



CISCO

Techtorial

The Power of the **Platform**





Cisco Secure Access: VPNaaS

Egyszerűbb és hatékonyabb Remote Access VPN kezelés a felhőben

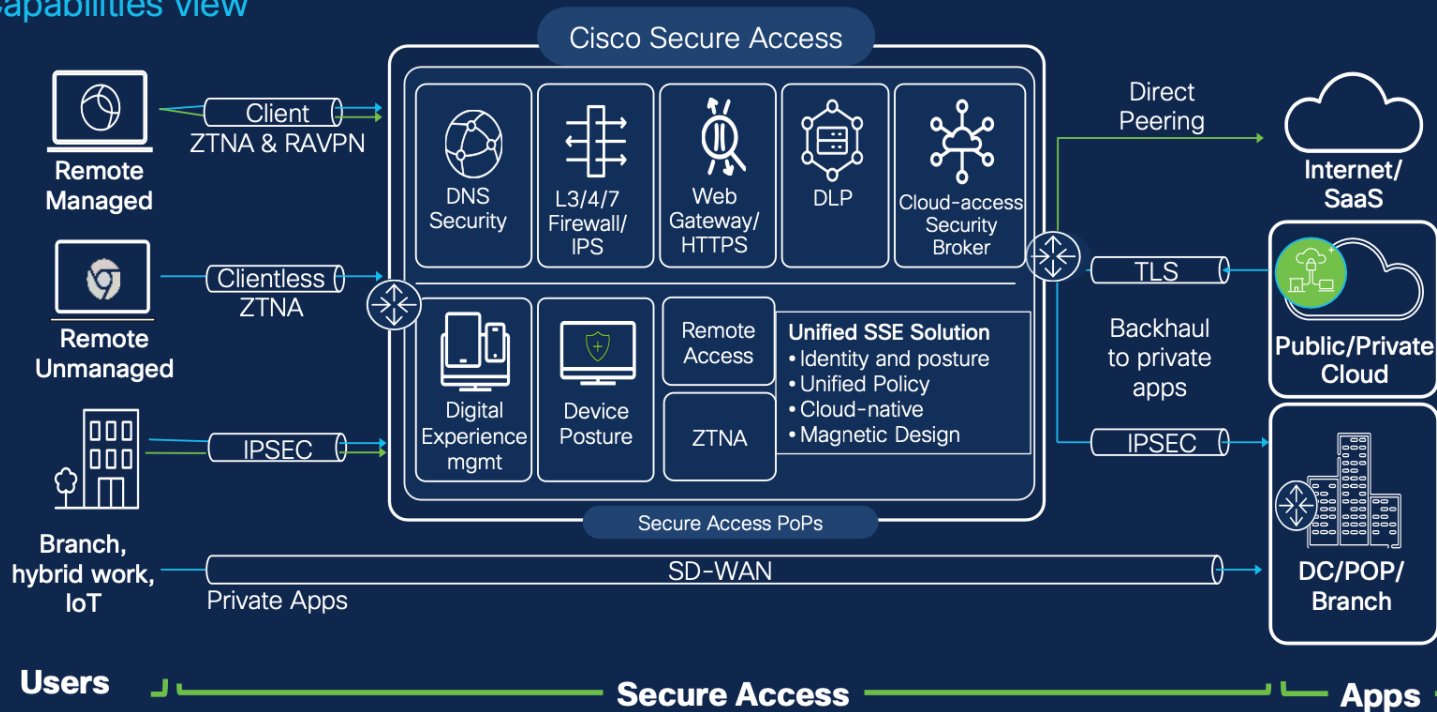
Borbás Zoltán
CCIE-S #68087
Senior Rendszermérnök
ACE Network Zrt.

Agenda

- Cisco Secure Access felépítése az SSE architektúra fő elemei.
- Cisco Secure Access „csomagok”
- Hagyományos RA VPN használatának hátrányai.
- Cisco Secure Access hozzáférési módok (VTI, RAVPN, ZTNA) high level ismertetése.
- Cisco Secure Access környezet bemutatása, RAVPN és ZTNA elérés konfigurálása (DEMO).

