Control who and what gets on your network

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

1. Control access to your network.
2. Automate segmentation.
3. Detect threats faster.
4. Provide highly secure access anywhere.

Step 1: Manage access policy

Job pursuit:

Prioritize and automate access policy using Cisco DNA.

Something to consider:

By 2021, there will be an average of 3.5 mobile devices per capita.*

Did you know?

Traffic from wireless and mobile devices will account for more than 63 percent of total IP traffic by 2021.


Recommendation:

• 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.

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)
• 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.

Something to consider:

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

Recommendation:

• 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.

Something to consider:

By blocking malicious Internet destinations before a connection is ever established, you can prevent malware from getting on your network and protect your users.

Recommended solutions:

• Cisco Umbrella
• Cisco AMP for Endpoints
• Cisco Security Connector for iOS

Benefits:

Protect users by stopping them from accessing malicious sites. Detect, block, and remediate advanced malware across all endpoints. And deepen visibility and control for iOS devices.

Test network readiness

Step 1: Manage access policy

See more

Step 2: Automate segmentation

See more

Step 3: Detect threats faster

See more

Step 4: Provide highly secure access anywhere

See more

* Source: Cisco VNI Report 2016

© 2018 Cisco and/or its affiliates. All rights reserved.