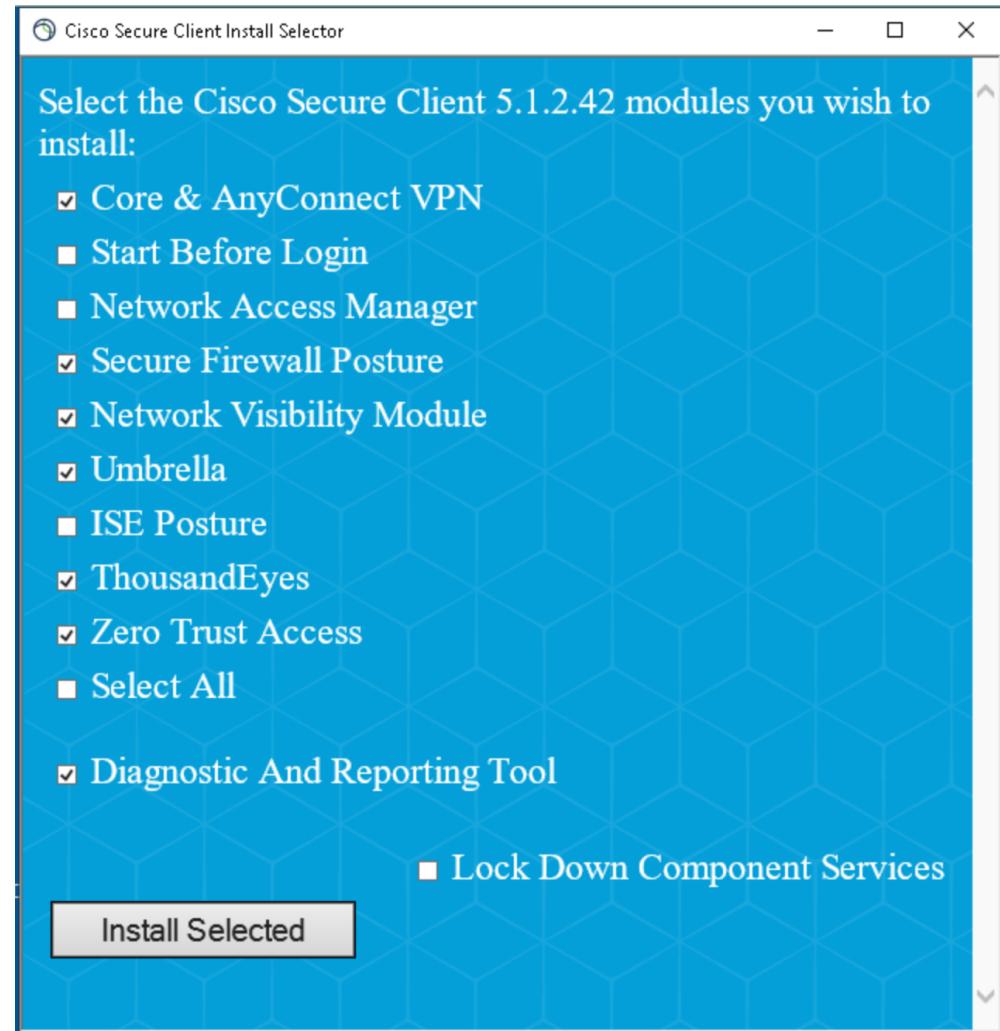
All Cisco Secure Client versions are available in [Cisco Software](#)

For cloud-based management of clients, use [Cisco SecureX](#)

[Close](#)

•

- Add the profiles inside the folders
- Install Secure Client



- Reboot
- Test VPN Login
-

2. Network Connections

- Network Tunnel Groups

The screenshot shows a configuration interface for 'Network Tunnel Groups'. On the left, there is a vertical navigation menu with numbered steps:

- 1 General Settings (selected)
- 2 Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

The main panel is titled 'General Settings' and contains the following fields:

- Tunnel Group Name: DC-NGFW
- Region: US (Pacific Northwest)
- Device Type: FTD

General Settings

Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

Tunnel ID and Passphrase

Configure the tunnel ID and passphrase tha

Tunnel ID Format

Email IP Address

Tunnel ID

bgimenez

Passphrase

.....

The passphrase must be between 16 and 64 cha

Confirm Passphrase

.....