Secure Access áttekintés

Capabilities view



Secure Access „csomagok”

Funkció	Secure Private Access (SPA)	Secure Internet Access (SIA)
Hozzáférési típus	Magán hálózatok elérése.	Nyilvános internethez és SaaS alkalmazások elérése.
Felhasználási terület	Vállalati belső alkalmazások.	Publikus cloud és internet elérés
Biztonság	Zero Trust.	Biztonságos internet kapcsolat, DNS alapú védelem.
Védelmi funkciók	Felhasználó és eszköz hitelesítés, belső alkalmazásokhoz a hozzáférés felügyelete.	Webbiztonság, internet forgalom ellenőrzése, tartalomszűrés.
Skálázhatóság	Vállalati szintű, akár nagy méretű belső hálózatokhoz is.	Nagymértékben skálázható, minden internet alapú hozzáféréshez



Hagyományos Remote Access VPN

Teljesítmény és késleltetés

- Sebesség problémák
- Túlterhelt VPN koncentrátorok

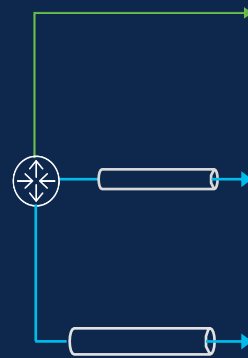
Remote User



Distributed Datacenters



Fragmented Security Stack & Policies



Internet/SaaS



Private Apps



Other offices/branches

Komplex konfiguráció és karbantartás

- Bonyolult beállítás
- Tűzfal- és hálózati beállítások kezelése
- Frissítések és hibajavítások

Biztonsági kockázatok

- Átjáró
- Cisco Secure Access VPNaaS szolgáltatás ezekre a kihívásokra ad megoldást!
- Támadási felület növekedése
- Átfogó hozzáférés

