Cisco Umbrella

随时随地无处不在保护客户安全

Cisco Umbrella

教主技术进化论 2021

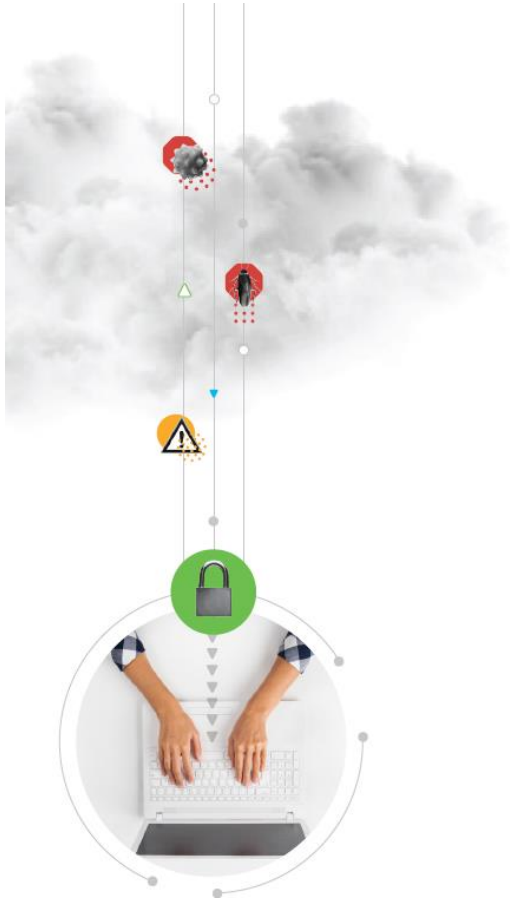
翻越下一座技术的高峰

目录

1.Cisco Umbrella介绍

Cisco Umbrella介绍（1）

The modern cybersecurity landscape 现代网络安全格局



For the majority of 2020, in the face of a global pandemic, the entire world has been grappling with massive change — in how we live, how we work, how we connect. But one area that's always been dynamic and rapidly evolving is the cyberthreat landscape.
从2020年的大部分时间里，面对全球大流行病，整个世界一直在应对着巨大的变化-我们的生活，工作方式，联系方式。但是，网络威胁形势一直是充满活力且迅速发展的领域

Cisco Umbrella has identified a number of major threat trends in the first three quarters of 2020 that will have serious implications for years to come:
Cisco Umbrella指出了2020年前三个季度的一些主要威胁趋势，这些趋势将对未来几年产生严重影响:

Cisco Umbrella介绍（2）

Trend #1: Trojans and droppers are getting a second life as new forms of malware delivery.
随着新形式的恶意软件交付，特洛伊木马和滴管正在重生

Trend #2: Orchestrated, multi-staged, evasive attacks are becoming the norm.
精心策划，多阶段，回避的攻击已成为常态

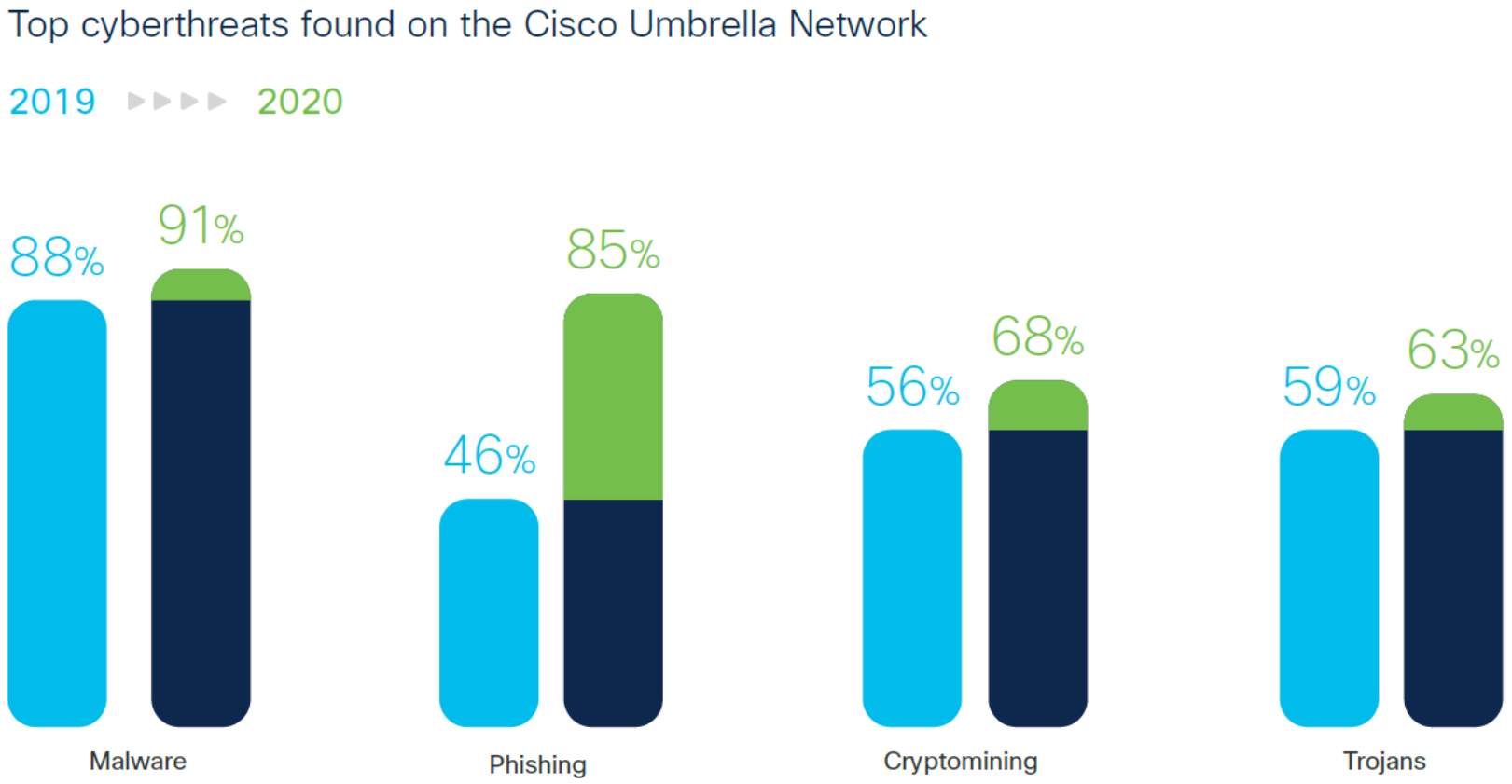
Trend #3: Cryptomining is opening the door to other types of cyberthreats.
加密货币正在为其他类型的网络威胁打开大门

Trend #4: Attackers are taking advantage of pandemic-related content to propagate attacks.
攻击者正在利用与大流行相关的内容来传播攻击

Cisco Umbrella介绍（3）

Today's threat landscape 当今的威胁形式

Phishing is on the rise as second most common threat. 网络钓鱼正在成为第二打常见威胁



Cisco Umbrella介绍（4）

Looking at the broad threats Cisco Umbrella's customer base encountered in the first nine months of 2020:
回顾2020年前九个月思科伞客户群面临的广泛威胁:

91%
of customers saw a domain linked to **malware**.

85%
saw a domain linked to **phishing**.

68%
saw a domain linked to **cryptomining**.

63%
saw a domain linked to **trojans**.

Cisco Umbrella介绍（5）

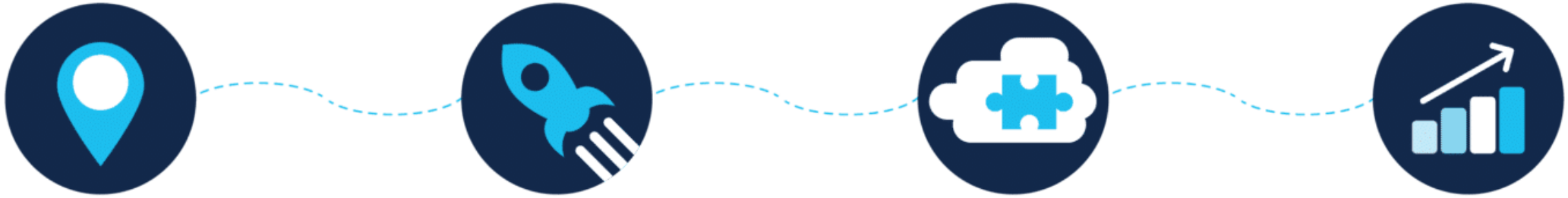
Cisco Umbrella: Flexible, fast, and effective cloud-delivered security 灵活，快速，有效的云交付安全

Cisco Umbrella offers flexible, cloud-delivered security when and how you need it. It combines multiple security functions into one solution, so you can extend protection to devices, remote users, and distributed locations anywhere. Umbrella is the easiest way to effectively protect your users everywhere in minutes.

当你需要无论如何umbrella提供灵活的,云交付的安全
保护扩展到任何地方的设备,远程用户和分布式位置
Umbrella可以在几分钟内保护无所不在的用户最简单的方法

Cisco Umbrella介绍（6）

The evolution of our cloud security service 云安全服务的发展



2006
Founded – as a recursive DNS provider (OpenDNS)
成立-递归DNS服务提供商

2012
Launched – DNS-layer security (OpenDNS Umbrella)
启动-DNS-layer安全

2015
Acquired – by Cisco
收购-思科

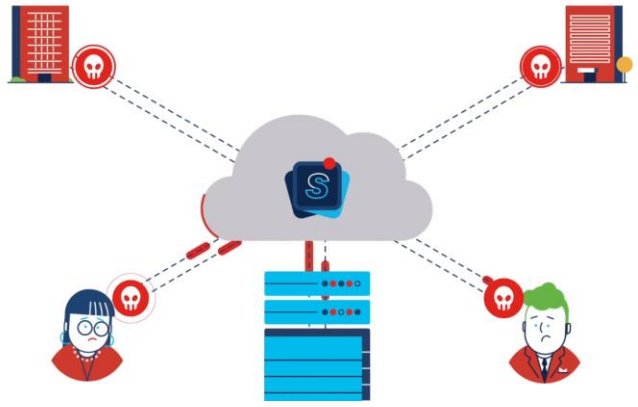
2019
Expanded – to integrate more security functions into a single service
扩展-在单一服务中集成更多的安全功能

Cisco Umbrella介绍（7）

Get to know the new Cisco Umbrella 了解新的思科umbrella

As a leading provider of recursive DNS services, we've helped businesses of all sizes and industries connect to the internet with confidence. We've built a reputation on easy deployment and powerful protection anywhere users work. 作为递归DNS服务的领先提供商，帮助各种规模和行业的企业连接到internet, 易于部署和用户工作在任何地方提供强大的保护

To help organizations embrace direct internet access, in addition to DNS-layer security and interactive threat intelligence, Cisco Umbrella now includes secure web gateway, firewall, and cloud access security broker (CASB) functionality, plus integration with Cisco SD-WAN, delivered from a single cloud security service.
除了DNS层安全性和交互威胁情报外，思科umbrella包括安全的web网关（SWG），防火墙，云访问代理（CASB）
以及与SD-WAN集成的云安全服务



Cisco Umbrella介绍（8）

Integrated cloud security service benefits

集成云安全服务的优势

Flexible security protection on and off network

灵活的网络内外安全保护

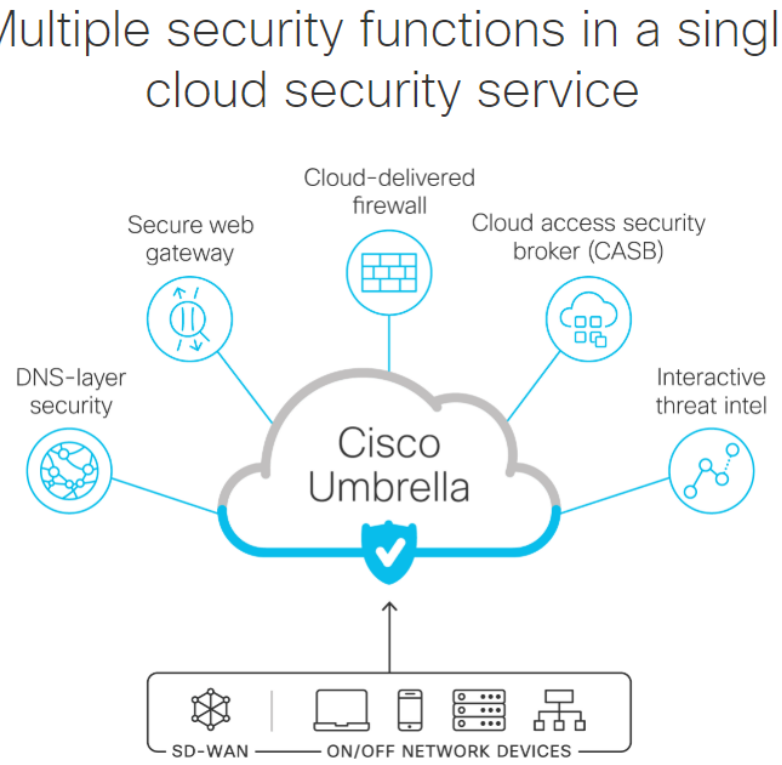
Consistent policies across remote locations

跨远程位置的一直策略

Better performance and user satisfaction everywhere

更好的性能和用户满意度

Cisco Umbrella介绍（9）



单个云安全服务中的多个安全功能

Cisco Umbrella介绍（10）

Cisco Umbrella's security functions

DNS-layer security
DNS层安全

Umbrella's DNS-layer security provides the fastest, easiest way to improve your security. It helps improve security visibility, detect compromised systems, and protect your users on and off the network by stopping threats over any port or protocol before they reach your network or endpoints.

通过组织任何端或协议商的威胁，提供高安全性和可见性，检测入侵，保护用户安全

Secure web gateway
安全web网关

Umbrella's secure web gateway logs and inspects web traffic for full visibility, URL and application controls, and protection against malware. Use IPsec tunnels, PAC files, or proxy chaining to forward traffic to our cloud-based proxy to enforce acceptable use policies and block advanced threats.

记录并检查web流量，实现完全可见性，URL和应用程序及恶意软件防护，基于云代理阻止高级威胁

Firewall
防火墙

Umbrella's firewall logs all activity and blocks unwanted traffic using IP, port, and protocol rules. To forward traffic, simply configure an IPsec tunnel from any network device. As new tunnels are created, policies are automatically applied for easy setup and consistent enforcement everywhere.

记录所有活动，并使用IP，端口和协议规则阻止不必要的流量，转发流量，配置IPSec隧道，自动应用策略，轻松设置和一直的实施

Cloud access security broker
云访问安全代理

Umbrella exposes shadow IT by providing the ability to detect and report on cloud applications in use across your organization. For discovered apps, view details on the risk level and block or control usage to better manage cloud adoption and reduce risk.

检查和报告使用的云应用程序的能力，可以查看并组织或控制有风险的应用程序，降低风险

Interactive threat intelligence
互动威胁情报

Our unique view of the internet gives us unprecedented insight into malicious domains, IPs, and URLs. Available via a console and API, Umbrella Investigate provides real-time context on malware, phishing, botnets, trojans and other threats enabling faster incident investigation and response.

对恶意域，IP和URL有空前的洞察力，通过控制台和API使用，提供威胁，更快调查和响应，

Integration with SD-WAN
与SD-WAN集成

The Umbrella and Cisco SD-WAN integration deploys easily across your network for powerful cloud security and protection against internet threats. Our integrated approach secures cloud access and efficiently protects your branch users, connected devices, and app usage from all direct internet access breakouts.

Umbrella和SD-WAN集成在网络中部署，实现强大的云安全性能并防御internet威胁

DNS-layer security介绍（1）

The leader in DNS-layer security

As a leading provider of network security and recursive DNS services, Cisco Umbrella provides the quickest, most effective way to improve your security stack. From small businesses without dedicated security professionals to multinational enterprises with complex environments, it takes mere minutes to gain a new layer of breach protection and internet-wide visibility on and off your network.

作为网络安全和递归DNS服务的领先提供商，Cisco Umbrella提供了最快，最有效的方法来改善您的安全性堆栈。从没有专门的安全专家的小型企业到具有复杂环境的跨国企业，只需几分钟就可以在网络上和网络外获得新的违规保护层和整个Internet范围的可见性。

1：DNS-layer security介绍（2）

Cloud security built into the foundation of the internet 云安全性已成为互联网的基础

We use the internet's infrastructure to our advantage to block malicious and unwanted domains, IP addresses, and cloud applications before a connection is ever established. Built 100% in the cloud, Umbrella provides better accuracy and detection of compromised systems — improving security visibility and network protection.

在建立连接之前，我们利用互联网的基础设施来阻止恶意和不需要的域，IP地址和云应用程序。 Umbrella在云中100％构建，可提供更高的准确性和对受感染系统的检测-改善安全可见性和网络保护。

1： DNS-layer security介绍（3）

Here's how:

DNS & IP layer enforcement

DNS和IP层实施

Umbrella uses DNS to stop threats over all ports and protocols – even direct-to-IP connections. Stop malware earlier and prevent callbacks to attackers if infected machines connect to your network.

使用DNS来阻止所有端口和协议（甚至是直接IP连接）上的威胁

Web security via selective proxy

选择性代理的网络安全

Umbrella routes requests to risky domains to a selective proxy for deeper URL and file inspection. Effectively protect without delay or performance impact.

请求到危险域的路由路由到选择性代理，进行更深入的URL和文件检查有效保护而不会延迟或影响性能

App discovery & blocking

应用发现和阻止

Umbrella provides visibility into cloud apps used across your organization, so you can identify potential risk and block specific applications easily.

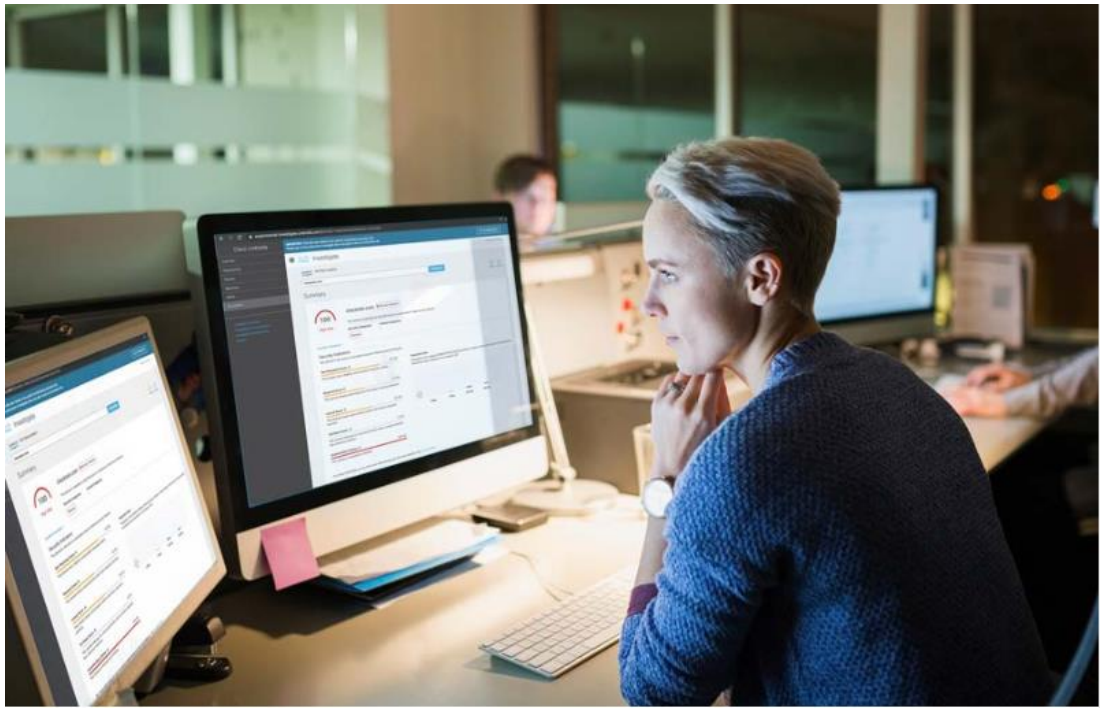
可以查看整个 阻止中使用的云应用程序，识别潜在风险并轻松阻止特定的应用程序

1： DNS-layer security介绍（4）

Unmatched threat intelligence to stop attacks earlier 无与伦比的威胁情报可尽早阻止攻击

Imagine having the strength of over 300 security researchers on your team — that's what you get with Cisco Talos threat intelligence in Umbrella. Umbrella also uses statistical and machine learning models to uncover new attacks staged on the internet. Plus, the Umbrella Investigate console and API provides real-time context on malware, phishing, botnets, and other threats enabling faster incident investigation and response.