Cancel

- Passphrase: C1sco12345C1sco12345
- Static Routing: 10.1.1.0/24
- FMC configuration
 - 1. VPN S2S

Create New VPN Topology

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

Point to Point Hub and Spoke Full Mesh

IKE Version:*

IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Node A

Device:*

NGFW1

Virtual Tunnel Interface:*

VTI1_to_SSE (IP: 169.254.2.1) +

Tunnel Source: outside (IP: 198.18.133.81)
 Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration:*

Email ID

bgimenez@8215246-621860075-

2. Routing

- Secure Access is always .1 IP address for VTI VPN-Based
- VPN1: 172.31.33.0/24
- VPN2: 172.31.34.0/24
- VPN_CGNAT: 100.64.0.0/10

Name	Value
VPN1	172.31.33.0/24
VPN2	172.31.34.0/24
VPN_CGNAT_SSE	100.64.0.0/10

Edit Static Route Configuration

?

Type: IPv4 IPv6

Interface*

VTI1_to_SSE

(Interface starting with this icon  signifies it is available for route leak)

Available Network C

+

Search

Add

11.11.60.0-24
11.11.61.0-24
11.11.62.0-24
11.11.63.0-24
11.11.64.0-24
198.19.0.0-16

Selected Network

VPN2
VPN_CGNAT_SSE
VPN1

Ensure that egress virtualrouter has route to that destination

Gateway

169.254.2.1

+

Metric:

1

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

+

•

•

3. ACP

- Create a rule at the top

Selected Sources: 6

Selected Destinations and Applications: 6

Collapse All

Remove All

Collapse All

ZONE 2 Objects
 InZone1
 VTI

ZONE 2 Objects
 InZone1
 VTI

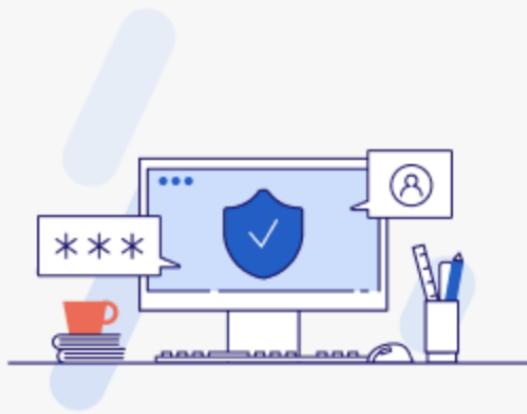
NET 4 Objects
 InsideLoop
 VPN1
 VPN2
 VPN_CGNAT_SSE

NET 4 Objects
 InsideLoop
 VPN1
 VPN2
 VPN_CGNAT_SSE

•

3. Users and Groups

- Configuration Management



Connect to any SAML and supported ID Providers.

Configure

Configure SSO Authentication

Manage how users are authenticated to Secure Access and log in. [Help](#)

Authentication Method
SAML

Identity Provider
Okta , Re-Authenticate Users
Daily

Configuration

SAML Provider Authentication

Configure how your IdP authenticates to Secure Access.

Select Identity Provider

You must complete the IdP's prerequisites before configuring it.

Okta

Entity ID

Use Secure Access's entity ID to authenticate Secure Access to your IdP.

Organization-specific Entity ID

Enable to configure SAML for multiple organizations that use the same IdP.

Disabled

Entity ID URL

Copy and save this Entity URL. It is required when configuring your IdP.

saml.fg.id.sse.cisco.com

[Copy URL](#)

IdP authentication frequency

Choose how often Secure Access verifies web proxy users by re-authenticating them.

Daily

Configuration

Select the configuration method to complete the SAML authentication process for your IdP.

SAML Metadata XML Configuration



1. Download the Service Provider XML file.

This XML file contains metadata required to configure your IdP.

[Download Service Provider XML file](#)



2. Generate an IdP Security Metadata XML File.

a. Upload the Service Provider XML file to your IdP.

b. From your IdP, create and download an IdP Security Metadata XML File.