Skálázhatósági problémák

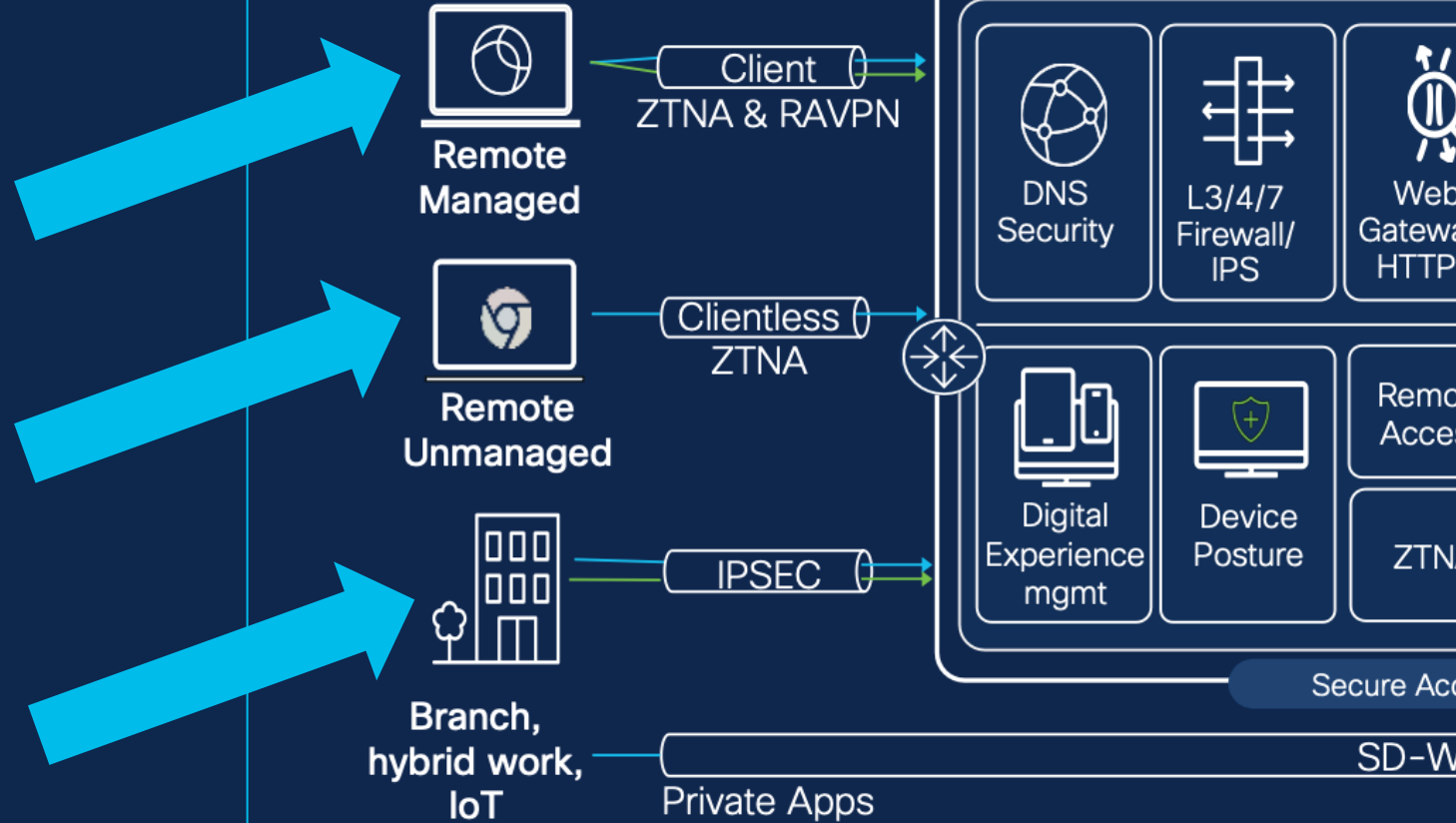
- Növekvő felhasználói bázis kezelése
- Teljesítmény