团队拥有300多名安全研究人员，这就是在umbrella中使用Cisco Talos威胁情报所获得的。umbrella还使用统计和机器学习模型来发现互联网上发生的新攻击。此外，Umbrella Investigate控制台和API提供了有关恶意软件，网络钓鱼，僵尸网络和其他威胁的实时上下文，从而可以更快地进行事件调查和响应

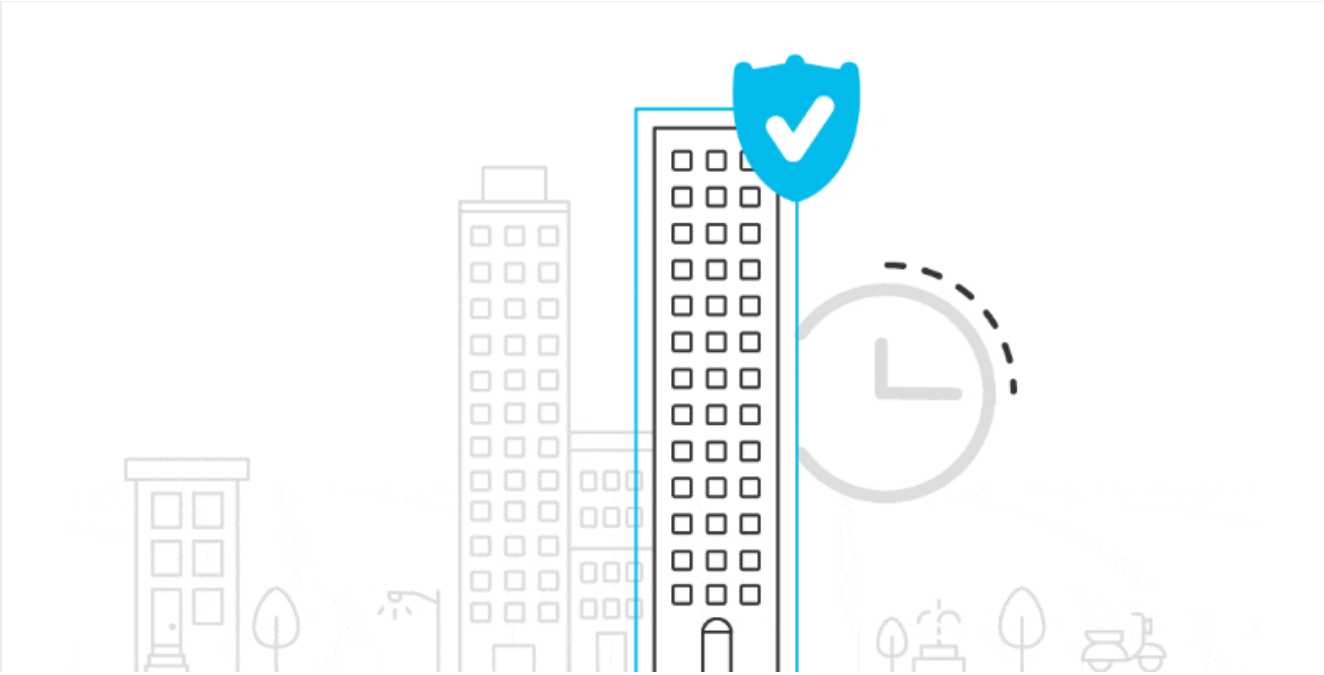


1：DNS-layer security介绍（5）

Deploy and configure in minutes for fast time to value

Umbrella is the simplest cloud security service you'll ever deploy. There is no hardware to install or software to manually update, and the browser-based interface provides quick setup and ongoing management.

Umbrella是将部署的最简单的云安全服务。无需安装硬件或手动更新软件，基于浏览器的界面可提供快速设置和持续管理



1：DNS-layer security介绍（6）

Here's how:

On-network devices
网络设备

Just point your DNS from any network device. Using your Cisco footprint – SD-WAN, ISR 1K and 4K, Meraki MR, and WLAN, provision protection across hundreds of network devices in one click. Implement powerful security without operational complexity.

只需从任何网络设备指向您的DNS。利用SD-WAN，ISR 1K和4K，Meraki MR和WLAN，一键式为数百个网络设备提供保护。实施功能强大的安全性，而无需操作复杂性

Off-network laptops
网外笔记本电脑

Protect laptops when the VPN is off with Umbrella's lightweight roaming client or built-in Cisco AnyConnect integration. Easily extend protection beyond the corporate network with our cloud security service.

当VPN处于关闭状态时，通过umbrella的轻量级漫游客户端或内置的Cisco Anyconnect集成来保护笔记本电脑，借助云安全服务，保护范为扩展到网络网络之外

Mobile devices
移动设备

Using the Umbrella Android client or the Cisco Security Connector iOS app and Umbrella extension, easily prevent mobile users from clicking on malicious links, protecting from threats even over cellular networks and public Wi-Fi.

使用umbrella android客户端或者Cisco security connector ios应用程序和umbrella扩展程序，轻松防止移动用户单机恶意链接，即使在蜂窝网络和公共WI-FI也能面手威胁

1：DNS-layer security介绍（7）

DNS-layer security benefits: DNS层安全性优势

Reduce malware and alerts
减少恶意软件和警报

Umbrella reduces the number of infections and alerts you see from other security products by stopping threats at the earliest point. With no hardware to install or software to manually update, ongoing management is simple.

Umbrella通过尽早阻止威胁来减少感染数量并从其他安全产品中看到警报，无需安装硬件或手动更新软件，管理非常简单

Improve internet performance
改善互联网性能

Umbrella has a highly resilient network that boasts 100% business uptime since 2006. Our 33+ plus data centers worldwide use Anycast routing so requests are transparently sent to the fastest available with automatic failover.

Umbrella具有高度灵活的网络，自2006年以来，该网络拥有100%的正常运行时间。我们遍布全球的33多个数据中心使用Anycast路由，因此可以透明地将请求发送到具有自动故障转移功能的最快的可用站点

Proactively respond to threats
主动应对威胁

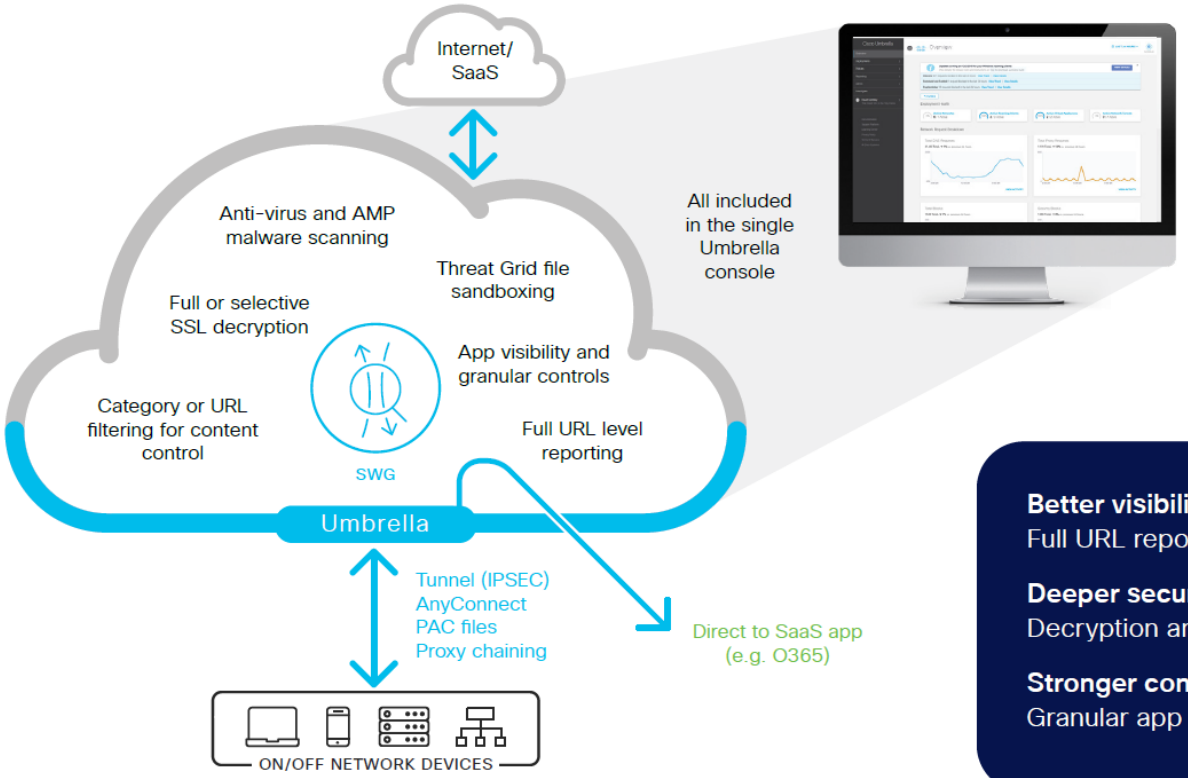
Umbrella logs all DNS activity to simplify investigations. Umbrella Investigate provides context to prioritize incidents and speed up response. Cisco Threat Response automates insights across Cisco products for quick answers.

Umbrella会记录所有DNS活动，以简化调查。Umbrella Investigate提供了用于确定事件优先级并加快响应速度的环境。思科威胁响应可自动提供有关思科产品的见解，以快速获得答案

2：Secure Web Gateway介绍（1）

The Umbrella SWG functionality provides cloud native, full proxy capabilities to improve performance and reduce risk by efficiently logging, inspecting, and controlling web traffic.

Umbrella SWG功能提供了云本机的完整代理功能，以提高性能通过有效地记录，检查和控制Web流量来降低风险。



Better visibility:
Full URL reporting

Deeper security:
Decryption and file inspection

Stronger control:
Granular app controls

2：Secure Web Gateway介绍（2）

Challenges 挑战

With the majority of attacks originating from the internet, you need to protect your users' web traffic wherever they are, from headquarters to branch offices, to roaming laptops. All web traffic must be logged to maintain compliance and enable investigations. At the same time, you have to protect users from malware and enforce acceptable use policies to maintain a healthy work environment and protect sensitive data. All of this must be done without hurting user performance or adding undue complexity to network and security infrastructure. As the number of branch offices and remote users increases, the concept of placing a proxy appliance at every location becomes impractical because of the cost and expertise required for deployment and maintenance. A viable solution must provide the visibility, control and protection required without impeding performance or end user satisfaction.

由于大多数攻击均来自互联网，因此需要保护用户的网络流量，无论他们身在何处，从总部到分支机构，再到漫游笔记本电脑。 必须记录所有Web流量以维护合规性并启用调查。 同时，必须保护用户免受恶意软件的侵害，并执行可接受的使用策略以维持健康的工作环境并保护敏感数据。 所有这些都必须在不损害用户性能或不给网络和安全基础架构增加不必要的复杂性的情况下完成。 随着分支机构和远程用户数量的增加，由于部署和维护所需的成本和专业知识，在每个位置放置代理设备的概念变得不切实际。 可行的解决方案必须提供所需的可见性，控制和保护，而又不影响性能或最终用户满意度

2：Secure Web Gateway介绍（3）

overview 概括

Cisco Umbrella secure web gateway functionality is a cloud-native service that can proxy all of your web traffic for a greater level of visibility and control. It enables you to log all usage, protect against viruses and malware, enforce acceptable use policies, and simplify investigations. These full proxy capabilities are part of Umbrella's SIG Essentials package which also includes DNS Security a cloud-delivered firewall, CASB functionality, and Umbrella's Investigate threat intelligence data to provide a robust, secure internet gateway.

Cisco Umbrella安全Web网关功能是一项云原生服务，可以代理所有Web流量，以实现更高级别的可见性和控制力。 它使您能够记录所有使用情况，防御病毒和恶意软件，实施可接受的使用策略并简化调查。 这些完整的代理功能是Umbrella的SIG Essentials软件包的一部分，该软件包还包括DNS安全性，云交付的防火墙，CASB功能以及Umbrella的Investigate威胁情报数据，以提供可靠，安全的互联网网关。

2：Secure Web Gateway介绍（4）

Feature brief 功能简介

While these capabilities are necessary from all locations, they are especially critical for branch offices and roaming users that are increasingly going direct to the internet. Umbrella provides a variety of ways to redirect outgoing traffic to the Umbrella cloud including IPSec tunnels, AnyConnect clients, PAC files or proxy chaining. Your traffic then can be inspected and controlled to both meet compliance requirements and internal acceptable use policies. It is also scanned to detect and block known malicious destinations. Files are scanned and known bad items blocked. New or suspicious files can be routed to a sandbox for deeper inspection and retrospective alerts can be generated if a file starts to display bad behavior. Umbrella can utilize the Microsoft API to route the appropriate O365 traffic directly to the nearest Microsoft data center to maximize performance.
All of these capabilities are integrated into a single, easy to use Umbrella interface along with market leading DNS security and cloud-delivered firewall functionality to reduce the amount of integration and management tasks for your security team.

尽管在所有位置都需要这些功能，但对于越来越多地直接连接到Internet的分支机构和漫游用户而言，它们尤其重要。 Umbrella提供了多种将传出的流量重定向到Umbrella云的方法，包括IPSec隧道，AnyConnect客户端，PAC文件或代理链接。然后可以检查和控制您的流量，以满足合规性要求和内部可接受的使用政策。还会对其进行扫描以检测和阻止已知的恶意目标。扫描文件，并阻止已知的不良项目。可以将新文件或可疑文件路由到沙箱以进行更深入的检查，如果文件开始显示不良行为，则可以生成追溯警报。伞可以利用Microsoft API将适当的O365通信直接路由到最近的Microsoft数据中心，以最大化性能。
所有这些功能都集成到一个简单易用的Umbrella界面中，并具有市场领先的DNS安全性和云交付的防火墙功能，从而减少了安全团队的集成和管理任务量。

2：Secure Web Gateway介绍（5）

Feature	Benefit
Full URL logging/reporting	Better visibility of trends and faster investigations which results in lower remediation costs 更好了解趋势和更快的调查，从而降低补救成本
Anti-virus and anti-malware file inspection and blocking	Thorough anti-virus and anti-malware scanning to reduce the number of successful attacks 彻底的反病毒和反恶意软件扫描，以减少成功攻击数量
SSL decryption (full/selective)	Ability to decrypt and inspect encrypted web traffic and block hidden attacks to lower the number of infections 解密和检查加密的web流量并阻止隐蔽攻击,降低感染数量
Content control (URL filtering, acceptable use enforcement)	Easily enforce acceptable use policies and block harmful URLs to ensure compliance and protect against malicious destinations 轻松实施可接受使用策略并阻止有害URL，以确保合规性和防御恶意目标
File sandboxing and retrospective alerts	Discover hidden threats and evasive malware that is used in advanced attacks to avoid breaches 发现用于高级攻击的潜在威胁和逃避性恶意软件，以避免破坏
Application visibility and control	Reduced risk from Shadow IT apps through visibility, blocking and granular activity controls 通过可见性,阻止和精细的活动控制来降低阴影IT应用程序带来的风险
Automated tunnel failover	Faster deployment and simplified management of tunnels 更快的部署和简化隧道管理

2：Secure Web Gateway介绍（6）

Key capabilities 关键能力

URL level logging and reporting URL级别的日志记录和报告

The Umbrella console includes detailed logging reports with the full URL address, network identity, allow or block action plus the external IP address. You can filter by protocol (HTTP, HTTPS), event type, identity type and the security category of the event. Web content filtering is also provided at the URL level to block specific destinations that you don't want users to access. Acceptable use policies can be enforced more broadly by selecting and blocking the designated categories that your organization wants to prohibit.

Umbrella控制台包含详细的日志记录报告，其中包含完整的URL地址，网络标识，允许或阻止的操作以及外部IP地址。 您可以按协议（HTTP，HTTPS），事件类型，身份类型和事件的安全性类别进行过滤。 在URL级别还提供了Web内容过滤，以阻止您不希望用户访问的特定目标。 通过选择和阻止组织要禁止的指定类别，可以更广泛地实施可接受的使用策略。

SSL traffic decryption and inspection SSL流量解密和检查

An increasing percentage of web traffic is encrypted and attackers are exploiting this to hide malware, hoping to avoid detection. Umbrella can decrypt and inspect either all or selective SSL encrypted traffic. Many organizations don't want to decrypt healthcare or personal finance information for their employees for privacy reasons, so they leverage the selective option for a more fine-tuned level of control.

越来越多的Web流量被加密，攻击者正在利用它来隐藏恶意软件，希望避免被检测到。 umbrella可以解密并检查所有SSL加密流量或选择性SSL加密流量。 许多组织不想解密医疗保健或出于隐私原因为其雇员提供的个人财务信息，因此他们利用选择性选项来实现更好的控制级别。

2：Secure Web Gateway介绍（7）

Advanced anti-virus and anti-malware protection 先进的防病毒和防恶意软件防护

Umbrella is powered by Cisco Talos threat intelligence which inspects over 1.5 million unique malware samples per day. Multiple tools are uses to scan for viruses and Cisco's Advanced Malware Protection engine searches hundreds of billions of events per day and blocks over 20 billion threats each day. All of this learning is used to protect the web traffic that is sent to the Umbrella secure web gateway.

Umbrella由Cisco Talos威胁情报提供支持，该情报每天检查超过150万个独特的恶意软件样本。 多种工具可用于扫描病毒，思科的高级恶意软件防护引擎每天可搜索数千亿个事件，每天可阻止超过200亿个威胁。 所有这些学习都被使用保护发送到Umbrella安全Web网关的Web流量。

App visibility and control 应用程序可见性和控制

Umbrella helps to expose shadow IT by providing the ability to detect and report on the cloud applications that are in use across your environment. We automatically generate overview reports on the vendor, category, application and the volume of activity for each discovered app. The drill down reports include risk information such as the web reputation score, financial viability and relevant compliance certifications. This insight enables better management of cloud adoption, risk reduction and the ability to block the use of offensive or inappropriate cloud applications in the work environment. In situations where a deeper level of control is required, Umbrella provides granular activity controls for a popular set of SaaS apps.

Umbrella提供了检测和报告整个环境中正在使用的云应用程序的能力，从而有助于揭露影子IT。 我们会自动生成有关每个发现的应用程序的供应商，类别，应用程序和活动量的概述报告。 深入报告包括风险信息，例如网络信誉评分，财务可行性和相关合规性证明。 这种洞察力可以更好地管理云的采用，降低风险，以及阻止在工作环境中使用令人反感或不合适的云应用程序的能力。 在需要更深层次控制的情况下，Umbrella为一组流行的SaaS应用程序提供了精细的活动控制。

2：Secure Web Gateway介绍（8）

Threat Grid sandboxing 威胁网格沙箱

The full proxy includes file sandboxing* for advanced threat protection. New or suspicious file types that make it through the AMP inspection are sent to the Threat Grid sandbox to find evasive threats including time-delayed malware. Administrators are sent retrospective alerts if files that were originally believed to be clean, start to show malicious behavior.

完整的代理包括用于高级威胁防护的文件沙箱。 通过AMP检查的新文件或可疑文件类型将被发送到Threat Grid沙箱，以发现包括时延恶意软件在内的回避威胁。 如果最初认为是干净的文件开始显示恶意行为，则会向管理员发送追溯警报。

Integration with SD-WAN and AnyConnect for secure, direct internet access

Many branches and remote users are moving to direct internet access for performance and cost reasons. Umbrella is integrated with Cisco SD-WAN and Meraki to simplify the process of redirecting web traffic to the Umbrella cloud service. The SWG is also integrated with the Cisco AnyConnect client to make it easy to extend Umbrella protection to both on and off-network devices that have the AnyConnect client installed. These integrations simplify deployment and strengthen security while streamlining traffic flow and improving end user performance.

与SD-WAN和AnyConnect集成，可实现安全，直接的Internet访问由于性能和成本原因，许多分支机构和远程用户都转向直接访问Internet。 Umbrella与Cisco SD-WAN和Meraki集成在一起，以简化将网络流量重定向到Umbrella云服务的过程。 SWG还与Cisco AnyConnect客户端集成在一起，可以轻松地将伞保护扩展到已安装AnyConnect客户端的网络内和网络外设备。 这些集成简化了部署并增强了安全性，同时简化了流量并提高了最终用户的性能。

2：Secure Web Gateway介绍（9）

Microsoft Office 365 direct internet connections Microsoft Office 365直接互联网连接

Migration to O365 has a significant impact on the amount and type of network traffic. This typically causes performance issues in traditional hub and spoke networks. Umbrella leverages a Microsoft API to dynamically detect O365 traffic. This allows Umbrella to immediately identify domains, URLs and IP addresses that are critical to the operation of Office 365. When O365 direct access is enabled on an Umbrella instance, the appropriate traffic will be routed directly to the nearest Microsoft location using Umbrella's peering relationships to maximize performance and user satisfaction.

迁移到O365对网络流量的数量和类型有重大影响。 这通常会在传统的集线器和分支网络中引起性能问题。 Umbrella利用Microsoft API动态检测O365流量。 这使Umbrella可以立即识别对Office 365的操作至关重要的域，URL和IP地址。在Umbrella实例上启用O365直接访问后，适当的流量将使用Umbrella的对等关系直接路由到最近的Microsoft位置。 最大化性能和用户满意度。

Multiple cloud security capabilities in one console 在一个控制台中提供多种云安全功能

In addition to the web gateway functionality, Umbrella also provides DNS-layer security, a cloud-delivered firewall, cloud access security broker (CASB) capabilities, and market leading threat intelligence — all configured and managed from a single, easy to use, cloud dashboard.