3. Upload your IdP Security Metadata XML file

Manual Configuration



- Single sign-on URL: <> AssertionConsumerService <>
- SP Entity ID: <> EntityDescriptor : entityID : https://<>

A SAML Settings

General

Single sign-on URL [?](#)

Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) [?](#)

Default RelayState [?](#)

If no value is set, a blank RelayState is sent

Name ID format [?](#)

Application username [?](#)

Update application username on





- Picture name: **IMG_7160.jpg**
- Enroll Win10 computer

2. Resources

1. Private Resources

Private Resource Name

Net-10-1-1-0-25

Description (optional)

Entire 10.1.1.0/25

Communication with Secure Access Cloud

Specify one or more addresses that will be used for communication between this resource and Secure Access. Secure

Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR) ⓘ

10.1.1.0/25

Protocol

Any TCP

Port / Range

22,80

[+ IP Address or FQDN](#) Use internal DNS server to resolve the domain**Endpoint Connection Methods**

Specify the ways user endpoints can reach this resource. Later, access rules will determine which users and devices

 Branch Connections

Allow users and devices on the network, such as printers or kiosks, to connect to this resource if allowed by access

 Zero-trust connections

Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#) ⓘ

 Client-based connection

Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over

Remotely Reachable Address (FQDN, Wildcard FQDN, IP Address) ⓘ

10.1.1.0/25

[+ FQDN or IP Address](#)

Communication with Secure Access Cloud

Specify one or more addresses that will be used for communication between this resource and Secure Access. Secure Access will route traffic to this address. [Help](#)

Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR) ⓘ

10.1.1.200

Protocol

TCP - (HTTP/HTTPS)

Port / Ranges

443

[+ Protocol & Port](#)

[+ IP Address or FQDN](#)

Use internal DNS server to resolve the domain

Endpoint Connection Methods

Specify the ways user endpoints can reach this resource. Later, access rules will determine which users and devices can access the resource.

Branch Connections

Allow users and devices on the network, such as printers or kiosks, to connect to this resource if allowed by access rules.

Zero-trust connections

Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#)

Client-based connection

Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture).

Remotely Reachable Address (FQDN, Wildcard FQDN, IP Address) ⓘ

10.1.1.200

[+ FQDN or IP Address](#)

Browser-based connection

Allow browser-based connections from endpoints that do not have the Secure Client installed. Enable this option when devices that your organization does not manage have access to this resource.

Public URL for this resource ⓘ

https:// webserver -8215246.ztna.sse.cisco.io [Open](#)

Private Resources

Search by resource name

Private Resource Group

Connection Method

2 Private Resources

Private Resource

Private Resource Group

Connection Method

Accessed by

Rules

Total Requests

Net-10-1-1-0-25

Client-based ZTA VPN

1

1

39

Net-10-1-1-200-32

Browser-based ZTA

Client-based ZTA

0

1

0

• Check ZTNA configuration on Win10

- C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments\cached_configs

6036a0a8-050b-451b-8dfa-c4f17c054b47.json - Notepad

File Edit Format View Help

{"ztnaConfig":{"cidr_rules":[{"cidr":"10.1.1.1/32"}, {"cidr":"10.1.1.200/32"}], "proxies": [{"address": "proxy-8215246.zpc.sse.cisco.com"}]}}

2. Internet and SaaS Resources

Internet and SaaS Resources

Configure groups of resources to simplify specifying destinations when creating a

Destination Lists

Application Lists

Content Category Lists

Use this page to create lists of web-based applications to simplify creating internet access rules (such as advanced application controls in the access rule.) [Help](#)

 Search by list name

Tinder App

List name

Tinder App

Applications

 tinder

Tinder

DELETE

List Name

Categories [SELECT ALL](#)