Költség

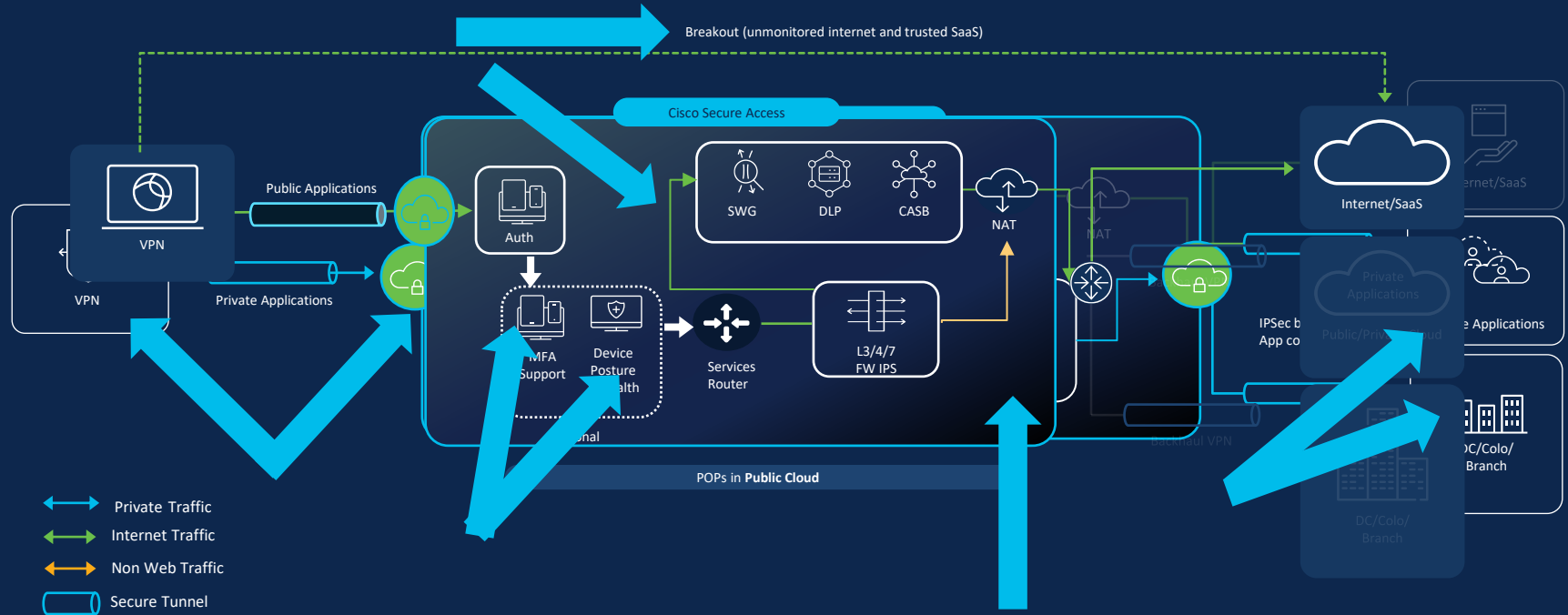
- Növekvő hardver és szoftver költségek
- Karbantartási költségek