除Web网关功能外，Umbrella还提供DNS层安全性，云交付的防火墙，云访问安全代理（CASB）功能和市场领先的威胁情报-所有这些都通过单个易于使用的云进行配置和管理。 仪表板。

2：Secure Web Gateway介绍（10）

Automated tunnel functions to simplify deployment and maintenance

自动化的隧道功能可简化部署和维护

Most other cloud-based SWGs require you to set up a primary and backup tunnel for each location which adds to the deployment time. In this case, when problems occur in the initial data center, the administrator has to go into the console to redirect the traffic to the backup tunnel. Umbrella uses patent pending Anycast related technology to provide automated tunnel failover which simplifies the deployment process and eliminates the need for a manual intervention to switch tunnels and data centers.

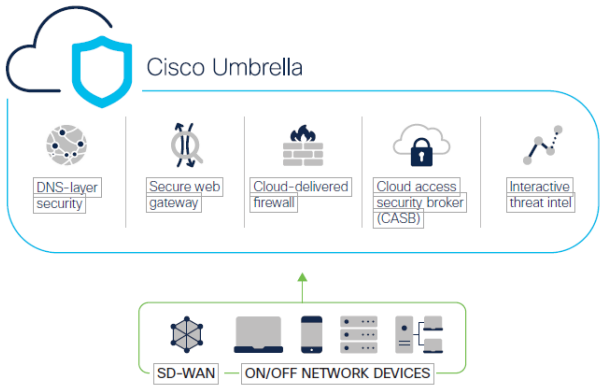
大多数其他基于云的SWG都要求为每个位置设置主要和备份隧道，这会增加部署时间。 在这种情况下，当初始数据中心出现问题时，管理员必须进入控制台以将流量重定向到备份隧道。 Umbrella使用正在申请专利的Anycast相关技术来提供自动隧道故障转移，从而简化了部署过程，并且无需人工干预来切换隧道和数据中心。

3：Cloud-Delivered Firewall介绍（1）

Shifting market propels cloud-delivered security 瞬息万变的市场推动了云交付的安全性

Unprecedented shifts in enterprise security and networking continue unabated. Expansive cloud application use is fundamental to business. Remote locations and roaming users are proliferating. Traditionally, organizations routed internet traffic from remote locations back to a central location for security, yet this has become impractical due to high cost and performance challenges. Remote offices find ways to use direct-to-internet access (DIA) for convenience and performance.
In response, many organizations are implementing software-defined WAN (SD-WAN) solutions to facilitate efficient DIA. Yet this brings new security challenges. To manage those, customers want security that is “built in” and does not require appliances everywhere. Customers are looking to cloud-delivered security services to answer these security requirements in a scalable and simple fashion.

企业安全性和网络方面的空前变化仍在继续。 广泛使用云应用程序是业务的基础。 远程位置和漫游用户正在激增。 传统上，组织为了安全起见将互联网流量从远程位置路由回中心位置，但是由于高成本和性能挑战，这已变得不切实际。 远程办公室找到了使用直接到Internet访问（DIA）的方法，以提供便利和性能。
作为响应，许多组织正在实施软件定义的WAN（SD-WAN）解决方案，以促进高效的DIA。 然而，这带来了新的安全挑战。 为了管理这些设备，客户需要“内置”的安全性，并且不需要到处都有设备。 客户希望通过云提供的安全服务以可扩展和简单的方式满足这些安全要求



3：Cloud-Delivered Firewall介绍（2）

Cisco Umbrella: Multiple security functions in a single, cloud-native service 单个云原生服务中的多种安全功能

Cisco Umbrella unifies multiple security functions in a single cloud service to secure internet access and control cloud app usage across networks, branch offices, and roaming users. Unlike disparate security tools, Umbrella brings together secure web gateway, cloud-delivered firewall, DNS-layer security, cloud access security broker functionality, and threat intelligence into a single cloud service. By enabling all of this from a single dashboard, Umbrella significantly reduces the time, money, and resources required for deployment, configuration, and integration tasks.

思科umbrella在一个云服务中统一了多个安全功能，以保护互联网访问并控制跨网络，分支机构和漫游用户的云应用使用情况。 与完全不同的安全工具不同，Umbrella将安全的Web网关，云交付的防火墙，DNS层安全性，云访问安全代理功能和威胁情报集成到单个云服务中。 通过在单个仪表板上启用所有这些功能，Umbrella大大减少了部署，配置和集成任务所需的时间，金钱和资源。

3：Cloud-Delivered Firewall介绍（3）

Intelligent traffic routing 智能流量路由

By intelligently steering different traffic types to the appropriate capability, Umbrella achieves an effective balance of security efficacy, user performance, and management simplicity. By using a single IPSec tunnel, outbound traffic is sent to Umbrella so that web traffic over ports 80/443 is secured by the secure web gateway, DNS requests by DNS-layer security, and non-web/non-DNS traffic by the cloud-delivered firewall. As the service evolves, deep inspection may inform when traffic should pass between functions to achieve even higher efficacy.

通过将不同的流量类型智能地引导到适当的功能，Umbrella可以在安全性，用户性能和管理简便性之间达到有效的平衡。 通过使用单个IPSec隧道，出站流量将发送到Umbrella，以便通过安全的Web网关，通过DNS层安全性进行的DNS请求以及通过云的非Web /非DNS流量来保护端口80/443上的Web流量。 交付的防火墙。 随着服务的发展，深度检查可以告知流量何时应在功能之间通过，以实现更高的功效。

3：Cloud-Delivered Firewall介绍（4）

Spotlight on cloud-delivered firewall 聚焦在云交付的防火墙上

The cloud-delivered firewall is essential today, yet in the future, its importance will considerably grow. As Umbrella steers traffic to the ideal security function, we commonly see 15% secured by cloud-delivered firewall. This could include mobile apps, peer-to-peer file sharing, collaboration (e.g. Webex or ZOOM), O365, or any non-web or non-DNS traffic. Although 15% may seem a relatively small portion, this type of traffic is on the cusp of exploding. Consider the shift of professionals working via phone that drives mobile app proliferation. Consider the expansion
of students who extensively use native apps in Macbooks. As these changes and more continue, the percentage of traffic secured by the cloud-delivered firewall will march upward.

云交付的防火墙在今天至关重要，但是在将来，其重要性将大大提高。 当雨伞将流量引导到理想的安全功能时，我们通常会看到15％的安全由云交付的防火墙保护。 这可能包括移动应用程序，对等文件共享，协作（例如Webex或ZOOM），O365或任何非Web或非DNS流量。 尽管15％的流量似乎只占很小的一部分，但这种流量正处于爆炸式增长的风口浪尖。 考虑通过电话工作的专业人员的转移，这推动了移动应用程序的普及。 考虑扩展
广泛使用Macbooks本机应用程序的学生。 随着这些变化以及更多变化的继续，由云交付的防火墙保护的流量百分比将继续上升。

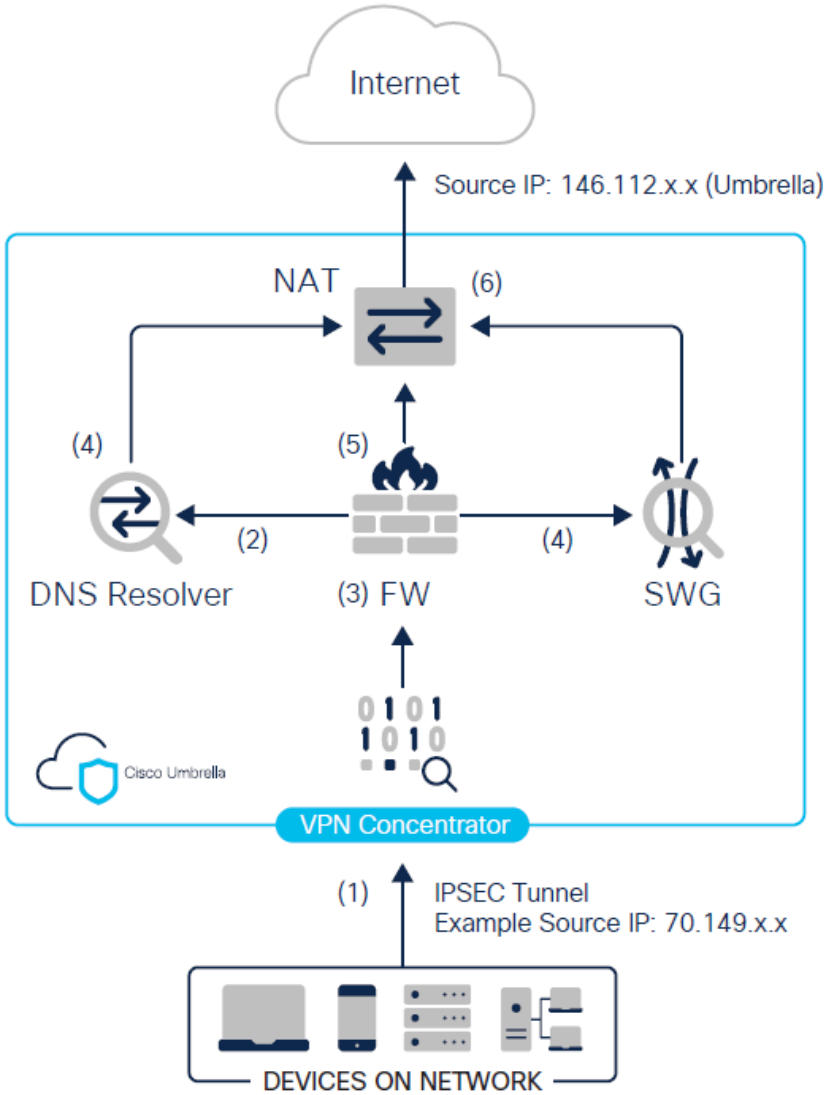
3：Cloud-Delivered Firewall介绍（5）

Cloud-delivered firewall for visibility and control 云交付的防火墙，用于可见性和控制

The Umbrella cloud-delivered firewall provides visibility and control for outbound internet traffic across all ports and protocols. It logs all activity and blocks unwanted outbound traffic using IP, port, and protocol rules (layer 3 / 4 firewall) as well as via application visibility and control (layer 7 firewall). Forward traffic to the cloud-delivered firewall by simply configuring an IPSec tunnel from any network device. With layer 7 application visibility and control, Umbrella recognizes non-web applications and takes appropriate action to block/allow them. The cloud-delivered firewall employs signature detection to identify and block 2,800 applications (more added on a regular basis). This extends the application detection and blocking already performed with Umbrella's DNS-layer security and secure web gateway. For example, an organization may choose not to allow Microsoft Teams (formerly Skype), an application whose capabilities use various ports and protocols. The Umbrella secure web gateway blocks Microsoft Team's web traffic over ports 80/443. However, the Umbrella cloud-delivered firewall expands coverage by blocking Team's voice and video traffic.

Umbrella云交付的防火墙可提供可见性和对跨所有端口和协议的出站Internet通信的控制。它记录所有活动，并使用IP，端口和协议规则（第3层/第4层防火墙）以及通过应用程序可见性和控制（第7层防火墙）来阻止不需要的出站流量。只需配置来自任何网络设备的IPSec隧道，即可将流量转发到云交付的防火墙。借助第7层应用程序的可见性和控制力，Umbrella可以识别非Web应用程序并采取适当的措施来阻止/允许它们。云交付的防火墙使用签名检测来识别和阻止2,800个应用程序（定期添加）。这扩展了已经通过Umbrella的DNS层安全性和安全Web网关执行的应用程序检测和阻止。例如，组织可以选择不允许Microsoft Teams（以前称为Skype），其功能使用各种端口和协议。 Umbrella安全的网络网关阻止Microsoft Team通过端口80/443进行的网络流量。但是，由Umbrella云提供的防火墙通过阻止Team的语音和视频流量来扩大覆盖范围。

3：Cloud-Delivered Firewall介绍（6）



Traffic flow

1. Forward traffic via IPSEC tunnel to the cloud
2. Resolve Umbrella DNS security per policy, allow or block. Traffic is logged.
3. Traffic inspected in CDFW. If Web traffic allowed over 80/443, it's sent to SWG (4). All other traffic inspected by firewall (goes to 5). Traffic is logged.
4. SWG does its policy inspection. Traffic is logged.
5. 'Allowed' traffic egresses through NAT

3：Cloud-Delivered Firewall介绍（7）

Anycast and beyond for rock-solid reliability cruise ahead 任播和其他应用程序可实现可靠性

Umbrella's IPSec tunnel approach, based on an innovative use of Anycast, simplifies deployment, boosts performance, and improves reliability. It enables the Umbrella infrastructure to execute planned updates, additions, and removals — even take down an entire data center — with minimal impact to users. And in the rare instance of an unplanned interruption, Umbrella's patent-pending Anycast deployment performs automatic data center failover with no loss of redundancy protection.

Umbrella的IPSec隧道方法，该方法以创新的方式使用任播，简化部署，提高性能，并提高可靠性。它启用了伞式基础设施执行计划的更新，添加和删除-甚至关闭整个数据中心-对用户的影响最小。 在极少数情况下Umbrella正在申请专利的Anycast部署是一项计划外的中断，可以执行自动数据中心故障转移，而不会丢失冗余保护。

Pace of change rockets forward 变革的步伐使火箭前进

Layer 7 application visibility and control recently enriched the Umbrella cloud-delivered firewall, but the pace of enhancement will not slow. Right on its heels will come further capabilities and enhancements to delight Umbrella customers.

第7层应用程序的可见性和控件最近丰富了Umbrella云交付的防火墙，但是增强的速度不会减慢。 紧随其后的将是进一步的功能和增强，以使伞的客户满意。

3：Cloud-Delivered Firewall介绍（8）

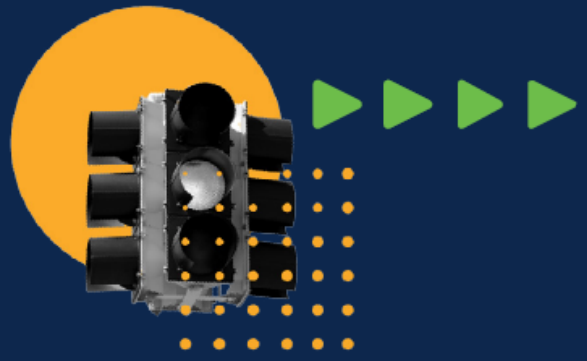
Use cases using layer 7 application visibility and control 使用7层应用可视性和控制

Block shadow IT over non-web ports

Example 阻止非web端口

Stop use of unapproved SaaS apps

- WebEx allowed
- MS Teams video not allowed
- Google Hangouts not allowed



Block insecure applications on non-standard ports

Example 阻止非标准端口上不安全应用

Stop remote virtual terminal connection into other networks

- (e.g. telnet via non-standard port 8080)

Stop file transfer

- (e.g. FTP via non-standard port 1003)

Block unsanctioned traffic over non-web ports

Example 阻止非web端口上未经批准

Stop use of unapproved traffic such as peer-to-peer traffic

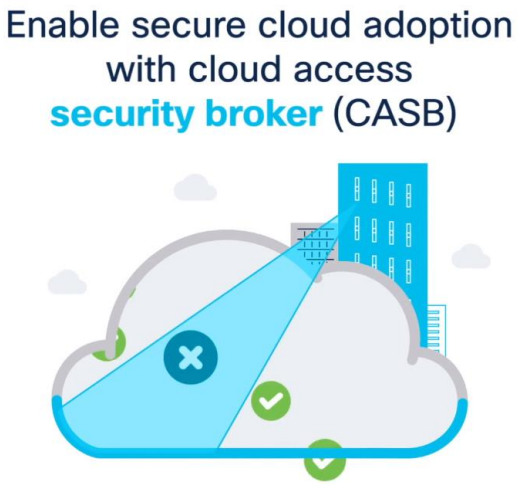
- (e.g. TOR or BitTorrent)

4：Cloud access security broker介绍（1）

Cloud services: Shadow IT challenges 影子IT挑战

Cloud usage continues to expand as end users and departments become more comfortable acquiring cloud services. The typical organization is only aware of a small fraction of its overall cloud activity. The lack of a coordinated cloud enablement strategy leads to a broad set of productivity, expense, security, and support issues.
You need full visibility and risk information to manage cloud adoption in a secure and organized fashion. Once decisions are made about specific apps, you need the ability to block access to applications that are not approved to reduce the risk of sensitive data loss, account compromises, and malware infections.

随着最终用户和部门越来越习惯于购买云服务，云使用量继续增长。 典型的组织仅了解其总体云活动的一小部分。 缺乏协调的云支持策略会导致一系列广泛的生产力，费用，安全性和支持问题。您需要全面的可见性和风险信息，才能以安全且有条理的方式管理云的采用。 一旦决定了特定应用程序，您就需要能够阻止对未经批准的应用程序的访问，以降低敏感数据丢失，帐户泄露和恶意软件感染的风险。



4：Cloud access security broker介绍（2）

Three key requirements
三大关键要求

Visibility
可视性
See the cloud services that are being accessed from your various networks and managed devices

查看正在从您的各种网络和受管设备访问的云服务

App and risk insight
应用程序和风险洞察
View details about each vendor and application including (business, usage, and compliance) risk elements

查看有关每个供应商和应用程序的详细信息，包括（业务，使用情况和合规性）风险要素

Optimization and blocking
优化和阻止
Ability to group apps by type, category, risk level, or number of requests to manage cloud adoption and help decide which apps to block. Automated blocking workflow to simplify administration

能够按类型，类别，风险级别或请求数量对应用程序进行分组，以管理云采用并帮助决定阻止哪些应用程序。自动阻止工作流程以简化管理

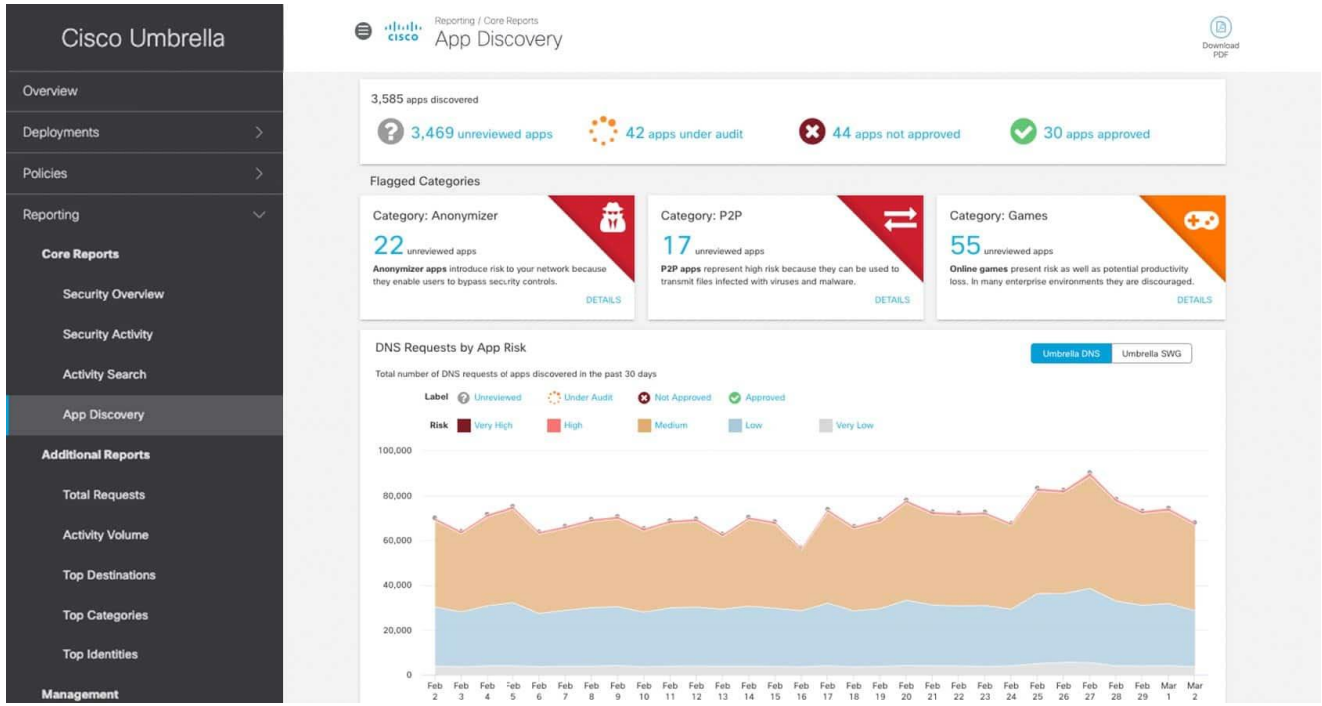
4：Cloud access security broker介绍（3）

App discovery and blocking 应用发现和阻止

Dashboard for visibility and trends
仪表板的可见性和趋势

The dashboard shows the level of cloud service activity and risk in your organization. It also provides a summary by app category that is sorted by risk level. This gives insight into potential policy and compliance violations if employees use a new cloud service instead of an approved app.