<input type="checkbox"/> Adult	<input type="checkbox"/> Health and Medicine	<input type="checkbox"/> Private IP Addresses as Host
<input type="checkbox"/> Advertisements	<input type="checkbox"/> Humor	<input type="checkbox"/> Professional Networking
<input type="checkbox"/> Alcohol	<input type="checkbox"/> Hunting	<input type="checkbox"/> Real Estate
<input type="checkbox"/> Animals and Pets	<input type="checkbox"/> Illegal Activities	<input type="checkbox"/> Recipes and Food
<input type="checkbox"/> Arts	<input type="checkbox"/> Illegal Downloads	<input type="checkbox"/> Reference
<input type="checkbox"/> Astrology	<input type="checkbox"/> Illegal Drugs	<input type="checkbox"/> Regional Restricted Sites (Germany)
<input type="checkbox"/> Auctions	<input type="checkbox"/> Infrastructure and Content Delivery Networks	<input type="checkbox"/> Regional Restricted Sites (Great Britain)
<input type="checkbox"/> Business and Industry	<input type="checkbox"/> Internet of Things	<input type="checkbox"/> Regional Restricted Sites (Italy)
<input type="checkbox"/> Cannabis	<input type="checkbox"/> Internet Telephony	<input type="checkbox"/> Regional Restricted Sites (Poland)
<input type="checkbox"/> Chat and Instant Messaging	<input type="checkbox"/> Job Search	<input type="checkbox"/> Religion
<input type="checkbox"/> Cheating and Plagiarism	<input type="checkbox"/> Lingerie and Swimsuits	<input type="checkbox"/> SaaS and B2B
<input type="checkbox"/> Cloud and Data Centers	<input type="checkbox"/> Lotteries	<input type="checkbox"/> Safe for Kids
<input type="checkbox"/> Computer Security	<input type="checkbox"/> Military	<input type="checkbox"/> Science and Technology
<input type="checkbox"/> Computers and Internet	<input type="checkbox"/> Mobile Phones	<input type="checkbox"/> Search Engines and Portals
<input type="checkbox"/> Conventions, Conferences and Trade Shows	<input type="checkbox"/> Museums	<input type="checkbox"/> Sex Education
<input type="checkbox"/> Cryptocurrency	<input type="checkbox"/> Nature and Conservation	<input type="checkbox"/> Shopping
<input type="checkbox"/> Dating	<input type="checkbox"/> News	<input checked="" type="checkbox"/> Social Networking

3. Secure

1. Data Classification

Add New Data Classification

Data Classification Name

DLP_CC_Lenient

Select Boolean Operator

OR AND

Selected Data Identifiers

Credit Card Number – Lenient i

2. Endpoint Posture Profiles

- Zero Trust Connection

Edit Client-based Posture Profile

Specify requirements for endpoint devices to connect to private resources. These requirements apply to devices on which the SSE Client is installed. Each requirement is optional. Requirements can be configured in any order. Endpoints must meet all configured requirements. [Help](#)

Name *

Firewall Required

① **Operating System**
Any

② **Firewall**
Require for Windows

③ **Endpoint security agents**
Not required

④ **System password**
Not required

⑤ **Disk encryption**
Not required

Firewall

Require the platform-native firewall to be running on the end-user dev

Operating systems requiring firewall

Windows x

 Windows

Require the platform-native firewall to be running on the endpoint.

[Cancel](#)

Add New Browser-based Posture Profile

Specify requirements for endpoint devices to connect to private resources. These requirements apply to devices on which no SSE Client is installed. Each requirement is optional. Requirements can be configured in any order. Endpoints must meet all configured requirements. [Help](#)

Name *

1 Operating System
Any

✓ Browser
Edge allowed

Browser

Require specific web browsers. [Help](#)

Browser

Edge

[Cancel](#)

- VPN Connection

Name *

1 Operating System
Any

2 Endpoint security agent
Not required

3 Windows registry entries
Not required

4 Firewall
Not required

5 Disk encryption
Not required

✓ File
Require for Windows

7 Processes
Not required

8 Certificate
Not required

File

Specified files must be present on the endpoint. [Help](#)

Operating systems requiring one or more specified files

Windows

Windows

Require of the specified files:

File must have been updated within the last:

File Path *

C:\Users\Administrator\Desktop\testfile.txt

Checksum

[Cancel](#)

← End User Connectivity
VPN Profile
A VPN profile allows for configuration of remote user connections through a VPN. [Help](#)

VPN Profile name

General settings
Default Domain: fagioli1.local | DNS Server: - | Protocol: TLS / DTLS

Authentication
 SAML

Traffic Steering (Split Tunnel)
Bypass Secure Access | 1 Exceptions

Cisco Secure Client Configuration

General settings
Select and configure the network, protocol and posture that this VPN profile will use. [Help](#)

Default Domain

DNS Server
 [+ New](#)

Protocol
 TLS / DTLS
 IKEv2

Connect time posture (optional)

 [+](#)
 [VPN-Posture](#)