Secure Access

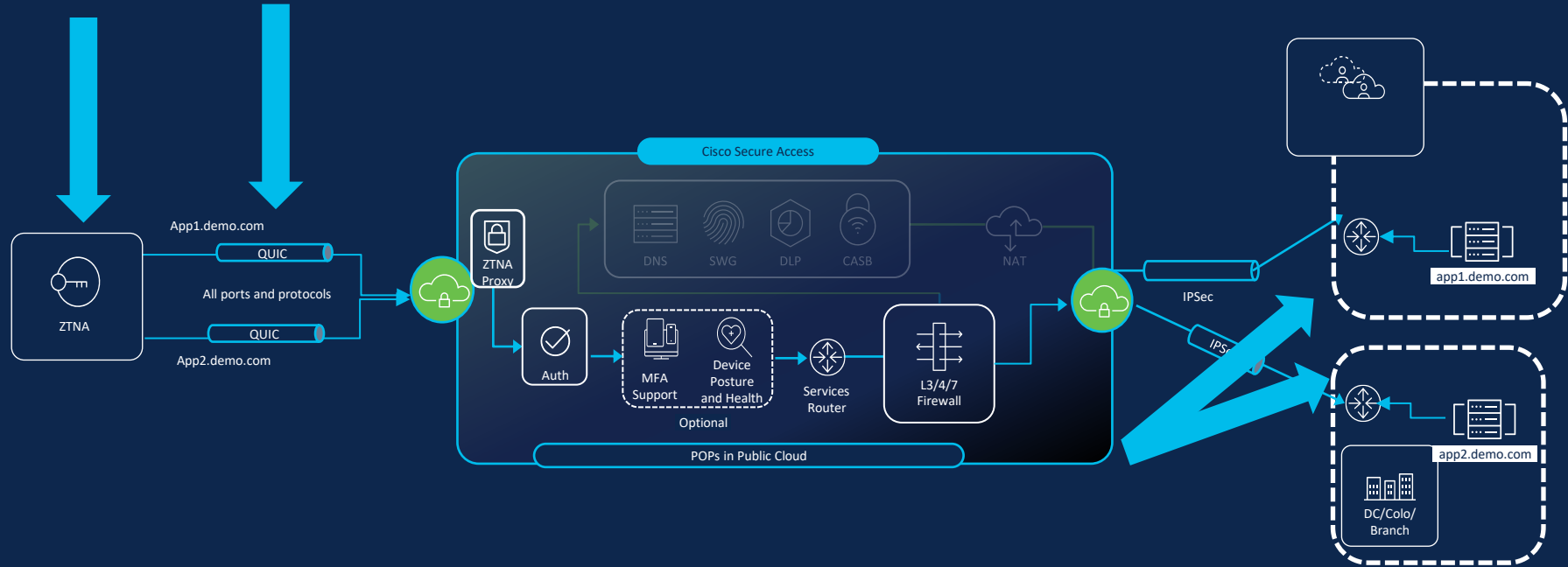
Capabilities view



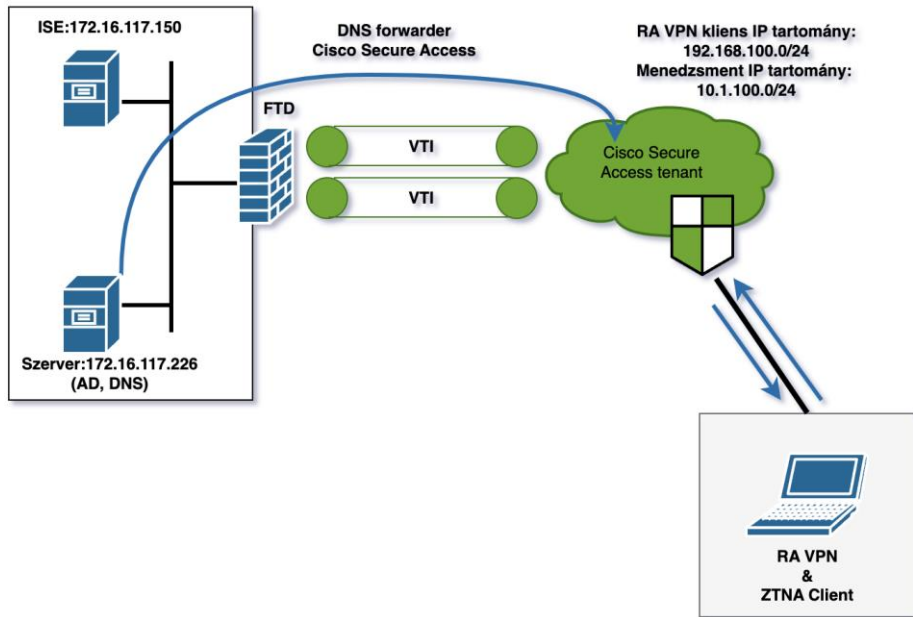
Secure Private és Internet hozzáférés (VPN kliens)



Secure Private Access (Client-based ZTNA)



DEMO



- Home
- Experience Insights
- Connect
- Resources
- Secure
- Monitor
- Admin
- Workflows

- Home
- Experience Insights
- Connect
- Resources
- Secure
- Monitor
- Admin
- Workflows

IPs

To

✓

Users and Groups

Last 24 Hours

VPN connection events

0 100% Decrease (last 24 hours)

ZTNA authorization events

1 99% Decrease (last 24 hours)



Top 5 Users created requests

3682 39% demo-dns

13 83% user1 (user1@acesec.hu)

10 100% Deleted identity

Private resources

Last 24 Hours

Applications accessed

1 (last 24 hours)

Unique user identities accessed

1 No change (last 24 hours)

Allowed

13 100% Decrease (last 24 hours)

Blocked

0 100% Decrease (last 24 hours)

Activity Search



VPN resources accessed

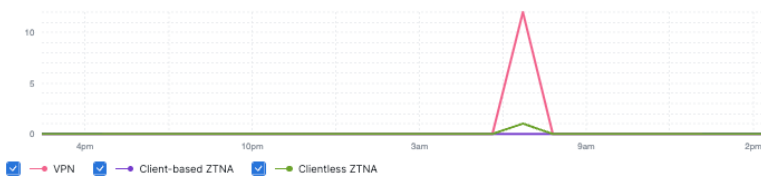
12 100% Decrease (last 24 hours)

Client-based ZTNA

0 100% Decrease (last 24 hours)

Clientless ZTNA

1



Top 3 resources accessed

1 98% ise-admin-panel

Előzetesen felvett beállítások

- Network Tunnel Groups
- Radius szerver és szerver group
- Felhasználók
- Registered Networks
- SSO autentikáció