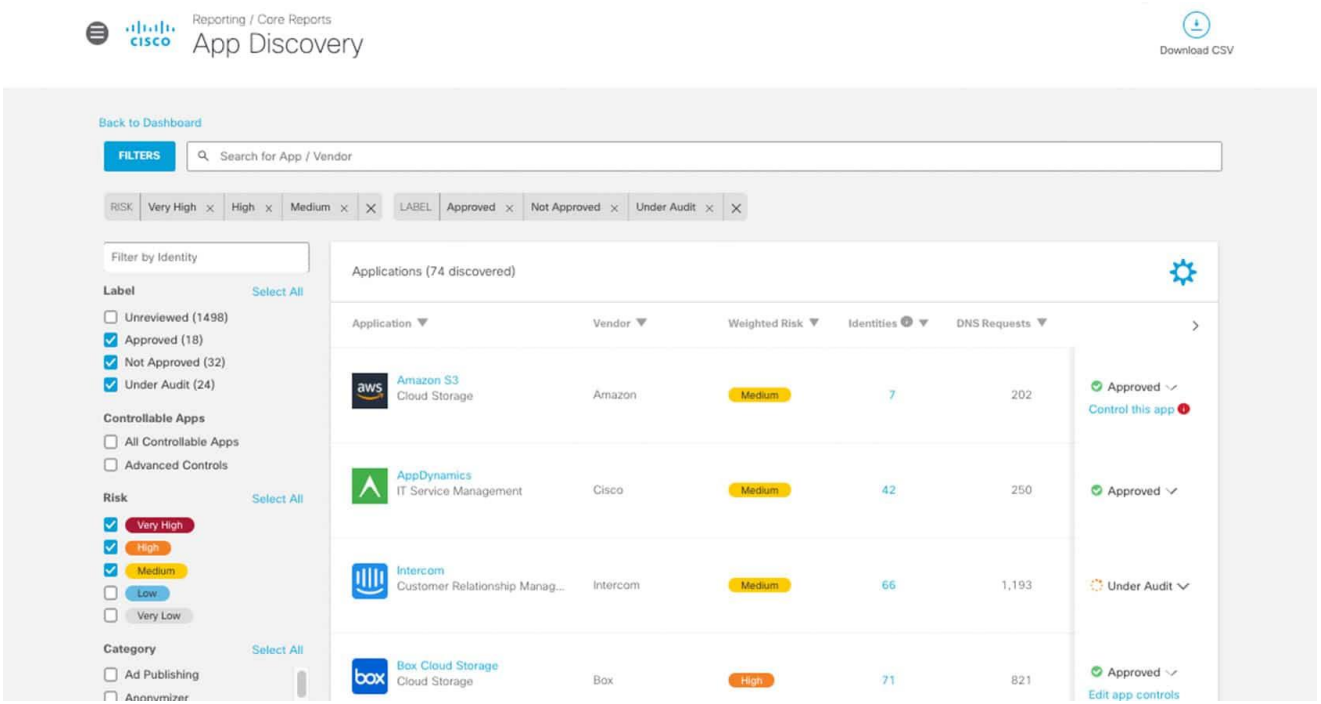
仪表板显示组织中云服务活动的级别和风险。它还提供了按应用类别的摘要，并按风险级别进行了排序。如果员工使用新的云服务而不是经过批准的应用程序，则可以深入了解潜在的策略和合规性违规行为。



4：Cloud access security broker介绍（4）

Application details 应用详情

Preset application-level reports provide a list of apps with each label: Unreviewed, Under Audit, Approved, and Not Approved. Easily apply filters to create custom views that help you understand and track use by category, usage, type, or status.
预设的应用程序级别报告提供了带有每个标签的应用程序列表：未审核，正在审核，已批准和未批准。轻松应用过滤器以创建自定义视图，以帮助您按类别，用途，类型或状态了解和跟踪用途

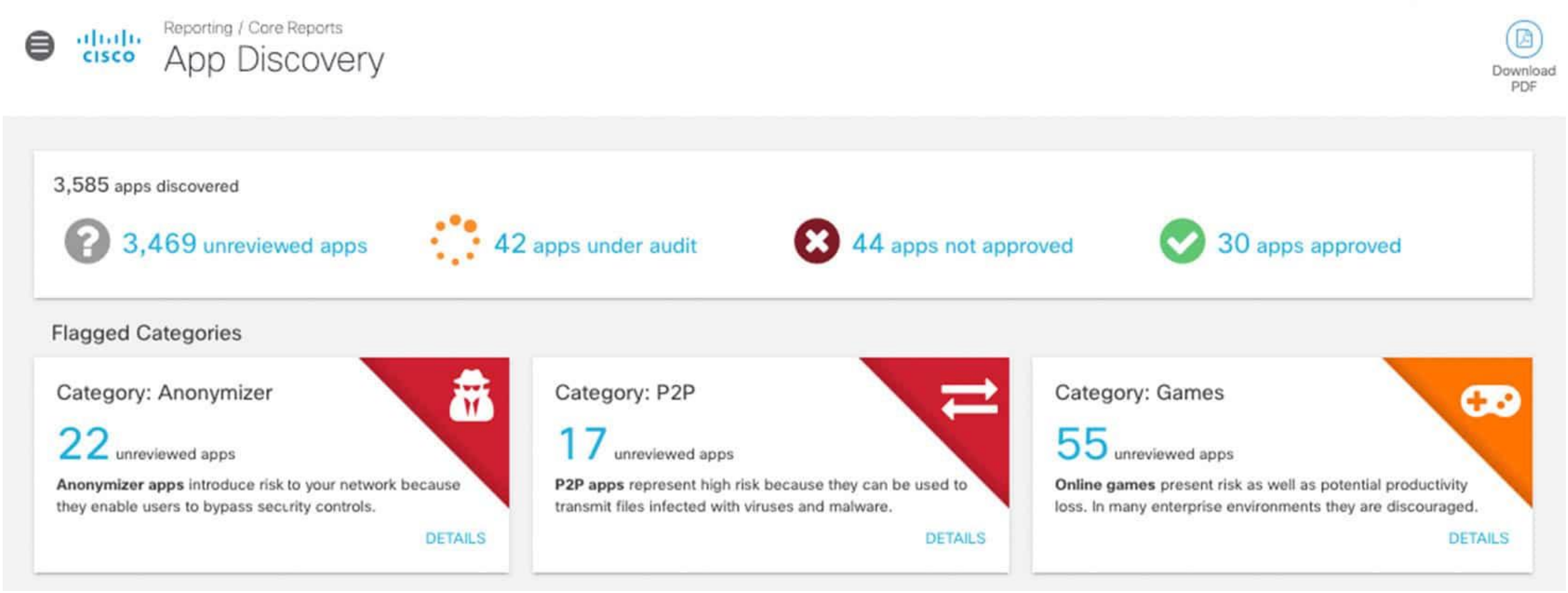


4：Cloud access security broker介绍（5）

Optimization 优化

Utilize the 30 application categories to organize the apps in use and filter by risk level or number of requests to understand your current exposure. Then make informed decisions about categories and assign the individual apps to the Approved, Under Audit, or Not Approved groups.

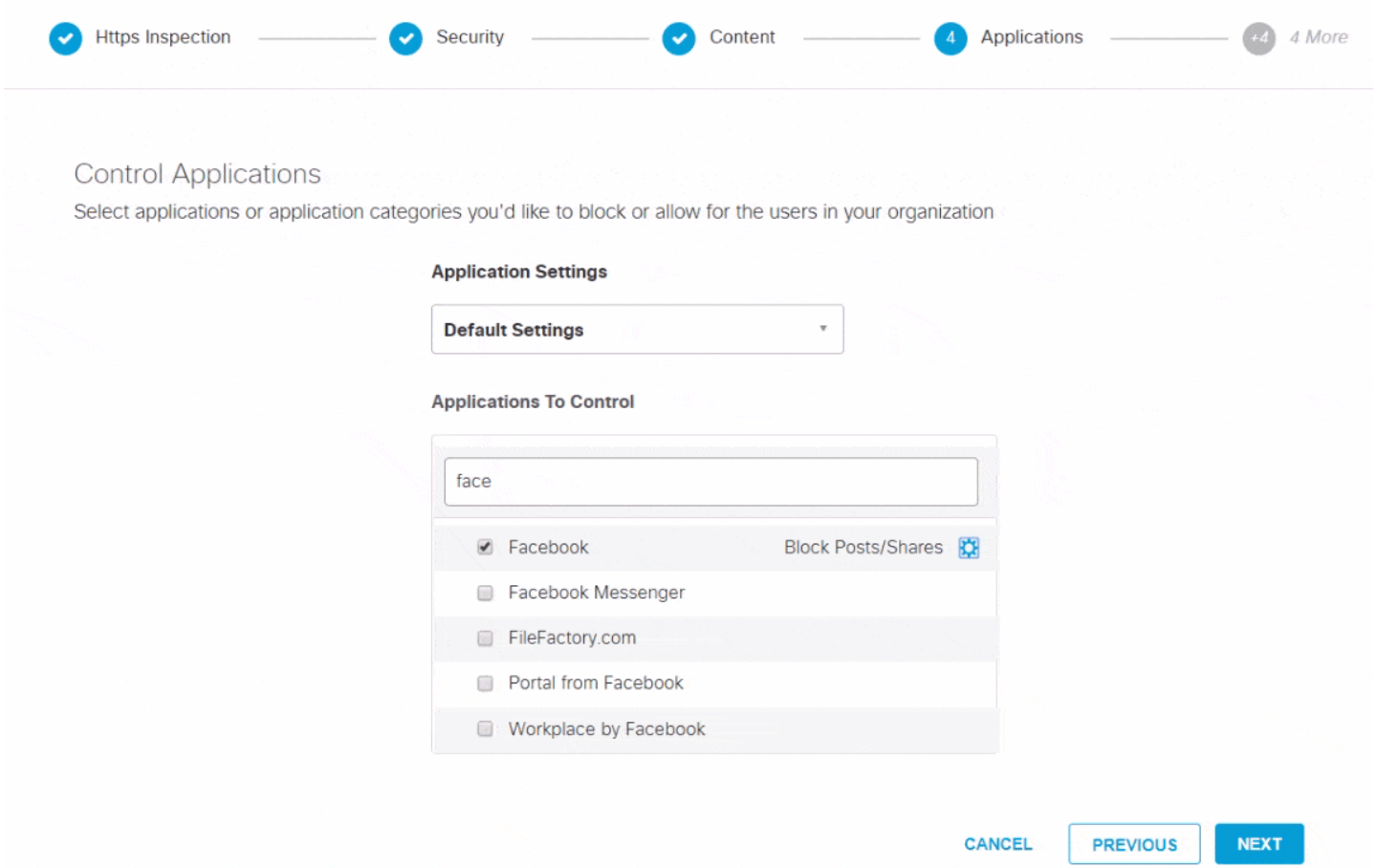
利用30种应用类别来组织使用中的应用，并按风险级别或请求数量进行过滤，以了解您当前的风险。然后，根据类别做出明智的决定，并将各个应用分配到“已批准”，“正在审核”或“未批准”组中



4：Cloud access security broker介绍（6）

Application blocking 应用程序阻止

Easily block the available apps by clicking on the link in the application listing or detail pages. Enforce this control for any network, group, or individual user accessible by Umbrella policies.
通过单击应用程序列表或详细信息页面中的链接轻松阻止可用的应用程序。对伞策略可访问的任何网络，组或个人用户强制执行此控制



5：Interactive threat intelligence介绍（1）

Cisco Umbrella Investigate umbrella调查

Umbrella Investigate gives the most complete view of the relationships and evolution of internet domains, IPs, and files — helping to pinpoint attackers' infrastructures and predict future threats. No other vendor offers the same level of interactive threat intelligence — exposing current and developing threats. Umbrella delivers the context you need for faster incident investigation and response.

Umbrella Investigate可以最全面地了解Internet域，IP和文件之间的关系和演变，从而帮助查明攻击者的基础设施并预测未来的威胁。没有其他供应商可以提供相同级别的交互式威胁情报，从而可以暴露当前和正在发展的威胁。伞为您提供了所需的上下文，以便更快地进行事件调查和响应。

5：Interactive threat intelligence介绍（2）

Investigate console 调查控制台

1. Risk score 风险评估

Access reliable threat scoring with rich visibility into what contributes to the score so you can triage faster.

获得可靠的威胁评分，并对导致评分的内容具有丰富的可见性，从而可以更快地进行分类

2. DNS request patterns DNS请求模式

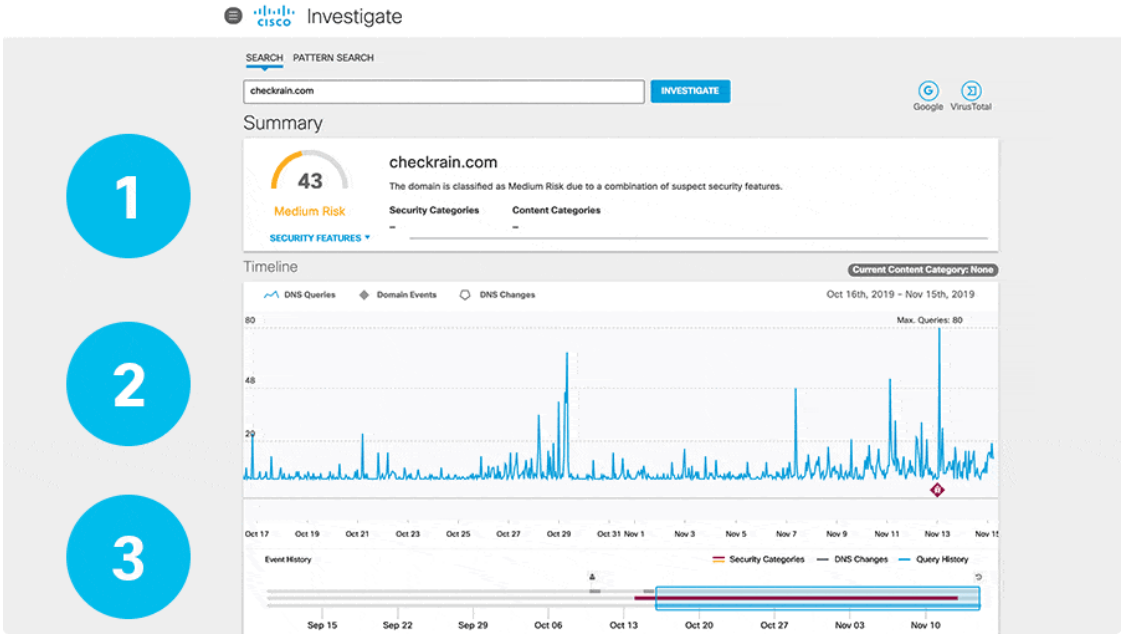
See up-to-the minute views of DNS requests to a particular domain. A sudden spike in traffic may indicate malicious activity.

查看对特定域的DNS请求的最新视图。流量突然激增可能表明存在恶意活动

3. Passive DNS 被动DNS

Get deeper context on the domain with a snapshot of key events and tagged security categories for the past 5 years.

通过过去5年的关键事件和标记的安全类别的快照在域上获得更深入的上下文



5：Interactive threat intelligence介绍（3）

The Investigate advantage 调查优势

Access our realtime threat intelligence to: 访问我们实时威胁情报

Proactively protect users
主动保护

Uncover attacker infrastructure and stop attacks before they launch

在攻击者发动攻击之前发现他们的基础架构并停止攻击

Better prioritize incidents
更好的确定事件的优先级

Identify what alerts need additional investigation

确定哪些警报需要进一步调查

Speed investigations
速度调查

Gain greater context for faster decision making and remediation

获得更大的环境，以便更快地做出决策和补救

5：Interactive threat intelligence介绍（4）

See attacks before they launch启动前查看攻击

We see the relationships between malware, domains, IPs, and networks across the internet. Similar to how Amazon learns from shopping patterns to suggest the next purchase, our threat analysis learns from internet activity patterns to automatically identify attacker infrastructure being staged for the next threat

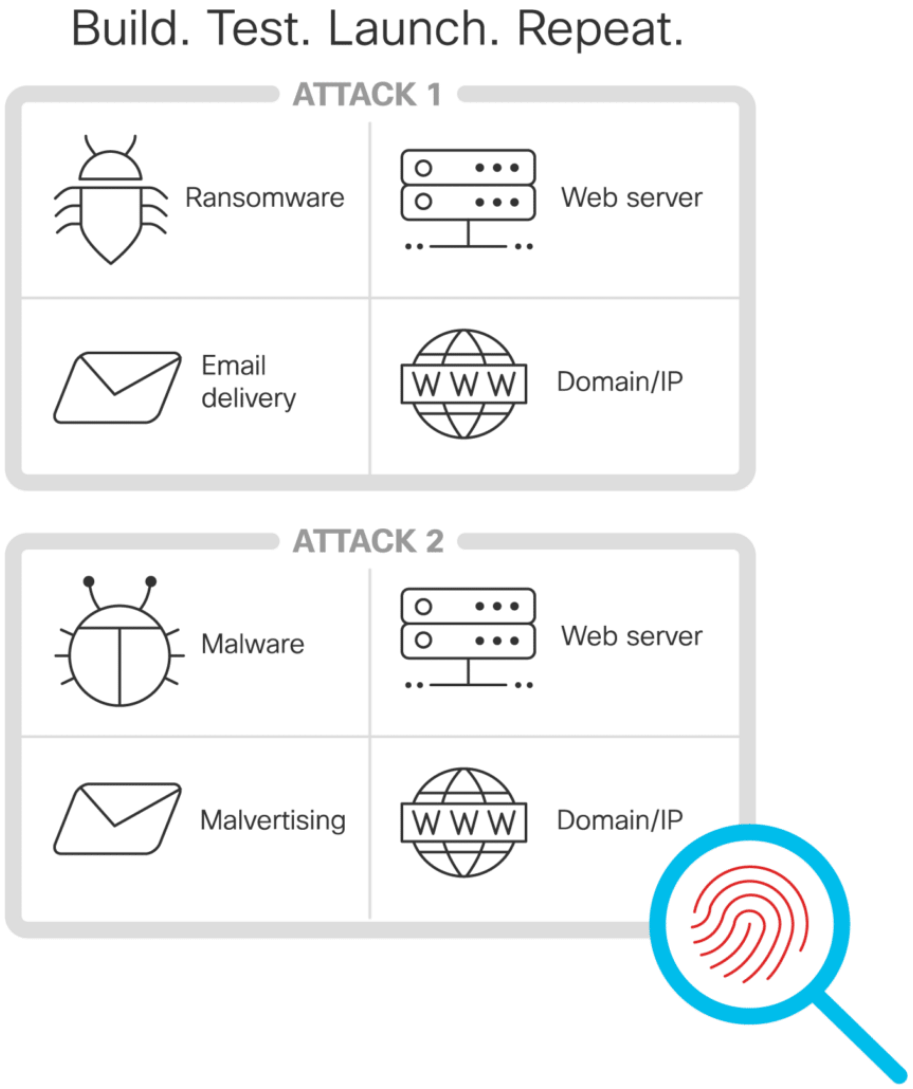
我们看到了Internet上恶意软件，域，IP和网络之间的关系。与亚马逊从购物模式中学习以建议下一次购买的方式类似，我们的威胁分析从互联网活动模式中学习以自动识别针对下一个威胁而准备的攻击者基础设施

5：Interactive threat intelligence介绍（5）

Attacks don't just suddenly happen攻击不只是突然发生

The development lifecycle to create new attacks is similar to that of new applications. An app developer builds something, tests it, and then launches it. Attackers do the same, which requires infrastructure, malware, and a web or email delivery scheme. While they modify and create new malware (e.g. ransomware variants) and draft new phishing emails, attackers often reuse the exact same infrastructure (e.g. web servers and IPs) for multiple attacks — leaving behind cyber fingerprints. We focus our cyber threat analysis on identifying those fingerprints, so we can pinpoint current attacks and even uncover emerging threats being staged.