3. Web Profiles

Web Profile 1	Applied To 0 Rules	Decryption Enabled	SAML Auth Enabled	Security and Acceptable Use 2 Control Types Selected	End-User Notifications System-provided	Last Modified Jan 31, 2024
Profile Name <input type="text" value="Web Profile - Decrypt all"/> CANCEL SAVE <input type="checkbox"/> Set as default Web Profile						
Decryption <small>Decryption is necessary to inspect content for security and acceptable use. When enabled, all web traffic will be decrypted except as specified in the selected Do Not Decrypt list.</small> Help						
SAML Authentication <small>Enable SAML authentication on the networks and tunnels configured for the rules that use this profile. Decryption must also be enabled for Network SAML enforcement.</small> Help						
Security and Acceptable Use Controls <small>Multiple levels of scanning and blocking can be enabled depending on your requirements.</small>						
Threat Categories	3 Categories Enabled		Default Settings			Edit
File Inspection	Enabled		Cisco Secure Malware Analytics: Disabled			Edit
File Type Blocking	Disabled					Edit
SafeSearch	Disabled					Edit

4. Data Loss Prevention Policy

Add New Real Time Rule

Configure this rule to set the criteria as to what triggers its enforcement. The Realtime DLP inspects data violation is detected, this rule's Action setting is automatically enforced. [Help](#)

Rule Name

block-CreditCard

Severity

● High



Data Classifications

Select where to search for the selected data classifications.

Content

File Name

Content and File Name

Select data classifications to add them to this rule.

Search Classifications

Built-in GDPR Classification

[PREVIEW](#)

Built-in HIPAA Classification

[PREVIEW](#)

Built-in PCI Classification

[PREVIEW](#)

Built-in PII Classification

[PREVIEW](#)

DLP_CC_Lenient

[PREVIEW](#)

Identities

Select identities to add them to this rule.

The screenshot shows a search bar at the top labeled "Search Identities". Below it is a section titled "All Identities" with the following items:

- AD Groups (1)
- AD Users (3)
- Network Tunnel Groups (2)
- Networks (2)
- Roaming Computers (2)

To the right, a dashed box highlights the selected item: "Roaming Computers".

Destinations

Manage destination lists and vetted applications for this rule.

All Destinations

Selecting All Destinations will scan the traffic to any application or website the user is browsing to.

Select Destinations Lists and Applications for Inclusion

Scans selected destination lists and vetted applications.

The screenshot shows a search bar at the top with the text "pastebin". Below it is a navigation bar: "Destinations / Application Categories / Content Management". A "Direction" button is also present. A checkbox next to "Pastebin (Vetted)" is checked. To the right, a panel titled "1 Selected for Inclusion" shows the selected application: "Applications Categories: Pastebin / Content Management".

Below this, a table titled "1 DLP Rule" lists the rule details:

Rule Type	Name	Severity	Action	Identities or File Owners	Destinations	Data Classifications	Last Modified
Real Time	block-CreditCard	High	Block	2 Identities	Inclusion 1 Application	Data Classifications File Labels DLP_CC_Lenient	Feb 18, 2024

5. Access Policy

The screenshot shows the configuration of an access policy rule. The rule is named "PrivateResource_2021.0-25" and has a rule order of 1. It uses the "Specify Access" action, which allows traffic if security requirements are met. The "From" field specifies the source as "Security-Team". The "To" field specifies the destination as "Net-10-1-1-0-25". The "Action" field shows two options: "Allow" (selected) and "Block". The "Zero-Trust Client-based Posture Profile" dropdown is set to "None".

Rule name PrivateResource_10.1.1.200-32 **Rule order** 2

1 Specify Access Specify which users and endpoints can access which resources. [Help](#)

Action

Allow Allow specified traffic if security requirements are met.

Block Block specified traffic.

From Specify one or more **sources**. **To** Specify one or more **destinations**.

Security-Team **Net-10-1-1-200-32**

Information about sources, including selecting multiple sources. [Help](#)

Endpoint Requirements For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. [Help](#)

Zero-Trust Client-based Posture Profile **Custom** Requirements for end-user devices on which the Cisco Secure Client is installed.

