Controlling who and what gets on your network

Make your workforce more productive by providing easy, highly secure mobile access anywhere.

By 2022, there will be an average of **28.5 billion network devices**, up from 18 billion in 2017.*

Control access to your network and evolve to an intent-based network in four easy steps:

Step 1: Manage access policy

Is access under control?

See more

Step 2: Automate segmentation

Can you minimize risk?

See more

Step 3: Detect threats faster

Is encrypted data a growing risk?

See more

Step 4: Provide highly secure access anywhere

Can you protect mobile users?

See more

Gain control of your network

Register for Webinar

Step 1: Manage access policy

Ask yourself
Are you bogged down with the complexity of managing access policy across your entire network?

Something to consider
By centralizing policy management, you gain contextual awareness of everything hitting your network. You can secure fast access consistently and efficiently while relieving the stress of complex access management.

Recommended solutions
- Identity Services Engine (ISE)
- Security Services for ISE

Benefits: In addition to gaining full control of all devices accessing your network, ISE allows you to apply threat intelligence so that you can contain suspicious devices fast.

Find out more

Learn more about ISE

Did you know?
Traffic from wireless and mobile devices will account for more than 82 percent of total IP traffic by 2022.

Source: Cisco Visual Networking Index: Forecast and Trends, 2017 – 2022

Back to top

Step 2: Automate segmentation

Ask yourself
Is there an easy way to reduce the risk of spreading malware by segmenting groups of employees, guests, partners, and IoT devices?

Something to consider
Due to time-consuming manual operations, many IT teams find it difficult to apply segmentation effectively. With automated policy-based segmentation, you can reduce both threats and administration overhead.

Recommended solutions
- Cisco Software-Defined Access (SD-Access)
- Cisco DNA Center
- Cisco Catalyst 9000 Wireless and Switching Family
- SD-Access services

Benefits: Get full control over which users have access to which resources, anywhere in your enterprise. Integrating with your existing ISE deployment, Cisco Services can help accelerate your transition to SD-Access.

Find out more

Learn about SD-Access

Did you know?
An estimates 80% of breaches originate from the internal network.

Source: ZK Research 2018.

Back to top

Step 3: Detect threats faster

Ask yourself
How can you gain full visibility into who is accessing which resources? And how can you detect threats or anomalies even if data is encrypted?

Something to consider
By applying advanced cognitive analytics to all data crossing your network, you can identify attacks that would otherwise go undetected.

Recommended solutions
- Stealthwatch Enterprise
- Encrypted Traffic Analytics (ETA)

Benefits: With intraflow telemetry captured on Catalyst 9000 switches and ISR 4000 and ASR 1000 routers, you can identify malware even in encrypted traffic, without compromising privacy. We can help you get started faster with full lifecycle services for Stealthwatch.

Find out more

Download ETA white paper

Did you know?
In 2019, 70% of attacks will use encryption.

Source: Encrypted Traffics Analytics white paper, Cisco, 2018.

Back to top

Step 4: Provide highly secure access anywhere

Ask yourself
How can you ensure end-to-end security while meeting the diverse needs of users, devices and applications from point-of-access all the way to the data center?

Something to consider
By extending policy-based segmentation into the data center and industrial environments, you can achieve end-to-end protection all the way from users and devices to applications and services.

Recommended solutions
- Extended Enterprise
- Cisco Application Centric Infrastructure (ACI)

Benefits: Automating policies with intent-based networking across your campus, branch, extended enterprise, and multi-cloud environments helps you manage growing complexity and risk of mobile devices, applications, and services.

Find out more

Learn about Intent-Based Networking

Did you know?
For enterprises, 50% believe that their mobile infrastructure is at a high risk for a security breach.

Source: Security Risk and Trustworthiness Study, Cisco, 2017.

Back to top

Gain control of your network

Register for Webinar

Transform to an intent-based network with Cisco DNA

* Source: Cisco Visual Networking Index: Forecast and Trends, 2017 – 2022