创建新攻击的开发生命周期与新应用程序相似。应用程序开发人员会构建，测试并启动它。攻击者也是如此，这需要基础结构，恶意软件以及Web或电子邮件传递方案。在攻击者修改和创建新的恶意软件（例如勒索软件变种）并起草新的网络钓鱼电子邮件的同时，攻击者经常将完全相同的基础架构（例如Web服务器和IP）重用于多次攻击，从而留下了网络指纹。我们将网络威胁分析的重点放在识别那些指纹上，因此我们可以查明当前的攻击甚至发现正在上演的新兴威胁

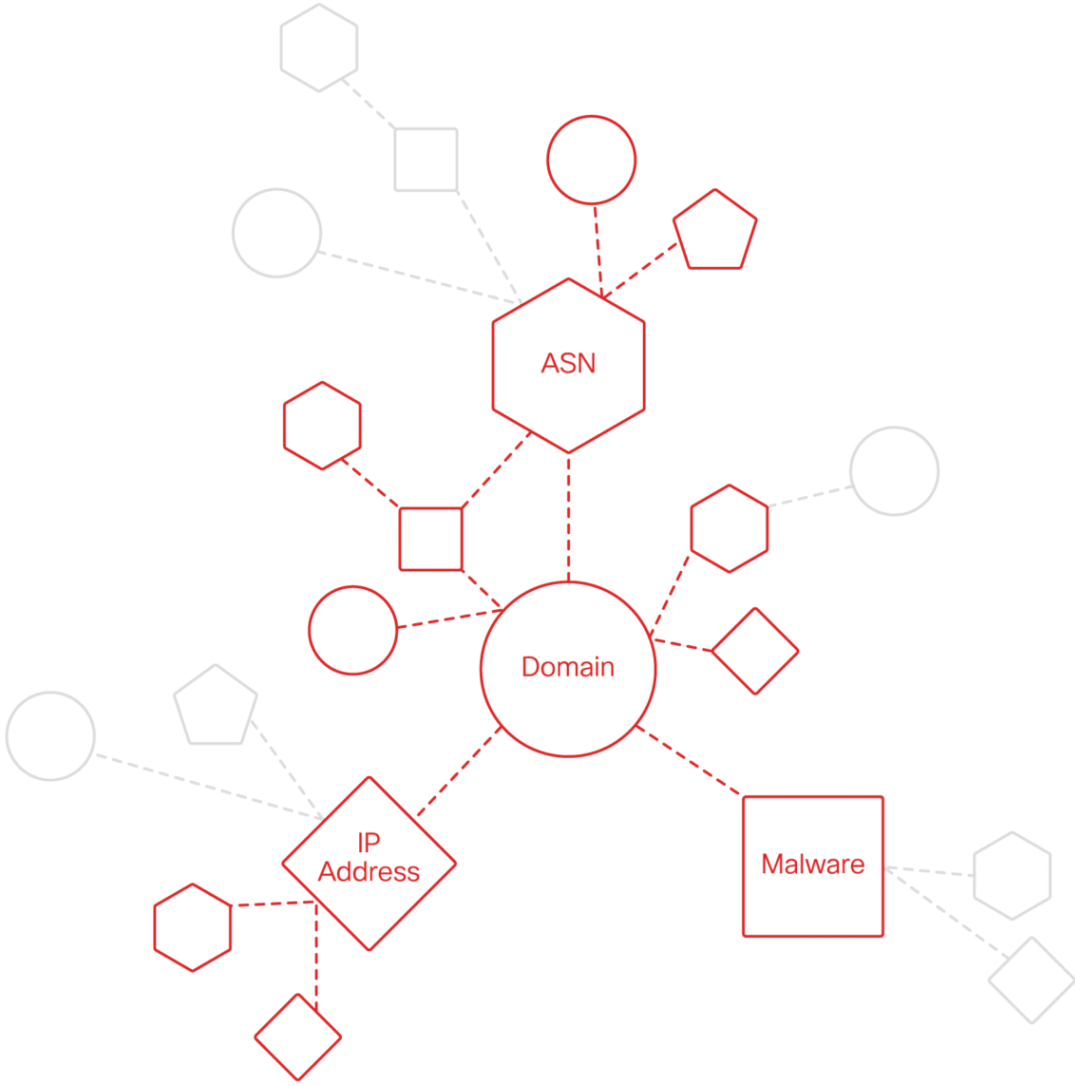


5：Interactive threat intelligence介绍（6）

Statistical models are our secret sauce 统计模型是我们的秘诀

We statistically score the “guilt” of domains and IPs to determine if they’re part of an attacker’s infrastructure. More than a reputation score that looks at the past, we analyze both historic and live data. And we’ve built statistical models to automatically score and classify all of our data, so we can detect anomalies, and uncover known and emergent threats. We use three main approaches: guilt by inference, guilt by association, and patterns of guilt.

我们对域和IP的“有罪感”进行统计评分，以确定它们是否属于攻击者基础架构的一部分。我们不仅分析过去的声誉得分，还分析历史数据和实时数据。我们已经建立了统计模型来自动对所有数据进行评分和分类，因此我们可以检测异常，并发现已知和紧急威胁。我们使用三种主要方法：因推理而感到内,、因联想而感到内gui以及有罪的模式



5：Interactive threat intelligence介绍（7）

Datasets must be diverse, global, and live

数据集必须是多样化的，全球的，实时的

620B

Daily internet requests

每日互联网请求

100M

Daily active users

每日活跃用户

190

Countries worldwide

世界各国

Leveraging threat intelligence from Cisco Talos, one of the largest commercial threat intelligence teams in the world, Umbrella uncovers and blocks a broad spectrum of malicious domains, IPs, URLs, and files that are being used in attacks.

Umbrella gathers 620 billion internet requests from over 100 million enterprise and consumer users across 190 countries every day at the moment a request is made. Our real-time DNS data is also enriched with diverse public and private data feeds. With such a massive and diverse data set, our threat analysis can uncover patterns that signal malicious behavior.

利用来自全球最大的商业威胁情报团队之一的Cisco Talos的威胁情报，Umbrella可以发现并阻止攻击中使用的各种恶意域，IP，URL和文件。

提出请求时，每天，Umbrella收集来自190个国家/地区的1亿多家企业和消费者用户的6,200亿个Internet请求。我们的实时DNS数据还丰富了各种公共和私人数据源。拥有如此庞大且多样化的数据集，我们的威胁分析可以发现表明恶意行为的模式

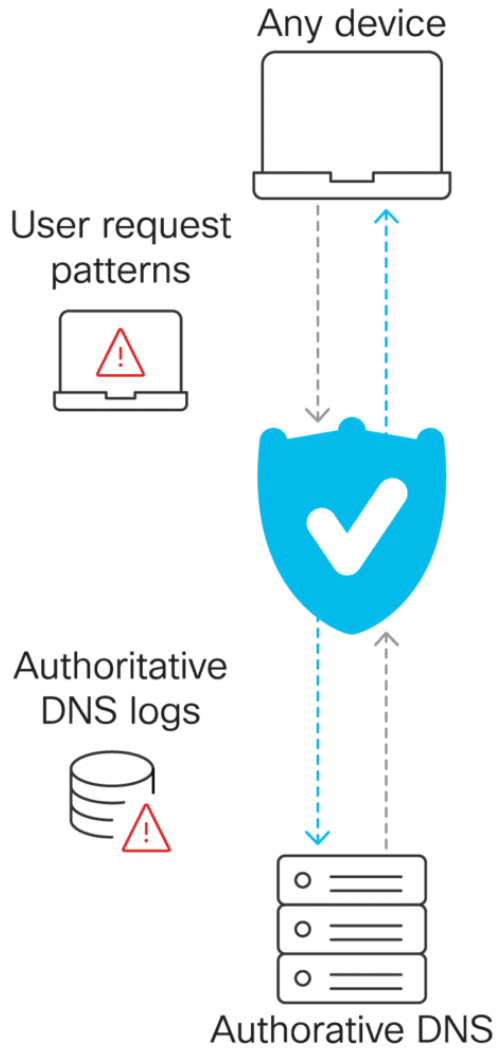
5：Interactive threat intelligence介绍（8）

Making discoveries through DNS resolution 通过DNS解析进行发现

We analyze the request patterns to detect many types of threats and anomalies. For example, we can determine if a system is compromised based on the types of requests it's making. If a device is making requests to a number of known-bad domains, it's more likely to be compromised. The user requests patterns across our user base give us great insight into potential threats.
In the second part of the process, if our global cache doesn't have a non-expired response to the request, then we recursively contact all of the nameservers that are authoritative for the domain requested. This process gathers authoritative logs for virtually every domain daily, which we use to find newly staged infrastructures and other types of anomalies.

我们分析请求模式以检测多种类型的威胁和异常。例如，我们可以根据发出的请求的类型来确定系统是否受到威胁。如果设备向多个已知的坏域发出请求，则很有可能会受到威胁。用户在我们整个用户群中的请求模式使我们能够深入了解潜在威胁。

在该过程的第二部分中，如果我们的全局缓存没有对请求的未过期响应，则我们将递归联系所有对所请求域具有权威性的名称服务器。此过程几乎每天收集每个域的权威日志，我们用它们来查找新近上演的基础架构和其他类型的异常情况。



5：Interactive threat intelligence介绍（9）

Efficacy is king
功效为王

Deploy enterprise-wide in less than 30 minutes

不到30分钟即可在企业范围内部署

Process and enforce 7M malicious domains and IPs

处理和执行7M恶意域和IP

Identify 60K+ new malicious destinations daily

每天识别6万多个新的恶意目的地

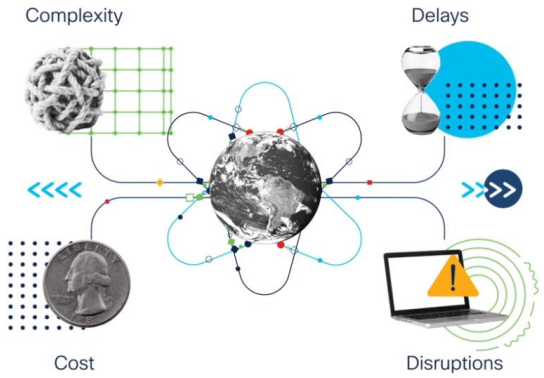
Threat intelligence is one thing, but you also need to act on all of that data. Cisco Umbrella has the horsepower to actively process and enforce more than 7 million unique malicious domains and IPs concurrently at the DNS layer – appliances and hybrid-cloud solutions can't come close to enforcing that many threats at once. And we're constantly adding to our block list – 60,000+ new destinations are added every day. Plus, Umbrella can be deployed enterprise-wide in minutes – making it one of the easiest ways to start protecting users.

威胁情报是一回事，但您还需要对所有这些数据采取行动。Cisco Umbrella具有在DNS层上同时主动处理和实施超过700万个独特恶意域和IP的能力-设备和混合云解决方案几乎无法立即实施这么多威胁。而且我们会不断添加到阻止列表中-每天添加60,000多个新目的地。此外，Umbrella可以在几分钟内在企业范围内部署-使其成为开始保护用户的最简单方法之一

6：Integration with SD-WAN介绍（1）

Simple cloud security across distributed networks 跨分布式网络的简单云安全

Cisco SD-WAN
Cloud-delivered WAN architecture for secure multi-cloud transformation.
云交付的WAN架构，可实现安全的多云转换



6：Integration with SD-WAN介绍（1）

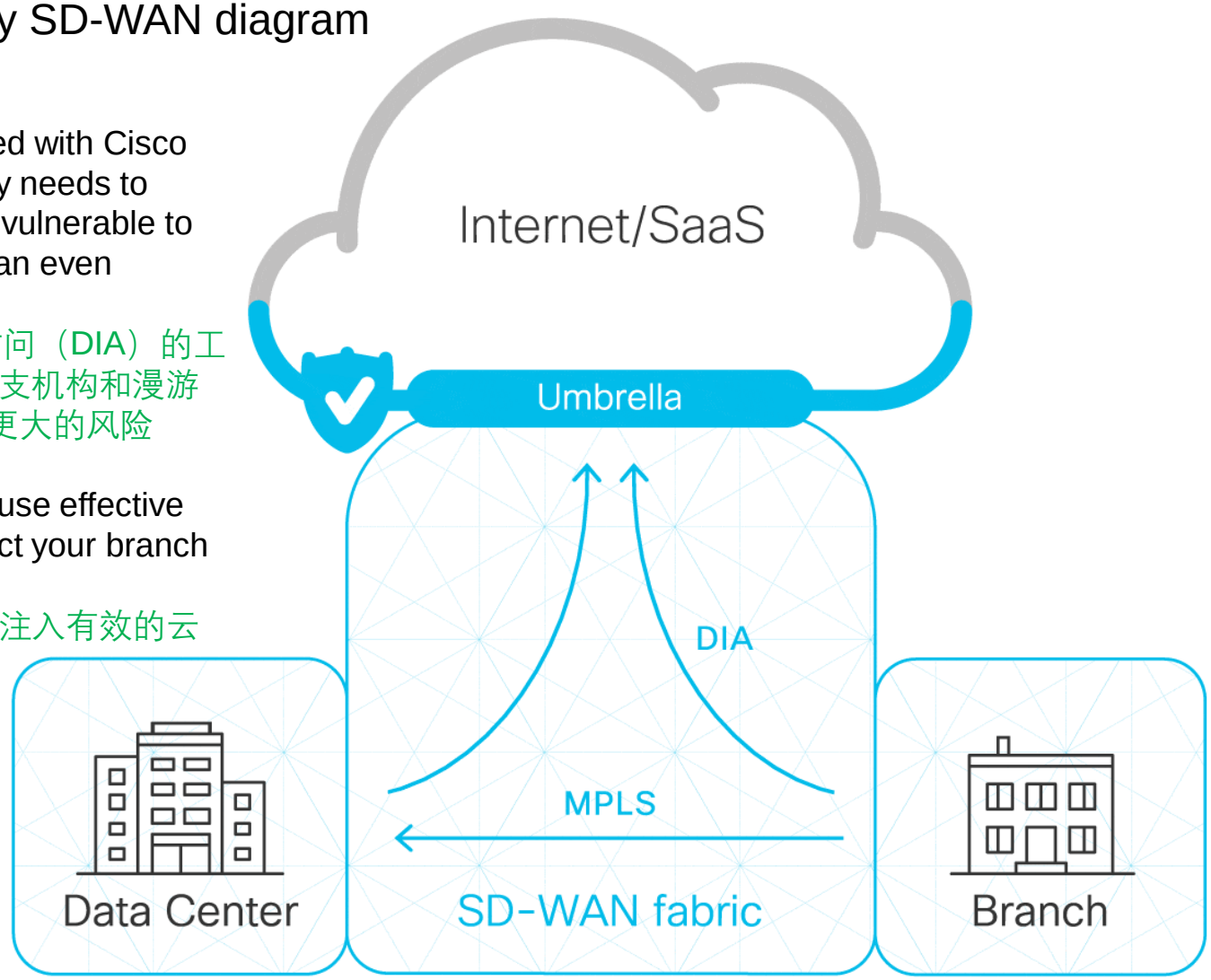
Fast forward time to value with automated security SD-WAN diagram
通过自动安全性快速实现价值

Enabling direct internet access (DIA) from the branch is simplified with Cisco SD-WAN technology. As organizations shift to SD-WAN, security needs to remain top of mind. Branch offices and roaming users are more vulnerable to attacks, and as organizations move to more DIA, this becomes an even greater risk.

借助Cisco SD-WAN技术，简化了从分支机构启用直接Internet访问（DIA）的工作。随着组织转向SD-WAN，安全性仍然是首要考虑的问题。分支机构和漫游用户更容易受到攻击，并且随着组织迁移到更多DIA，这将带来更大的风险

The Cisco SD-WAN and Umbrella integration enables you to infuse effective cloud security throughout your SD-WAN fabric so you can protect your branch offices and roaming users

思科SD-WAN和Umbrella的集成使您可以在整个SD-WAN结构中注入有效的云安全性，从而可以保护分支机构和漫游用户



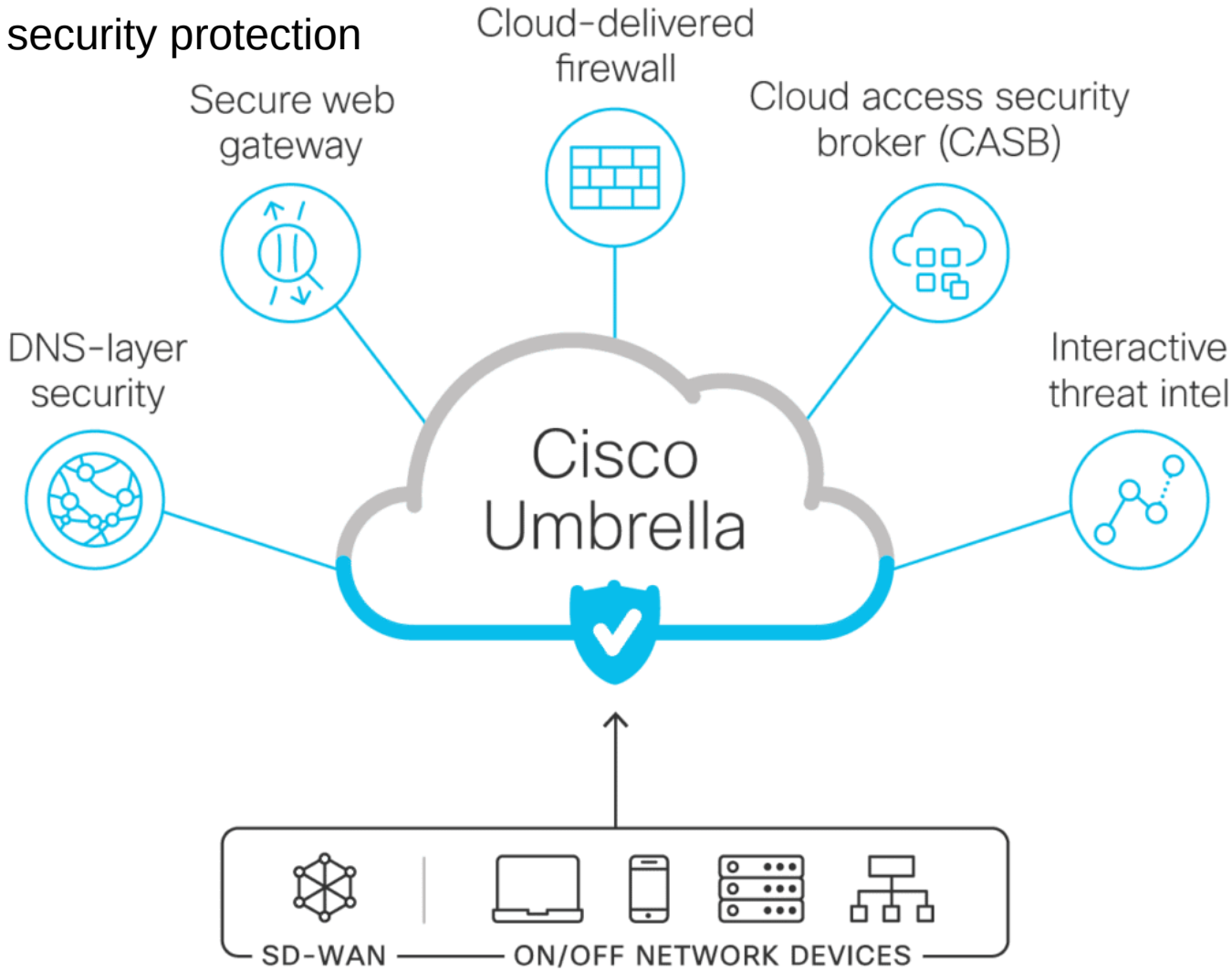
6：Integration with SD-WAN介绍（1）

Secure direct internet access locations with the best security protection
通过最佳的安全保护来保护直接访问Internet的位置

Umbrella unifies multiple security capabilities in a single cloud-delivered service for powerful, integrated protection that is easy to deploy and simple to manage. Umbrella extends protection to devices, remote users, and distributed locations anywhere.
Umbrella在单个云交付服务中统一了多种安全功能，以提供易于部署和管理的强大集成保护。伞将保护扩展到了设备，远程用户和任何地方的分布式位置

You can deploy cloud security across your SD-WAN fabric to thousands of branches in minutes, and instantly gain protection against threats on the internet. Powered by Umbrella's global network and Cisco Talos threat intelligence, it's the easiest way to deliver protection to users anywhere they access the internet and cloud apps. With simple automated tunnel creation from Cisco SD-WAN combined with Umbrella's secure web gateway and cloud-delivered firewall, you gain additional flexibility and more granular security controls.

您可以在几分钟内跨SD-WAN结构将云安全性部署到数千个分支机构，并立即获得针对Internet威胁的保护。在Umbrella的全球网络和Cisco Talos威胁情报的支持下，这是向用户访问Internet和云应用程序的任何地方提供保护的最简单方法。通过从Cisco SD-WAN进行简单的自动隧道创建，再加上Umbrella的安全Web网关和云交付的防火墙，您将获得更多的灵活性和更精细的安全控制



6：Integration with SD-WAN介绍（1）

The Cisco Advantage

As a leader in both networking and security, only Cisco can deliver an automated secure SD-WAN experience that is integrated into our network solutions.