Components	IKEv2 (Phase I) (no IKEv1 support)	ESP (Phase II)
Encryption	AES-256-16 (GCM) , AES-256-8 (GCM), AES-128-16 (GCM), AES-128-8 (GCM), AES-128(CBC), AES-256(CBC)	AES-256-16(GCM) , AES-128-16(GCM), AES-256(CBC), AES-128(CBC), NULL(GCM) - AES-256 GMAC, NULL(GCM) - AES-192 GMAC, NULL(GCM) - AES-128 GMAC NULL(CBC)
Hashing	SHA256 , SHA1	SHA256 , SHA1
DH Group	20, 19 , 15, 14	20, 19 , 15, 14
Authentication	Pre-Shared Key (PSK)	N/A
Protocol	N/A	ESP in UDP (NAT-T) (Port - UDP 4500)
Total Child SAs Supported	N/A	1
Lifetime	Based on client settings (IKE default is 4 hours)	Based on client settings (Child SA default is one hour)
Perfect Forward Secrecy (PFS)	N/A	Allowed (Ciphers configured with both PFS and non-PFS.) Note: If the remote end prefers to negotiate PFS, it has to set the child rekey timer lower than the head end and/or allow both PFS and non-PFS. Reason: CNHE prefers non-PFS. We configured both, but if the other side wants PFS, we can negotiate.

tunnel group overlaps with other IP address spaces in your network. When selected, private applications behind these tunnels

is tunnel group.

by your organization. For example, 128.66.0.0/16, 192.0.2.0/24.

Add		
DPD Timeouts	30 seconds (back_off = 2, retransmit timeout = 2, retries = 5) (Maximum DPD timeout = 156 seconds)	N/A
IP fragmentation	Not supported	Not supported
IKE Fragmentation (RFC 7383)	Enabled	N/A
Extended Sequence Number (ESN)	N/A	Allowed and preferred

Save

Secure Access

Server

dem

IP Add

Cisco

Home

Experience Insights

Connect

Resources

Secure

Monitor

Admin

Workflows

← Users and Groups

Configuration Management

For more information about connecting your users, see our documentation. [Help](#)

Configurations Advanced Settings

Provisioning

Add users and groups to Secure Access through a supported IdP. [Help](#)

Current AD user configurations include the following

Others

Manually Added

[Provision users and groups](#)

SSO authentication

Connect to any SAML and supported IdP to configure SSO authentication. [Help](#)

Current SSO authentications include the following

SWG, Zero Trust (Browser-based and Client-based)

My SAML Configuration Enabled

SAML configuration details

Identity Provider

Duo Security

Re-authenticate Web Proxy Users

Daily

Organization-specific Entity Id

Disabled

Entity Id

saml.fg.id.sse.cisco.com

IP Surrogate

Internal Network bypass 0

Enabled

[Test Configuration](#)

[Delete](#)

Cancel

Save

1813

© 2021 Cisco and/or its affiliates. All rights reserved.

DEMO

RA VPN és ZTNA hozzáférés beállítás



Home

Experience
Insights

Connect



Resources



Secure



Monitor



Admin



Workflows

Overview

The Overview dashboard displays status, usage, and health metrics for your organization. Use this information to address security threats and monitor system usage. [Help](#)

Connectivity

Last 24 Hours

Network tunnel groups 1 total

1 Connected



Resource connector groups 0 total

0 Connected



Data Transfer

Last 24 Hours

TOTAL USAGE

Usage data - delayed up to 30 min.