Firewall Required

Private Resources: **Net-10-1-1-200-32**

Zero Trust Browser-based Posture Profile **Custom** Requirements for end-user devices on which the Cisco Secure Client is NOT installed.

OnlyEdge_Allowed

Private Resources: **Net-10-1-1-200-32**

Edit Block_Tinder For information about configuring an internet access rule, see [Help](#)

Rule is enabled Logging is enabled [Edit](#)

Summary

Rule name Block_Tinder **Rule order** 3

1 Specify Access Specify which users and endpoints can access which resources. [Help](#)

Action

Allow Allow specified traffic if security requirements are met.

Block Block specified traffic.

Warn Allow access but display a warning.

Isolate Allow access to specified destinations, but isolate the traffic.

From Specify one or more sources. **To** Specify one or more destinations.

Any Roaming Computers **Social_Networking**

Information about sources, including selecting multiple sources. [Help](#)

Information about destinations, including selecting multiple destinations. [Help](#)

Web Profile **Custom**

The following web-related settings will apply to traffic that matches this rule. [Help](#)

Web Profile 1

Decryption **Enabled**

Add WarnBlock_SocialNetworking Create a rule to control and secure access to specified internet destinations from within your network and from managed devices. For an end-to-end guide to completing prerequisites and configuring a rule, see [Help](#)

Rule is enabled Logging is enabled [Edit](#)

Summary

Rule name WarnBlock_SocialNetworking **Rule order** 4

1 Specify Access Specify which users and endpoints can access which resources. [Help](#)

Action

Allow Allow specified traffic if security requirements are met.

Block Block specified traffic.

Warn Allow access but display a warning.

Isolate Allow access to specified destinations, but isolate the traffic.

From Specify one or more sources. **To** Specify one or more destinations.

Any Roaming Computers **Social_Networking**

Information about sources, including selecting multiple sources. [Help](#)

Information about destinations, including selecting multiple destinations. [Help](#)

4 Rules									Customize view	
	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status	...	
1	PrivateResource_10.1.1.0-25	Private	Allow	Security-Te...	Net-10-1-1-0...	🛡️	-	●	...	
2	PrivateResource_10.1.1.200-32	Private	Allow	Security-Te...	Net-10-1-1-2...	🛡️	-	●	...	
3	Block_Tinder	Internet	Block	Any Roaming ... +1	Tinder App	🚫	-	●	...	
4	WarnBlock_SocialNetworking	Internet	Warn	Any Roaming ... +1	Social_Netwo...	⚠️	-	●	...	

4. Tests

1. Posture for VPN and ZTNA

- VPN
 - Check file testfile.txt exists in Desktop. It fails if it doesn't
- ZTNA Client-based
 - SSH to 10.1.1.1 - it doesn't require firewall, it should work
 - HTTPS to 10.1.1.200 - Requires Firewall, it should fail otherwise
- ZTNA Browser
 - Access clientless from other computer to <https://webserver-8215246.ztna.sse.cisco.io/> - only Edge allowed, it should fail otherwise

2. VPN on

- Ping 10.1.1.1-126 - it should work
- Ping 10.1.1.200 - it should fail, it is not published via VPN access

3. Web Access

- DLP - pastebin using creditcard - it should fail
- Tinder - Application block - it should fail (on/off VPN) - since it is NOT full tunnel, always comes using Roaming client
- Facebook - Content category block - since it is NOT full tunnel, always comes using Roaming client

