Cisco Identity Services Engine

Intent-Based Network Segmentation

Some walls are there for a good reason. But they must be adaptive.

For centuries, shipbuilders have used bulkhead partitions to help damaged ships stay afloat. With independent watertight compartments, a ship could withstand a hull breach in some sections without flooding the entire ship. However, permanent partitions can’t adapt to changing conditions and the ship can still sink if a particular breach exceeds design limits.

Traditional network segmentation is a lot like that. It partitions your network so that a cybersecurity breach or operational problem is confined to a certain area and doesn’t sink your entire network. The downside to traditional segmentation? It’s too static and cannot dynamically adjust to growing networks, changing conditions, and unexpected threats. Plus it’s often difficult to manage and scale, increasing the chances of configuration mistakes. Systems that require separation may actually be able communicate with each other, and what you thought was a watertight design might have big, hidden holes.

You need effective network segmentation to keep your organization afloat, but it must be simple, manageable, scalable, and adaptive. It needs to enforce the security policy you actually intend. That’s why you need Cisco Intent-Based Network (IBN) Segmentation.

Why do you need Cisco IBN Segmentation?

Astonishingly effective. It’s built directly into the network so that nothing unintended slips by.

Simple to manage. Gone are the days of lines and lines of complex, static configurations.

Dynamic and reactive. It adapts to today’s evolving cyber landscape and new, unexpected threats.

Highly scalable. It grows with your ever-changing network. You can start small and go big with ease.
With Cisco ISE, you can:

- Grant and control the right level of network access
- Improve your security posture and quickly contain breaches
- Gain complete endpoint visibility with context
- Streamline your access control policy management

To learn more, please visit [https://www.cisco.com/go/ise](https://www.cisco.com/go/ise) or contact your account representative.

---

**Cisco ISE implements segmentation precisely the way you intended**

Cisco Identity Services Engine (ISE) makes it easy to control segmentation policy consistently across wireless, wired, and VPN connections. Segmentation is just one of several use cases that makes ISE a critical part of your cybersecurity program.

We call it Group-Based Policy, meaning that ISE defines segmentation policy quickly through dynamic, scalable groups of roles and systems. Skip the time and expense associated with lines and lines of static, confusing configuration code. Adapt to changing conditions by dropping new systems into existing groups, and changing access permissions when a threat emerges. You can also reduce the scope of compliance with regulations like PCI, HIPAA, and DFARS. With Cisco ISE, you’ll gain all the benefits of network segmentation without the complexity.

**Licensing**

Segmentation requires the Base incense and does not consume any Session licenses. You can also get Segmentation with our Cisco Software-Defined Access (SD-Access) solution too.

Check out the [Cisco ISE Ordering Guide](https://www.cisco.com/go/orderingguide) and the [Cisco SD-Access Ordering Guide](https://www.cisco.com/go/orderingguide) for details.

---

### Which method enforces the policy you want?

**Without ISE**

Segmentation policy buried in lines of configuration code

```
Switch-1#show ip access-list
Extended IP access list SegPolicy
10 permit tcp 10.1.100.0 0.0.0.255 172.16.100.0 0.0.0.255 eq 80
20 permit tcp 10.1.100.0 0.0.0.255 172.16.100.0 0.0.0.255 eq 443
30 permit tcp 10.1.100.0 0.0.0.255 172.16.100.0 0.0.0.255 eq 8080
40 deny   tcp 10.1.100.0 0.0.0.255 172.16.100.0 0.0.0.255 eq 8081
```

**With ISE**

Segmentation policy enforced the way you actually intended through dynamic Group-Based Policy.

<table>
<thead>
<tr>
<th></th>
<th>Internet</th>
<th>ERM</th>
<th>Ordering</th>
<th>DevOps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visitor</td>
<td>Permit</td>
<td>Deny</td>
<td>Deny</td>
<td>Deny</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Permit</td>
<td>Permit</td>
<td>Deny</td>
<td>Deny</td>
</tr>
<tr>
<td>Sales</td>
<td>Permit</td>
<td>Deny</td>
<td>Permit</td>
<td>Deny</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>Permit</td>
<td>Deny</td>
<td>Deny</td>
<td>Permit</td>
</tr>
</tbody>
</table>