2.01 MB Total traffic

176.55 MB
Decrease (last 24 hours)

29.34 KB Received

17.70 MB
Decrease (last 24 hours)

1.98 MB Sent

158.85 MB
Decrease (last 24 hours)1.9 MB
1.7 MB
1.5 MB
1.3 MB
1.1 MB
1.0 MB
0.8 MB
0.6 MB
0.4 MB
0.2 MB
0.0 MB

19:00 - 21:00 22:00 - 00:00 01:00 - 03:00 04:00 - 06:00 07:00 - 09:00 10:00 - 12:00 13:00 - 15:00 16:00 - 18:00

- ☒ Branch
- ☒ Browser-based ZTA
- ☒ Client-based ZTA
- ☒ RAVPN

☒ Select All

Security

Last 24 Hours

Security Activity

Top Security Categories

File Retrospective

Access Events

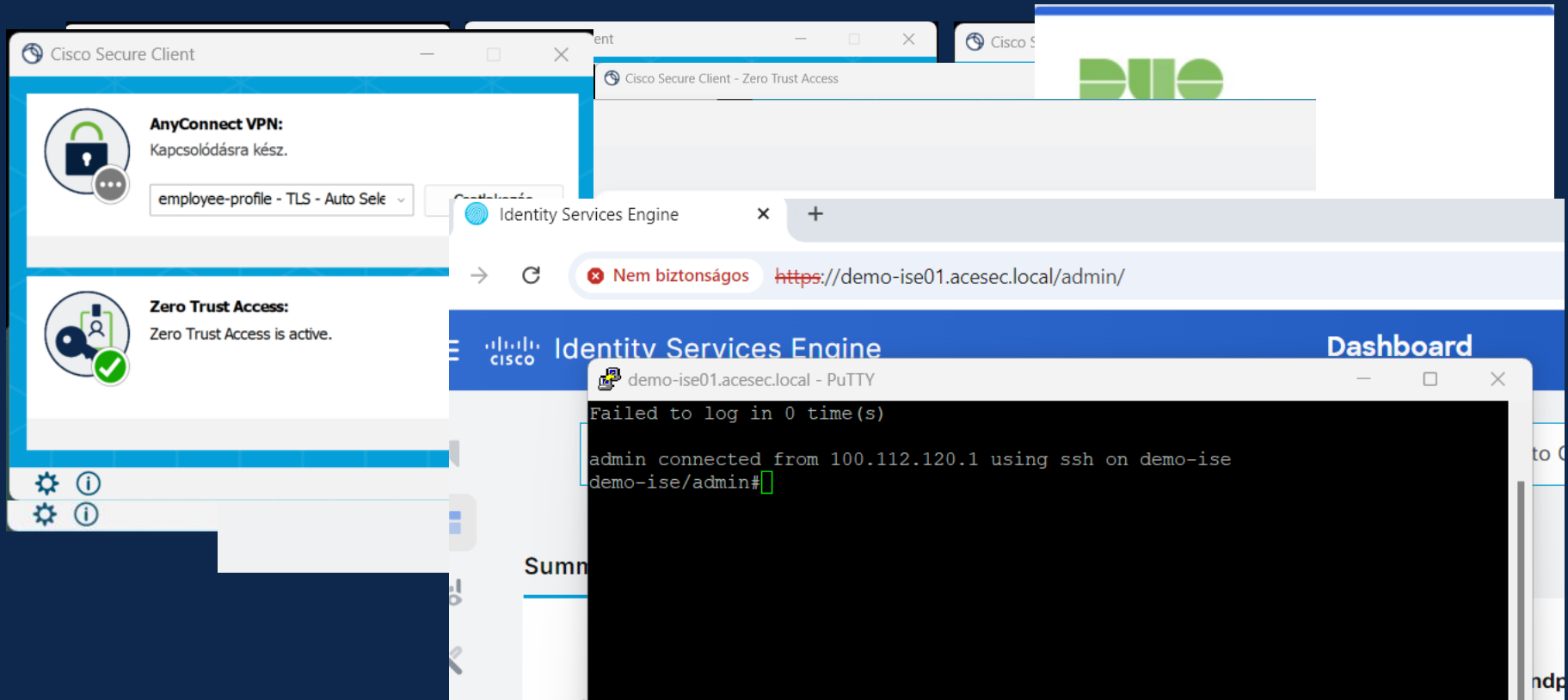
Requests

3761
68% Decrease (last 24 hours)

Blocks

0
100% Decrease (last 24 hours)

Mi történik a kliensen ezután?...