Key benefits of Cisco Secure SD-WAN: 优势:

- **Easy to consume:** Simple ordering with Cisco SD-WAN and Cisco Umbrella bundled into one offer.
  易于使用：捆绑到一个产品中的Cisco SD-WAN和Cisco Umbrella即可轻松订购。
- **Fast to deploy:** With our automated provisioning and tunnel creation you can easily protect your branch offices and users in minutes, not months, from within the Cisco SD-WAN console.
  部署迅速：通过我们的自动配置和隧道创建，您可以在几分钟（而不是几个月）内从Cisco SD-WAN控制台轻松保护分支机构和用户。
- **Best security protection:** New AV-TEST research places Umbrella first in security efficacy. Umbrella's real-time threat intelligence is derived from a massive set of global internet activity and Cisco Talos threat intelligence.
  最佳安全保护：最新的AV-TEST研究将伞的安全功效放在首位。 Umbrella的实时威胁情报来自大量的全球互联网活动和Cisco Talos威胁情报。

6：Integration with SD-WAN介绍（1）

Integration features

Feature	Why it matters
Auto-provisioning 自动配置	Reduce the time it takes to set-up protection for your branch offices by automatically connecting the Cisco Umbrella Dashboard to vManage via Smart Accounts 通过自动通过智能帐户将Cisco Umbrella仪表板连接vManage，减少为分支机构设置保护所需的时间
Auto-tunneling 自动隧道	Simplify management and provision thousands of sites to Cisco Umbrella in minutes with a few clicks 只需单击几下，即可在几分钟内简化管理并向Cisco Umbrella提供数千个站点
Automatically generate unique credentials for each tunnel 自动为每个隧道生成唯一的凭据	Added security: a single compromised router doesn't require all tunnels to be rekeyed 增强的安全性：单个受损的路由器不需要重新设置所有隧道的密钥
Automatic best path selection to the nearest data center 自动选择最佳路径到最近的数据中心	Remove added complexity by automatically selecting the closest low latency data center from Umbrella's global infrastructure 通过自动从Umbrella的全球基础架构中选择最接近的低延迟数据中心来消除增加的复杂性
Redundancy is built into Cisco Umbrella's global infastructure 冗余已内置在Cisco Umbrella的全球基础架构中	Improve internet performance with Umbrella's highly resilient network. Intra and inter datacenter failover is automatic via patent-pending hybrid Anycast 利用Umbrella的高弹性网络提高互联网性能。 内部和内部数据中心故障转移通过正在申请专利的混合Anycast自动进行

6：Integration with SD-WAN介绍（1）

AV-TEST places Cisco Umbrella first in secure web gateway to protect remote workers
AV-TEST将Cisco Umbrella置于安全Web网关的首位，以保护远程工作者

AV-TEST places Cisco Umbrella, the heart of Cisco's SASE architecture, first in security efficacy in a recent test. Cisco Umbrella is a cloud-native security service that simplifies network security by helping you secure internet access and control cloud application usage across your network, branch offices, and roaming users. Umbrella unifies DNS-layer security, secure web gateway, firewall, and cloud access security broker (CASB) functionality. Umbrella integrated with Cisco AnyConnect provides secure endpoint access to the network so employees can work from any device, at any time, in any location.

最近的一项测试中，AV-TEST将Cisco Sum架构的核心Cisco Umbrella置于安全功效的第一位。Cisco Umbrella是一项云原生安全服务，可通过帮助您保护Internet访问并控制整个网络，分支机构和漫游用户的云应用使用来简化网络安全。umbrella统一了DNS层安全性，安全的Web网关，防火墙和云访问安全代理（CASB）功能。与Cisco AnyConnect集成的伞 提供了对网络的安全端点访问，因此员工可以随时随地在任何设备上使用任何设备进行工作

> *Umbrella received top marks across the board, with a whopping 96.39% total detection rate, crushing the competition.*

6：Integration with SD-WAN介绍（1）

Umbrella places first in 2020 cloud security efficacy test umbrella在2020年云安全功效测试中排名第一

In September and October 2020, AV-TEST performed a review of Cisco Umbrella's secure web gateway and DNS-layer security functionality, alongside comparable offerings from Akamai, Infoblox, Palo Alto Networks, Netskope, and Zscaler. The test was commissioned by Cisco to determine how well vendors protected remote and roaming workers against malware, phishing sites, and malicious websites. AV-TEST also carried out a false positive test against known clean popular websites and downloads from Alexa's top list.

2020年9月和2020年10月，AV-TEST对Cisco Umbrella的安全Web网关和DNS层安全功能以及Akamai，Infoblox，Palo Alto Networks，Netskope和Zscaler的同类产品进行了审查。该测试是由思科委托进行的，目的是确定供应商如何保护远程和漫游工作者免受恶意软件，网络钓鱼站点和恶意网站的侵害。AV-TEST还对已知的干净流行网站和Alexa最高列表中的下载进行了误报测试。

6：Integration with SD-WAN介绍（1）

Secure Web Gateway Test

A secure web gateway is based on a full web proxy that sees and inspects all web connections. Unlike DNS-layer protection which only analyzes domain names and IP addresses, a web proxy sees all files and the full URLs enabling more granular inspection and control. For secure web gateway testing, the products achieved the following blocking and false positive rates (ordered by best detection rate):

安全的Web网关基于完整的Web代理，该代理可查看和检查所有Web连接。与仅分析域名和IP地址的DNS层保护不同，Web代理可以查看所有文件和完整URL，从而可以进行更精细的检查和控制。对于安全的Web网关测试，这些产品达到了以下阻止和误报率（按最佳检测率排序）：

Product	Package	Detection rate	False positive rate
Number of test cases		3,572	2,165
Cisco Umbrella	SIG Essentials	96.39%	0.65%
Zscaler Internet Access	Transformation	89.67%	0.69%
Palo Alto Networks Prisma Access	Prisma Access for Mobile Users	73.15%	1.29%
Netskope Secure Web Gateway	NG-SWG	61.90%	4.53%
Akamai Enterprise Threat Protector	Advanced Threat	58.43%	1.89%

6：Integration with SD-WAN介绍（1）

DNS-Layer Protection Test

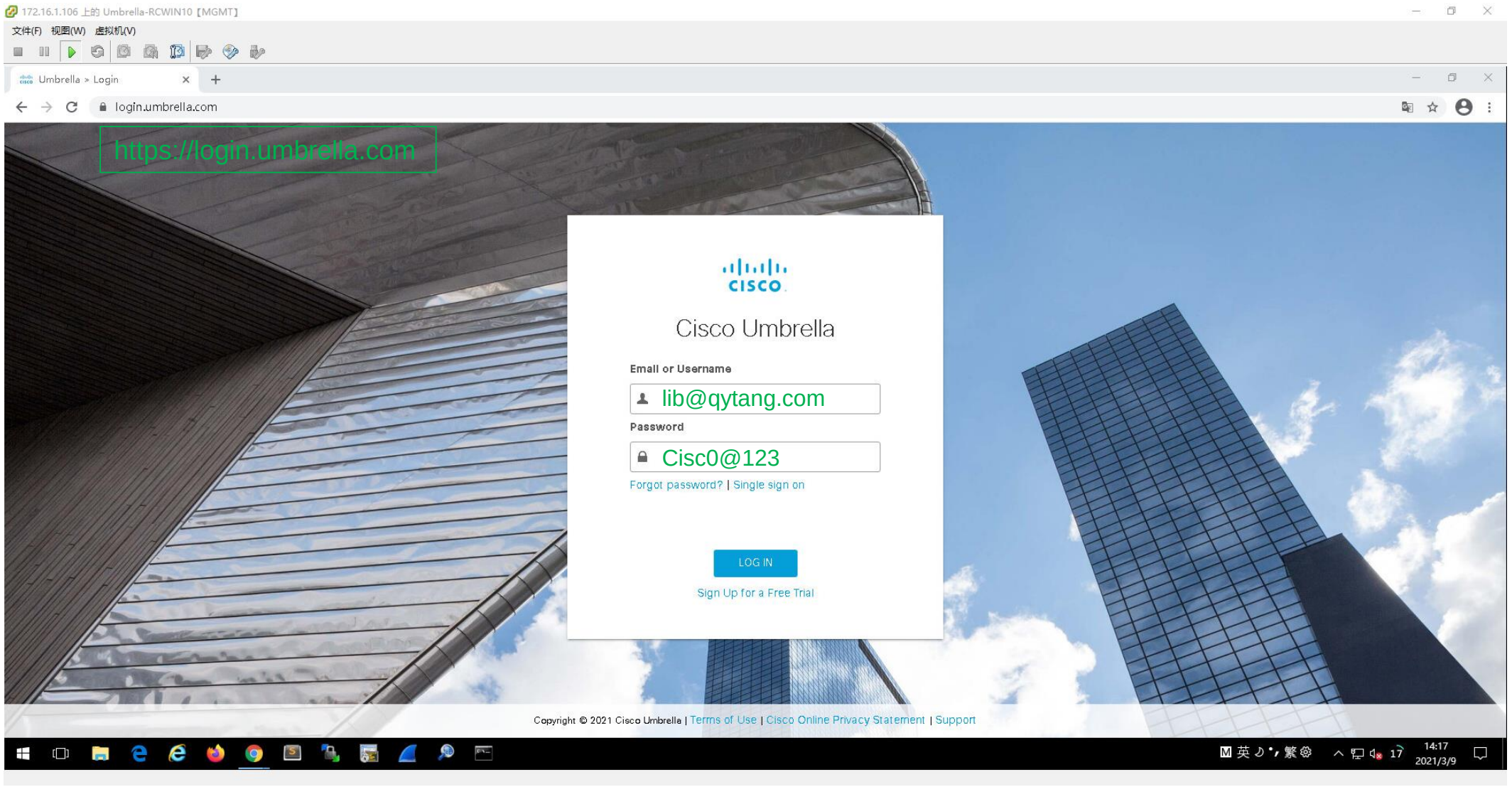
DNS-layer protection uses the internet's infrastructure to block malicious and unwanted domains, IP addresses, and cloud applications before a connection is ever established as part of recursive DNS resolution. DNS-layer protection stops malware earlier and prevents callbacks to attackers if infected machines connect to your network. DNS-layer protection with selective cloud proxy redirects only risky domain requests for deeper inspection of their web content, and does so transparently through the DNS response. For the DNS-layer protection testing, the products achieved the following blocking and false positive rates (ordered by best detection rate):

DNS层保护使用Internet的基础结构来阻止恶意和不需要的域，IP地址和云应用程序，然后再将其建立为递归DNS解析的一部分。DNS层保护可以更早地阻止恶意软件，并在受感染的计算机连接到您的网络时阻止向攻击者的回调。带有选择性云代理的DNS层保护仅重定向有风险的域请求以更深入地检查其Web内容，并通过DNS响应透明地进行。对于DNS层保护测试，这些产品达到了以下阻止和误报率（按最佳检测率排序）：

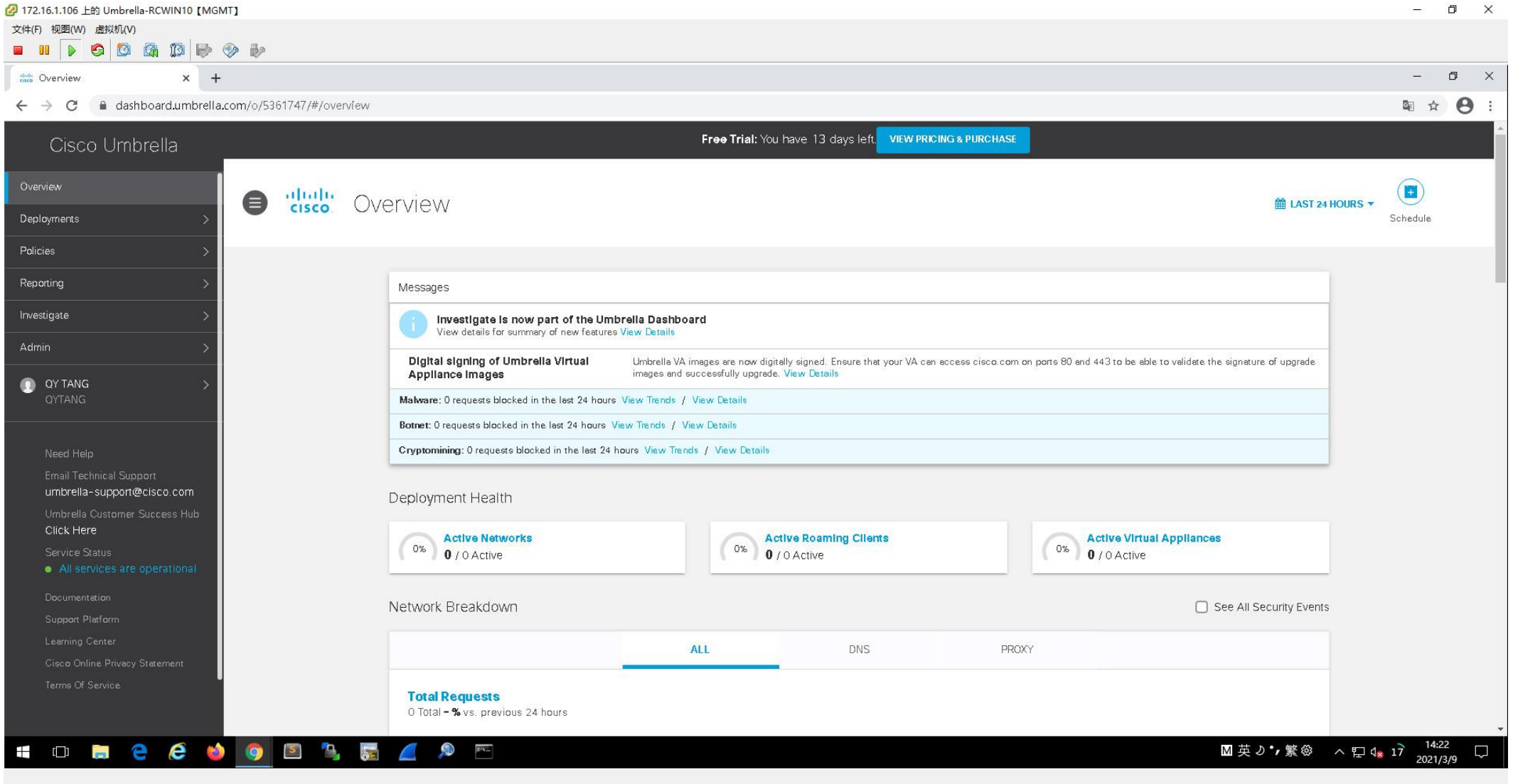
Product	Package	Detection rate	False positive rate
Number of test cases		3,572	2,165
Cisco Umbrella	DNS Security Advantage	70.69%	0.28%
Akamai Enterprise Threat Protector	Intelligence	53.58%	1.34%
Infoblox BloxOne	Advanced	36.28%	11.78%