5. Monitor

1. ZTNA Client-Based

116 Total									Viewing activity from Feb 17, 2024 3:40 PM to Feb 18, 2024 3:40 PM			Page: 1			Results per page:	50	1 - 50
Source	Rule Identity	Destination	Action	Resource/Application	Rule Name	OS	Browser	Location	Location IP	Date & Time	...						
↳ Read Only (readonly@fagioli.local)	↳ Read Only (readonly@fagioli.local)	10.1.1.1	Allowed	Net-10-1-1-0-25	PrivateResource_10.1.1.0-25	↳ win 10.0.19045.3155	US	64.100.12.5	Feb 18, 2024 3:38 PM								
↳ Read Only (readonly@fagioli.local)	↳ Read Only (readonly@fagioli.local)	10.1.1.200	Blocked	Net-10-1-1-200-32	For all private access	↳ win 10.0.19045.3155	US	64.100.12.5	Feb 18, 2024 3:38 PM								
↳ Read Only (readonly@fagioli.local)	↳ Read Only (readonly@fagioli.local)	10.1.1.200	Blocked	Net-10-1-1-200-32	For all private access	↳ win 10.0.19045.3155	US	64.100.12.5	Feb 18, 2024 3:38 PM								
↳ Read Only (readonly@fagioli.local)	↳ Read Only (readonly@fagioli.local)	10.1.1.200	Blocked	Net-10-1-1-200-32	For all private access	↳ win 10.0.19045.3155	US	64.100.12.5	Feb 18, 2024 3:38 PM								
↳ Read Only (readonly@fagioli.local)	↳ Read Only (readonly@fagioli.local)	10.1.1.200	Blocked	Net-10-1-1-200-32	For all private access	↳ win 10.0.19045.3155	US	64.100.12.5	Feb 18, 2024 3:38 PM								

Event Details



Action

Allowed

Time

Feb 18, 2024 3:37 PM

Rule Name

PrivateResource_10.1.1.200-32

Identity

Read Only (readonly@fagioli.local)

Security-Team

Policy or Ruleset Identity

Read Only (readonly@fagioli.local)

Resource/Application

Net-10-1-1-200-32

OS

win 10.0.19045.3155

Location

US

Location IP

64.100.12.5

Enpoint Security Agent
windows-defender[]

Firewall

System

System Password

enabled[]

Disk Encryption

None

2. ZTNA Browser-based

Action

Blocked

Time

Feb 18, 2024 3:32 PM

Rule Name

For all private access

Source



Bruno Fagioli (bgimenez@cisco.com)

Rule Identity



Bruno Fagioli (bgimenez@cisco.com)

Resource/Application

Net-10-1-1-200-32

OS

Mac OS X 10.15

Browser

Chrome 121.0

3. Web access

Event Details

X

Action

Blocked — Public Application

Time

Feb 18, 2024 4:49 PM

Rule Name

Block Tinder

Source

 **ciscosse**

Rule Identity

 **ciscosse**

Internal IP Address

198.18.133.252

External IP Address

64.100.12.5

Destination

<https://www.tinder.com/>

Hostname

www.tinder.com

Categories

Application Block, Dating

[Dispute Categorization](#)

Resource/Application

Tinder

Application Category

Social Networking

Event Details



Action

Allowed — Warn Page Displayed

Time

Feb 18, 2024 4:49 PM

Rule Name

Warn - Social Networking

Source

ciscosse

Rule Identity

ciscosse

Internal IP Address

198.18.133.252

External IP Address

64.100.12.5

Destination

<https://facebook.com/>

Hostname

facebook.com

Categories

Social Networking

Dispute Categorization

Resource/Application

Facebook

Application Category

Social Networking

Content Type

text/html

File Action (Remote Browser Isolation)

•

Event Details

X

Action

Blocked — Public Application

Time

Feb 18, 2024 4:56 PM

Rule Name

Block Tinder

Source

 **Read Only (readonly@fagioli.local)**

 **Security-Team**

Rule Identity

 **Security-Team**

Internal IP Address

-

External IP Address

172.31.33.1

Destination

<http://tinder.com/>

Hostname

tinder.com

Categories

Application Block, Dating

[Dispute Categorization](#)

Resource/Application

Tinder

Application Category Social Networking

1 Total Events Viewing activity from Jan 19, 2024 at 6:05 PM to Feb 18, 2024 at 6:05 PM											...	X	
Event Type	Severity	Identity	File Owner	Event Actor	File Name ▾	Destination	Rule	Action	Detected ▾	...	Severity	...	X
	● High	Deleted Identity	N/A	N/A	Form	pastebin.com	block-CreditCard	● Blocked	Feb 18, 2024 at 4:03 PM	...	● High	Classification	
											D_P_CCL.unlmt		
											1 Match	Credit Card Number – Lenient	
											XXXXXXXXXXXX0126		
											Content Type		
											text/plain		
											Total Size in Bytes		
											15.0 B		
											SHA256 Hash		
											c4fdbf6fc2740911ac19e48600164e3b6d1b9fa26ba9a23a3ae...7...		
											Copy		
											Export ID		
Results per page: 50 ▾ 1-1 < >													