Activity Search

FILTERS

Search by domain, identity, or URL

Search filters

2271 Total View

Response

Select All

- ☐ Allowed [Advanced](#)
☐ Blocked

Warn Page Behavior

Select All

- ☐ Warned
☐ Accessed After Warn

Isolate

- ☐ Isolated

IPS Signature

Select All

- ☐ Log Only
☐ Would Block
☐ Blocked

Protocol

Select All

- ☐ HTTP
☐ HTTPS

Event Type

Select All

- ☐ Public Application
☐ Private Applications and Networks
☐ Destination List
☐ Any Security Category
☐ Any Content Category
☐ Cisco AMP Disposition is Malicious
☐ Antivirus Disposition is Malicious
☐ Integration

Request

DNS

WEB

WEB

WEB

DNS

WEB

WEB

WEB

WEB

WEB

DNS

ZTNA CLIENT-BASED

FW

ZTNA CLIENT-BASED

ZTNA CLIENT-BASED

ZTNA CLIENT-BASED

FW

FW

FW

FW

FW

ZTNA CLIENT-BASED

Event Details

Connection Method

ZTNA Client-based

Time

okt. 2, 2024 6:33 DU

Action

Allowed

Access details

Identity

[support \(support@acesec.hu\)](#)

Resource/Application

support-access

Destination

demo-ise01.acesec.local

Destination IP

172.16.117.150

Destination Port

22

Resource Connector Group

-

Ingress Region

Europe (Central)

Tunnel Type

HTTP2

Transaction ID

agimo02GNZQJOUdNhazEcn022pLh4ftG

Endpoint details

Client Location

HU

Client Location IP

85.67.103.111

OS

win 10.0.22631.4249

Endpoint Security Agent

windows-defender

Disk Encryption

None

Firewall

System

System Password

enabled

Endpoint Application

putty.exe

Application Signature (SHA 256)

512e27ef54ccaca2dded62e43b7983bff7c29
ef911ce504d099253ff03ef73da

Endpoint Username

[demo-isev1.acesec.local](#)

[https://demo-ise01.acesec.local](#)

[https://demo-ise01.acesec.local](#)

[https://demo-ise01.acesec.local](#)

[https://demo-ise01.acesec.local](#)

[https://demo-ise01.acesec.local](#)

[https://demo-ise01.acesec.local](#)

[demo-ise01.acesec.local](#)

Source IP	Destination Port	Destination Country	Internal IP	External IP	Action	Created
253				62.77.211.199	Allowed	Ch
3.199				192.168.100.1	Allowed	Sc
1.122				192.168.100.1	Allowed	Sc
				62.77.211.199	Allowed	Sc
.182				192.168.100.1	Allowed	Sc
.114				192.168.100.1	Allowed	Sc
.114				192.168.100.1	Allowed	Sc
.114				192.168.100.1	Allowed	Sc
.182				192.168.100.1	Allowed	Sc
				62.77.211.199	Allowed	Sc
.150	22				Allowed	
.150:22					Allowed	Ur
.150	443				Allowed	
.150	443				Allowed	n
c.hu)	demo-isev1.acesec.local	172.16.117.150	443		Allowed	
c.hu)	https://demo-ise01.acesec.local	172.16.117.150:443			Allowed	Ur
c.hu)	https://demo-ise01.acesec.local	172.16.117.150:443			Allowed	Ur
c.hu)	https://demo-ise01.acesec.local	172.16.117.150:443			Allowed	Ur
c.hu)	https://demo-ise01.acesec.local	172.16.117.150:443			Allowed	Ur
c.hu)	https://demo-ise01.acesec.local	172.16.117.150:443			Allowed	Ur
c.hu)	demo-ise01.acesec.local	172.16.117.150	443		Allowed	



Partner

Gold Provider
Gold Integrator

ACE NETWORK
INNOVATE TOGETHER

Köszönöm a figyelmet!