2. Cisco Umbrella部署

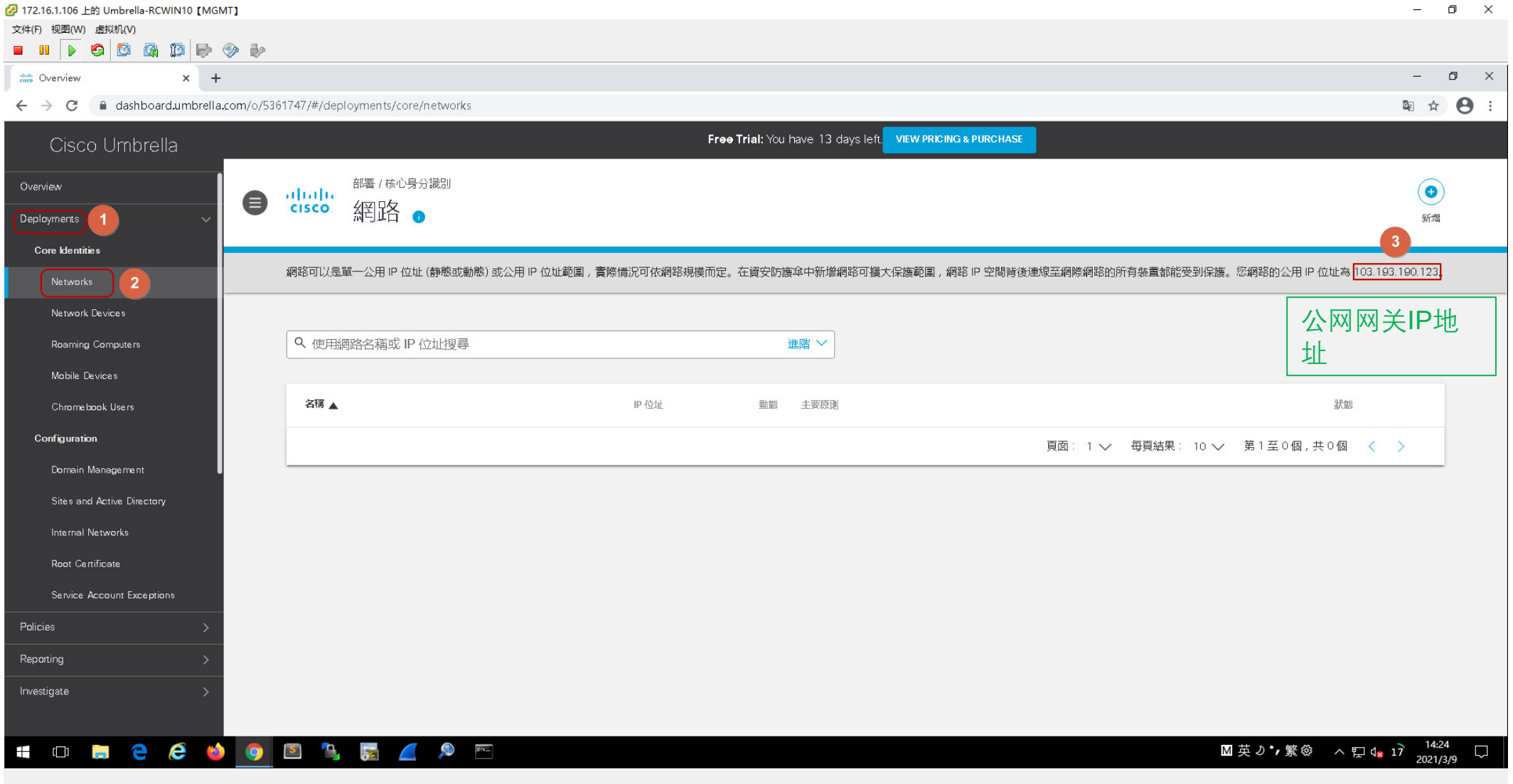
Cisco Umbrella部署（1）



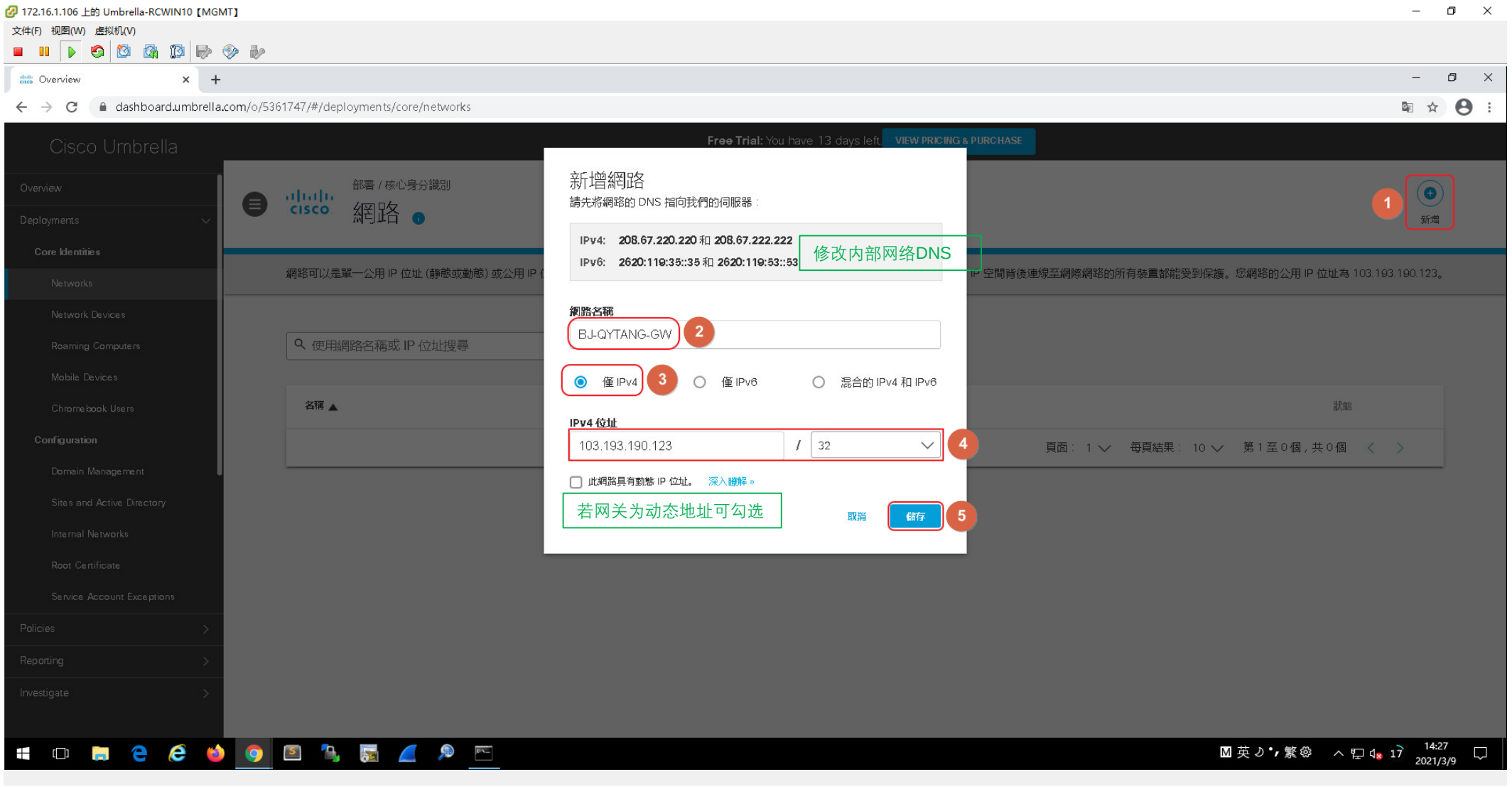
Cisco Umbrella部署（2）



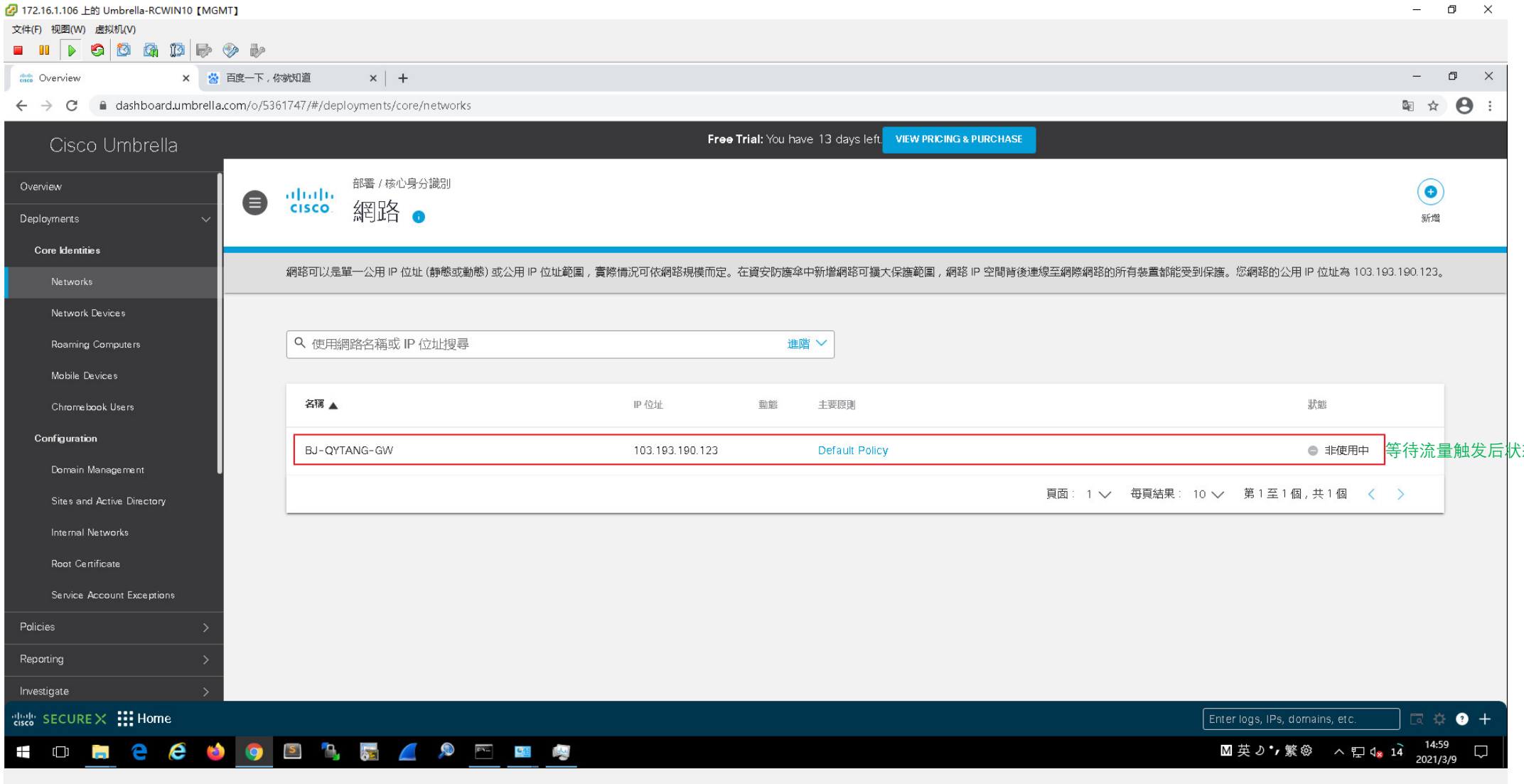
Cisco Umbrella部署（3）



Cisco Umbrella部署（4）

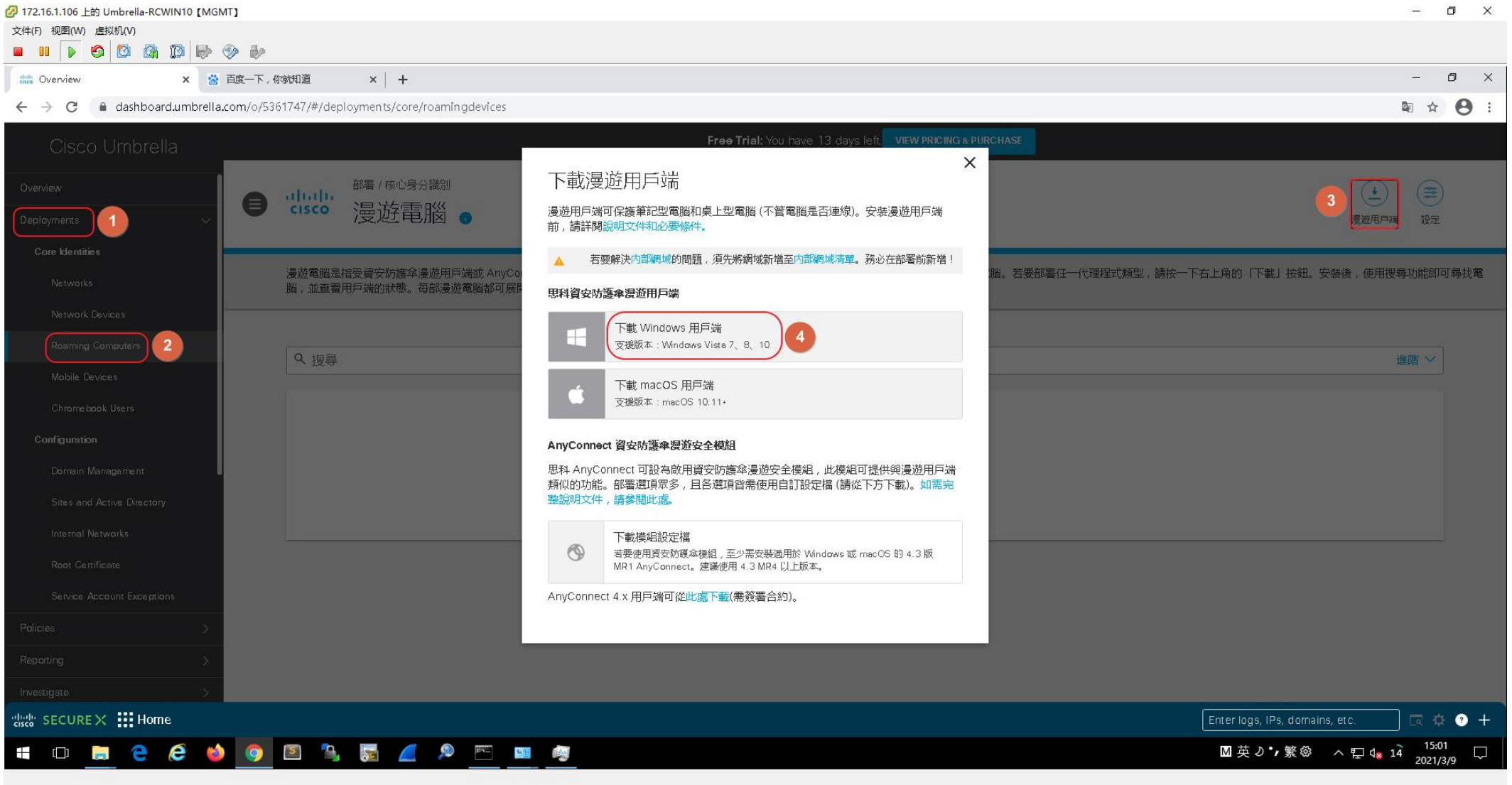


Cisco Umbrella部署（5）

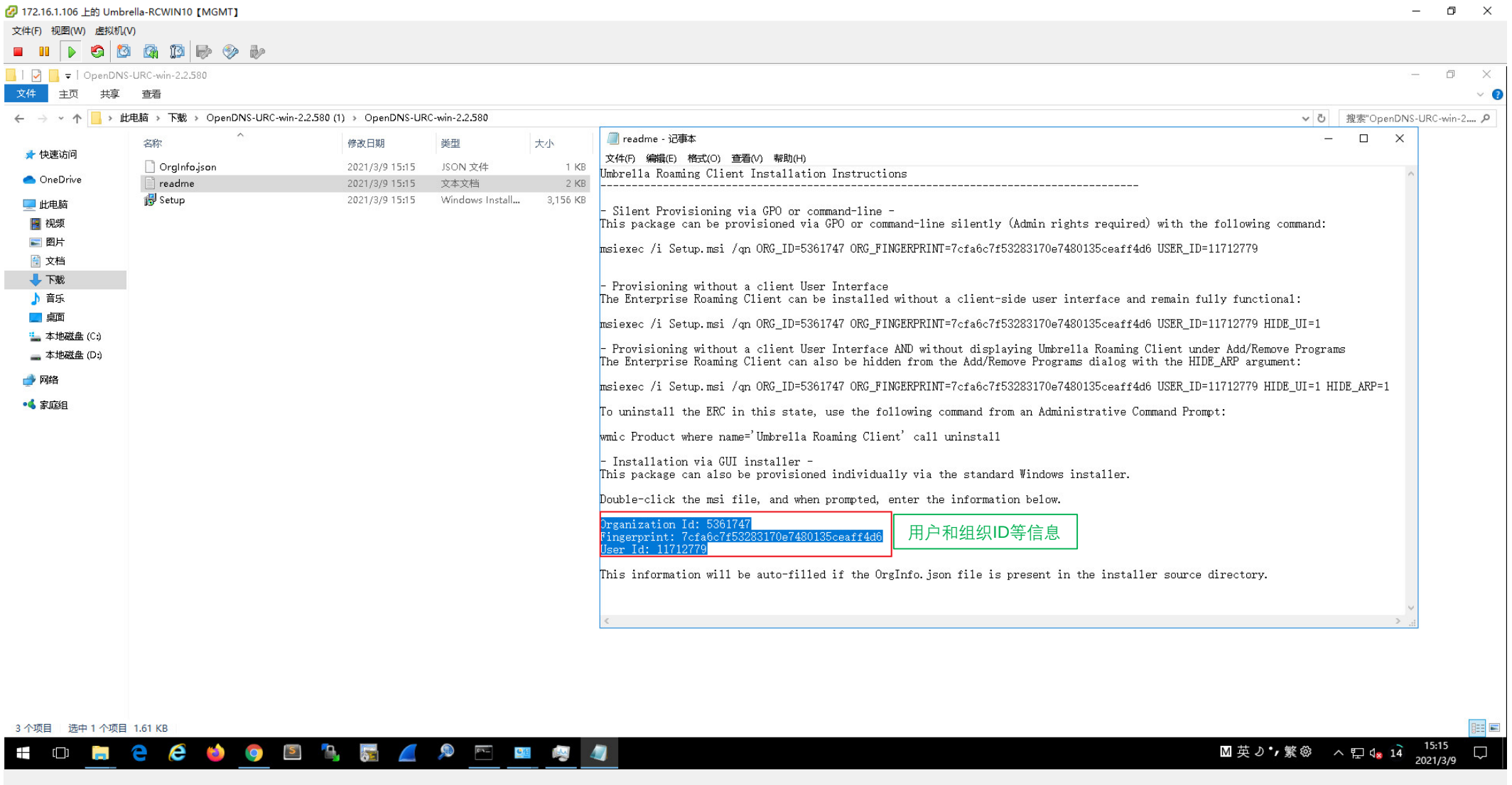


等待流量触发后状态：使用中

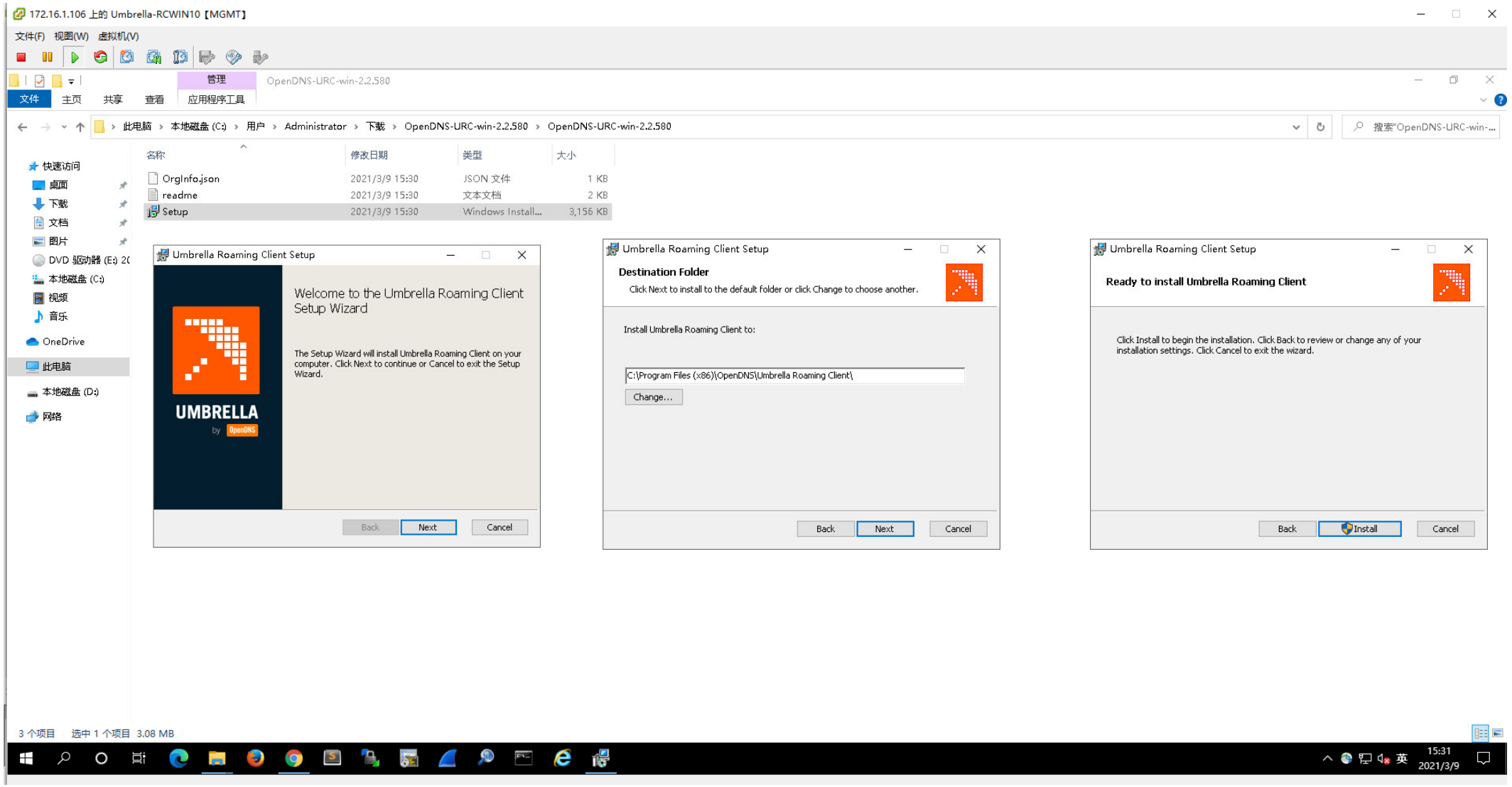
Cisco Umbrella部署（6）



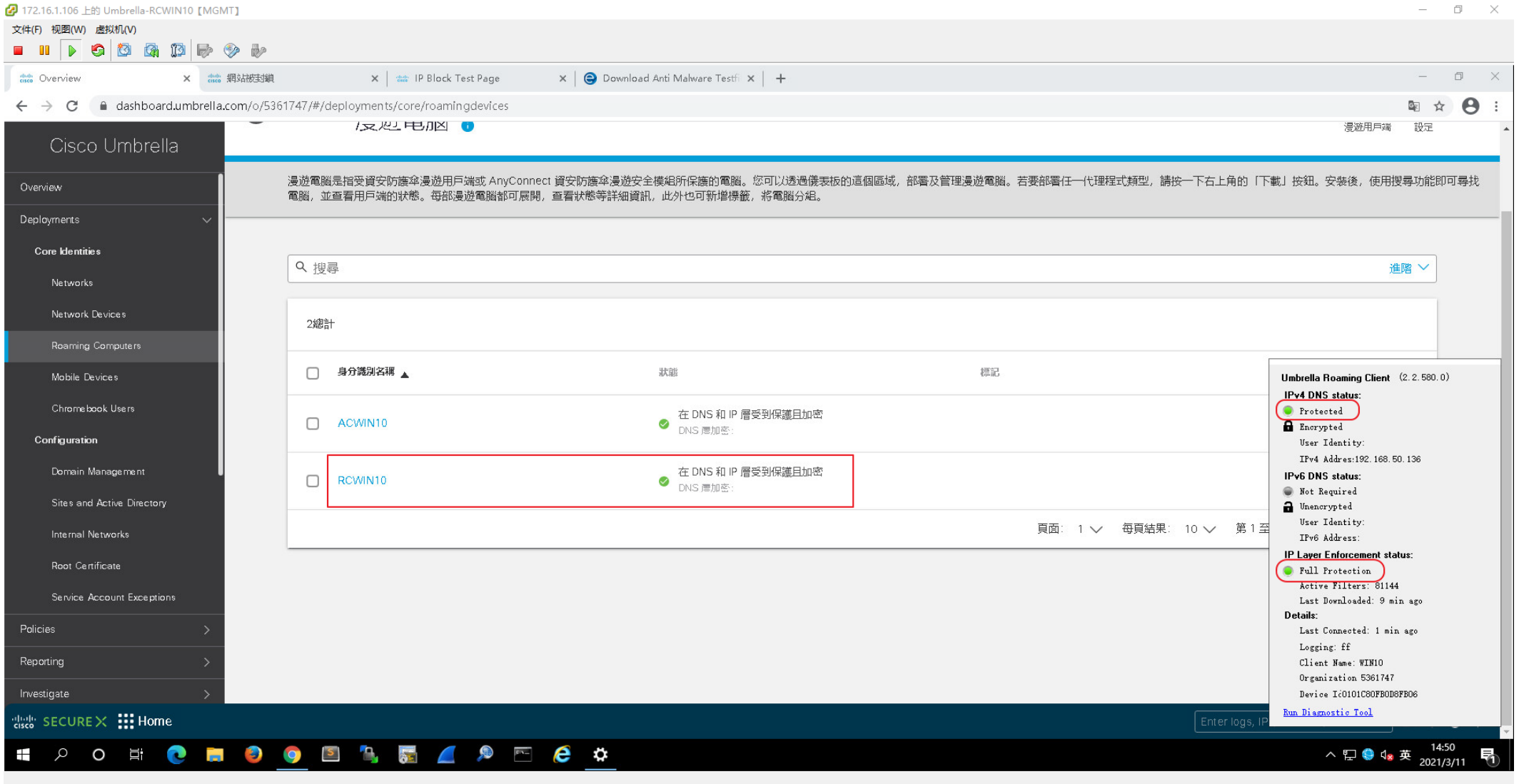
Cisco Umbrella部署（7）



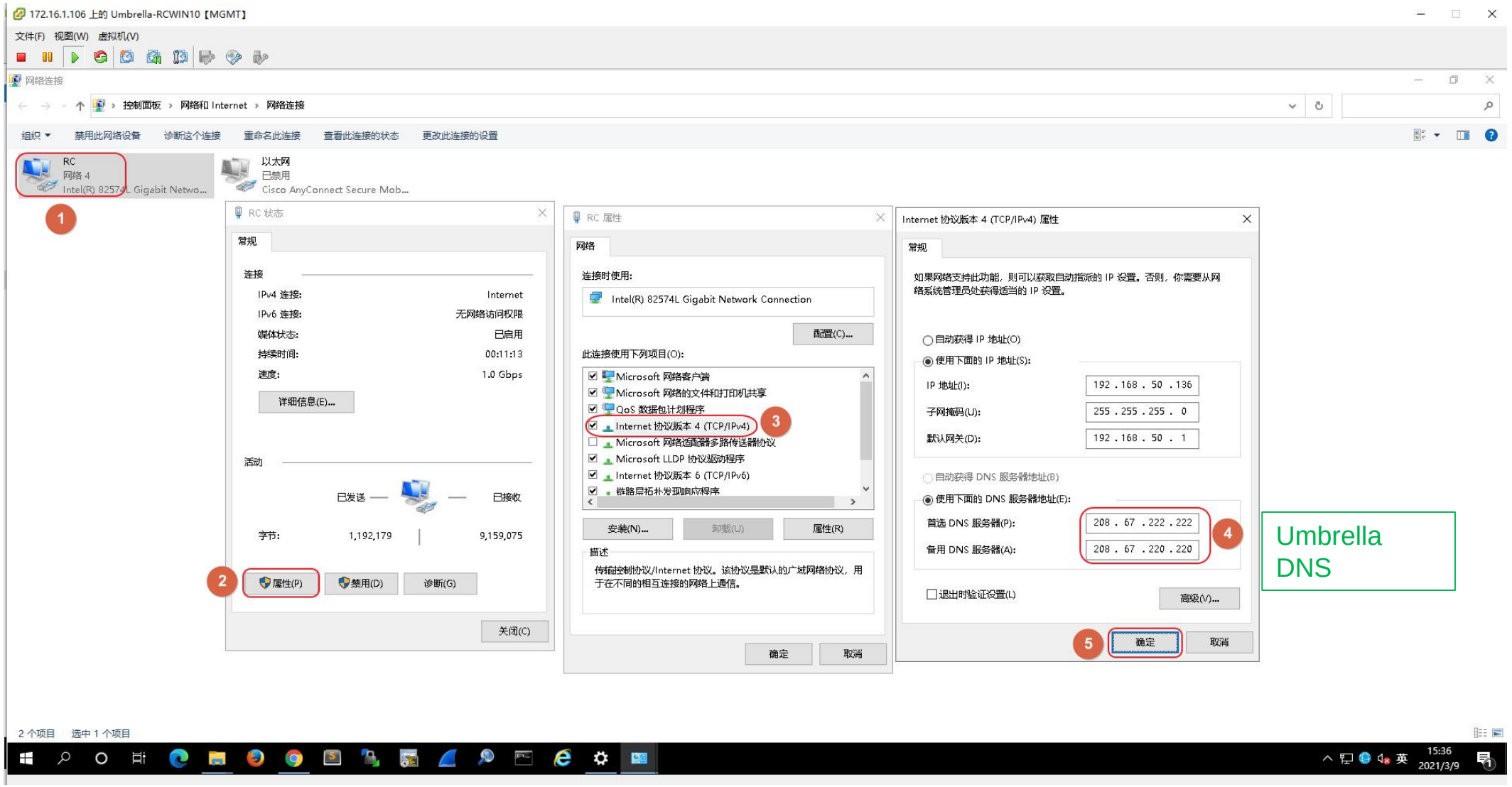
Cisco Umbrella部署（8）



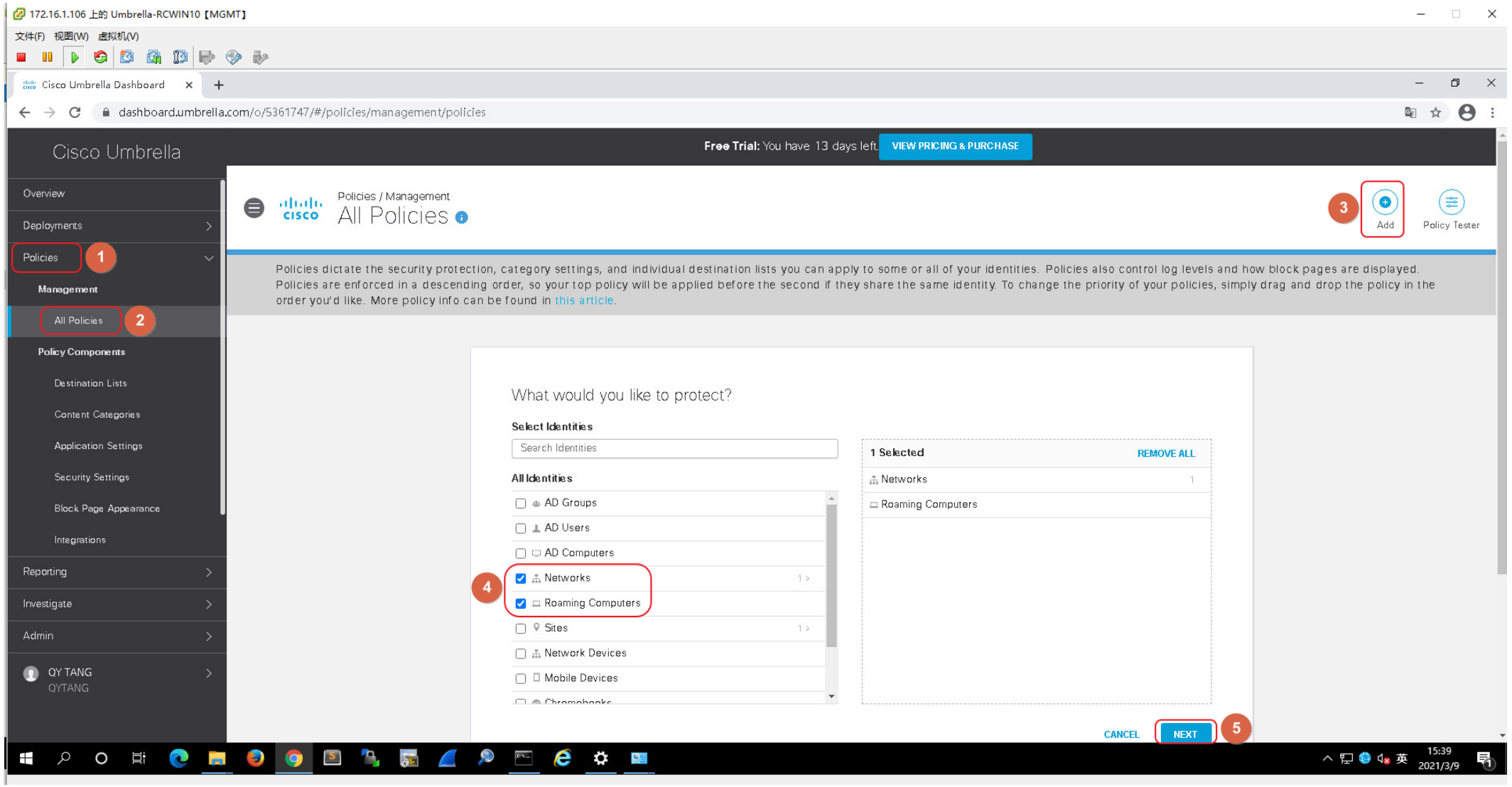
Cisco Umbrella部署（9）



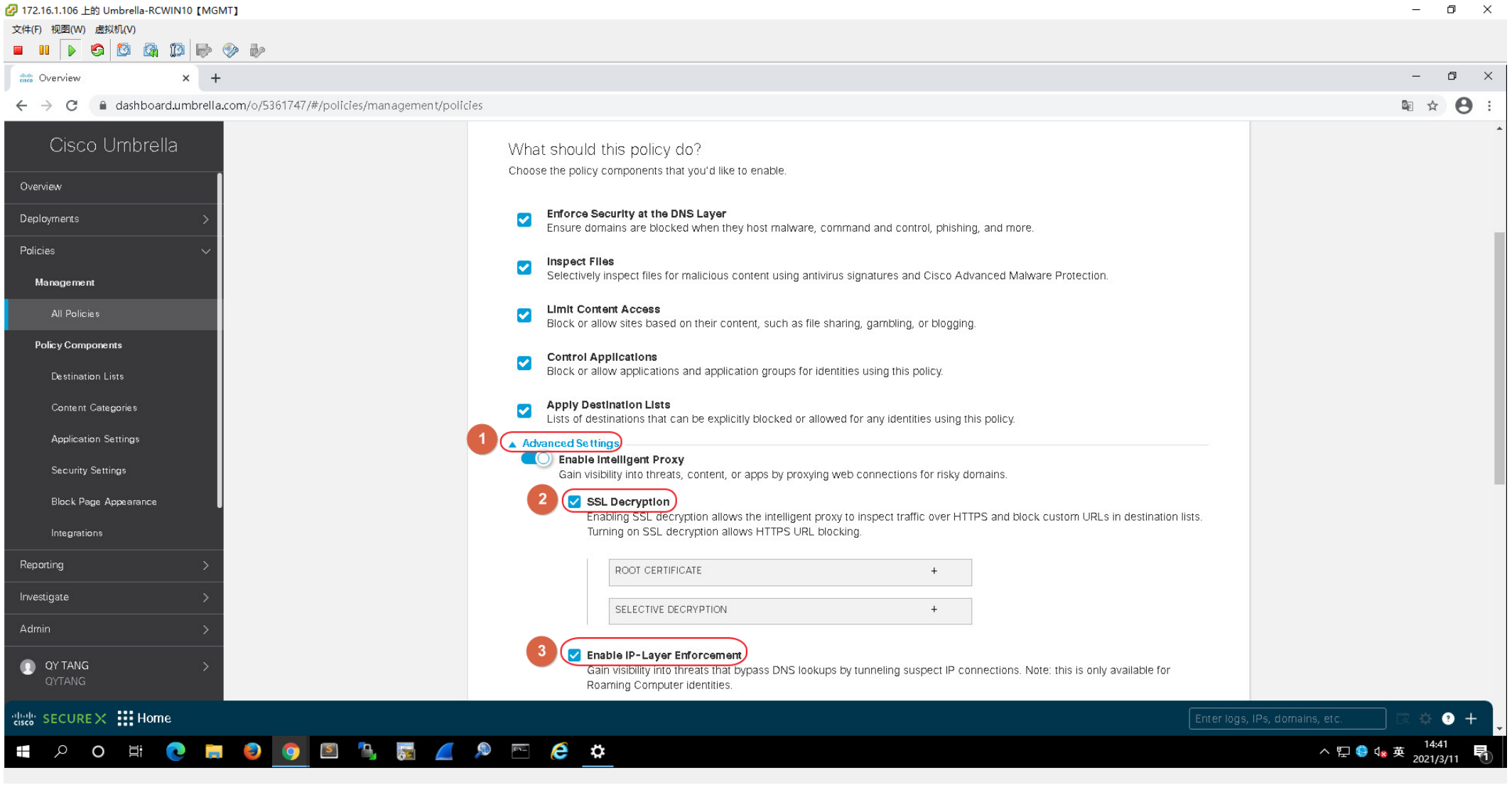
Cisco Umbrella部署（10）



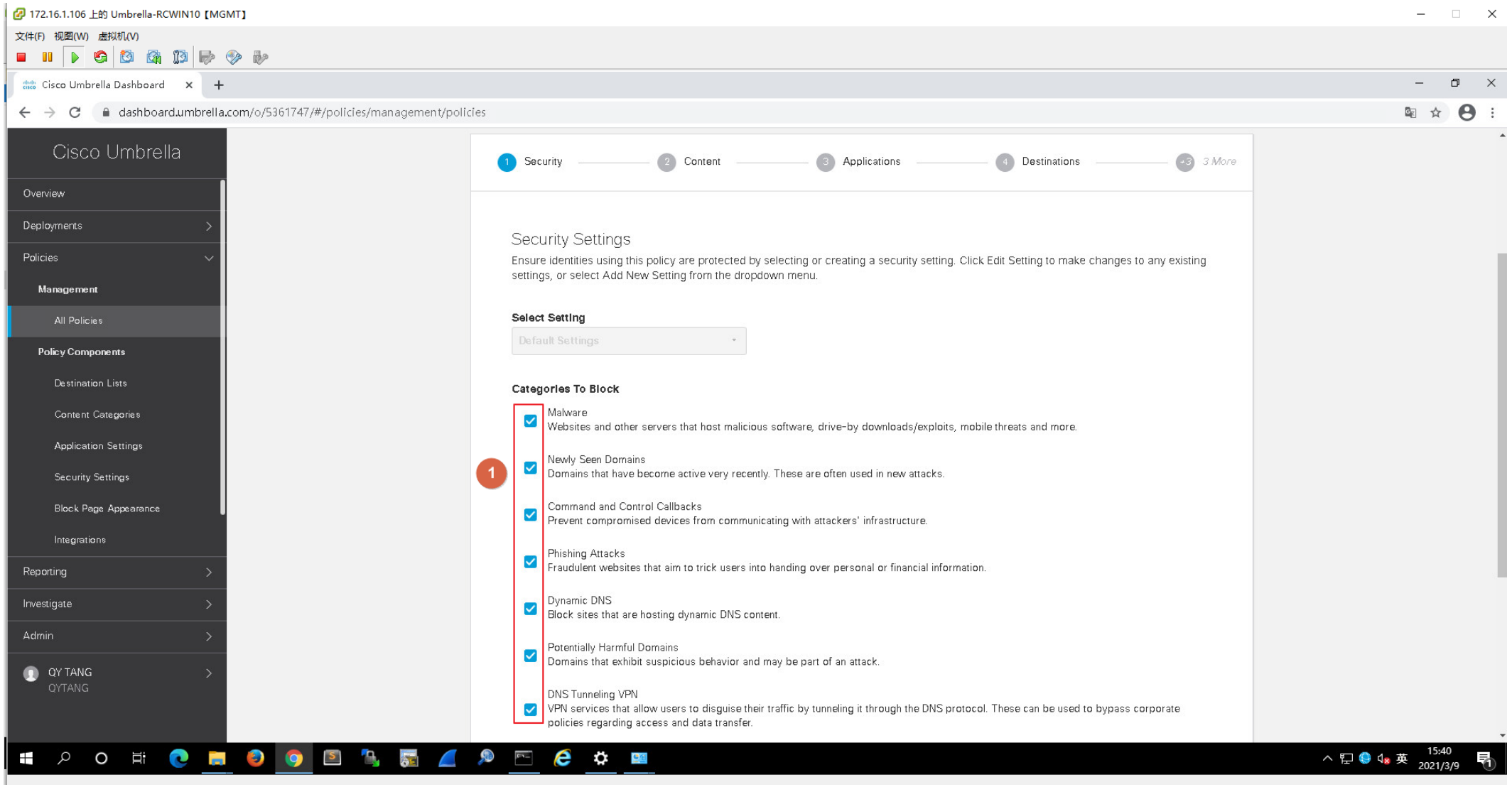
Cisco Umbrella部署（1）



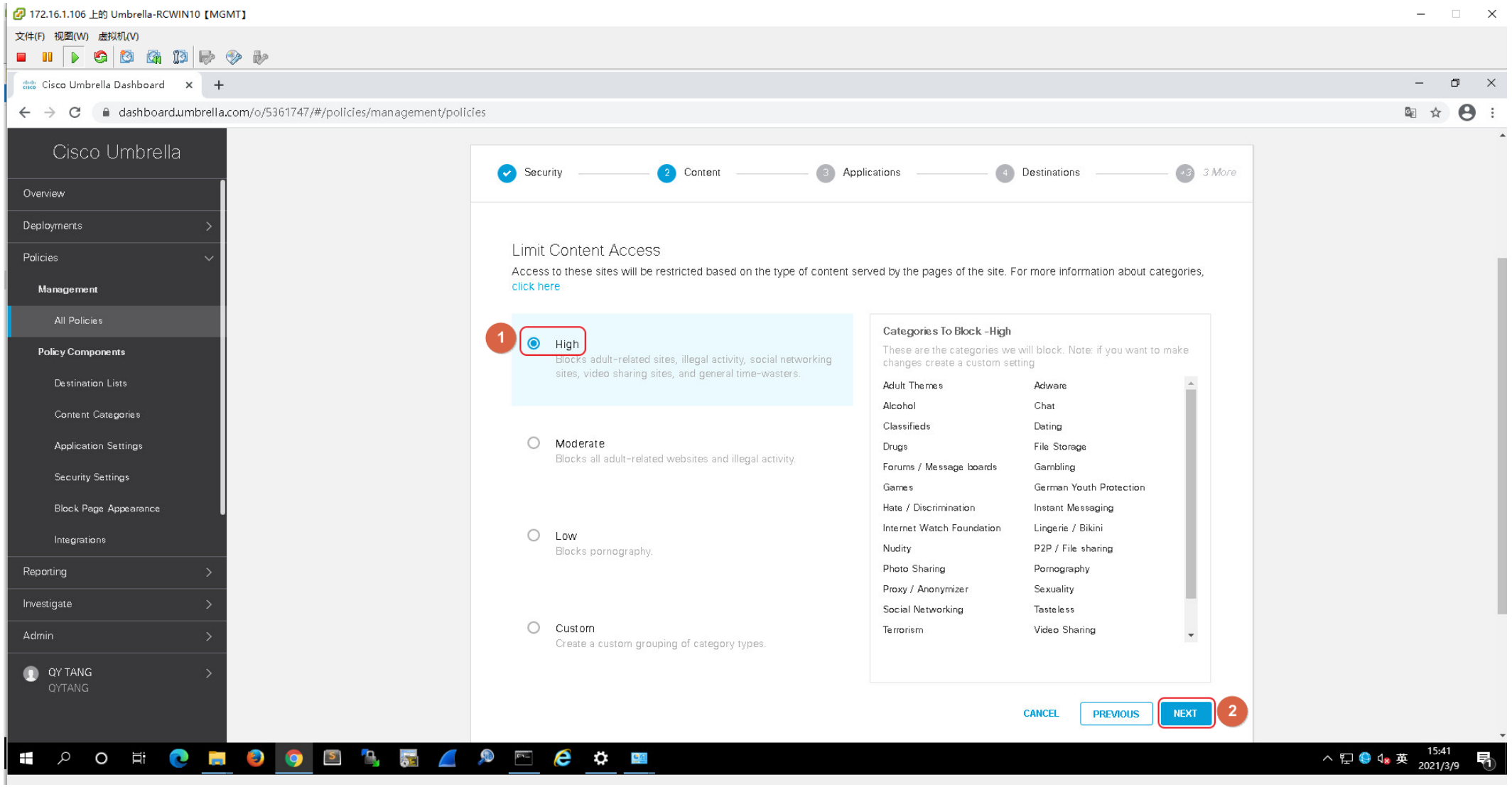
Cisco Umbrella部署（11）



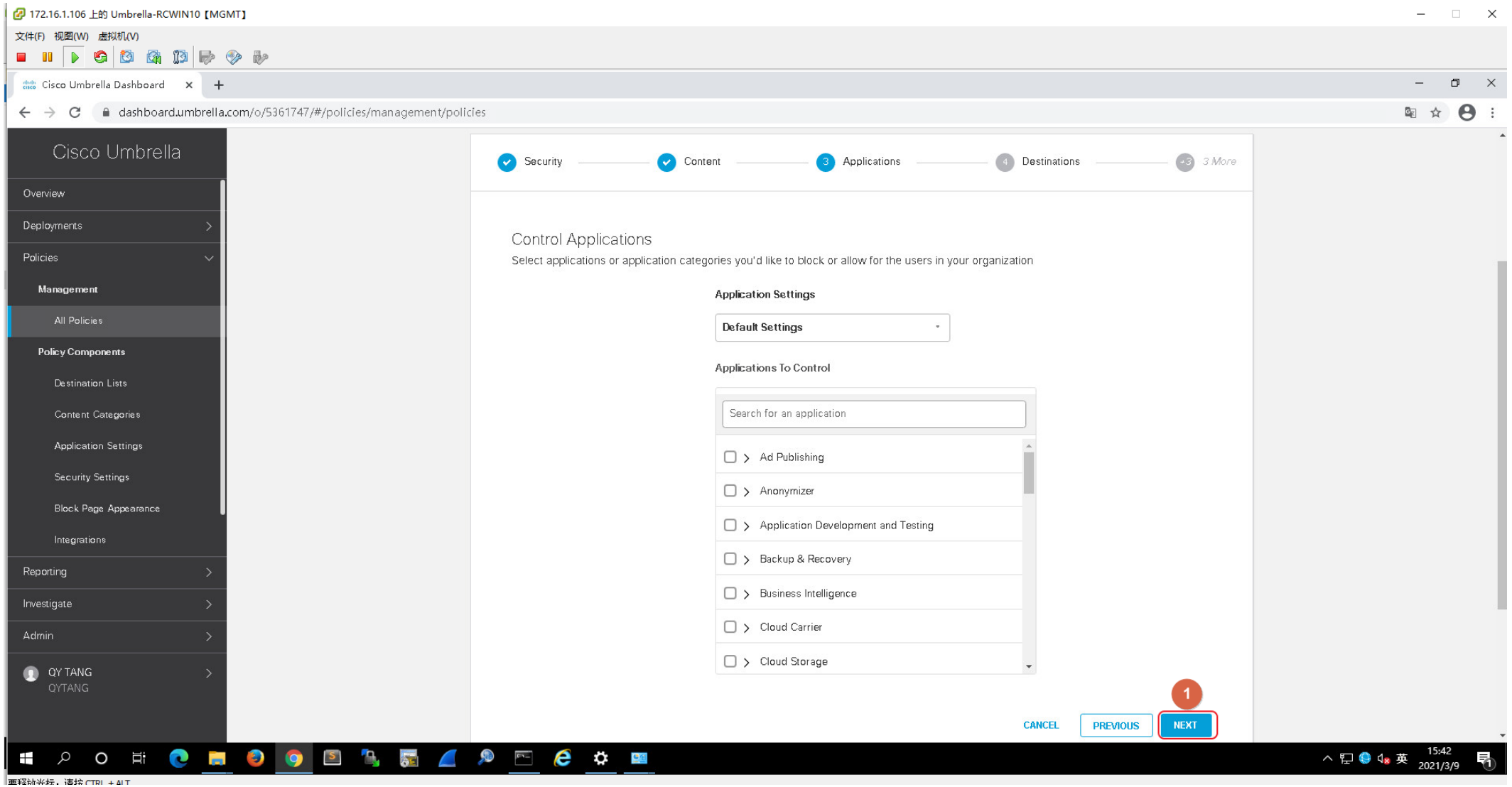
Cisco Umbrella部署（12）



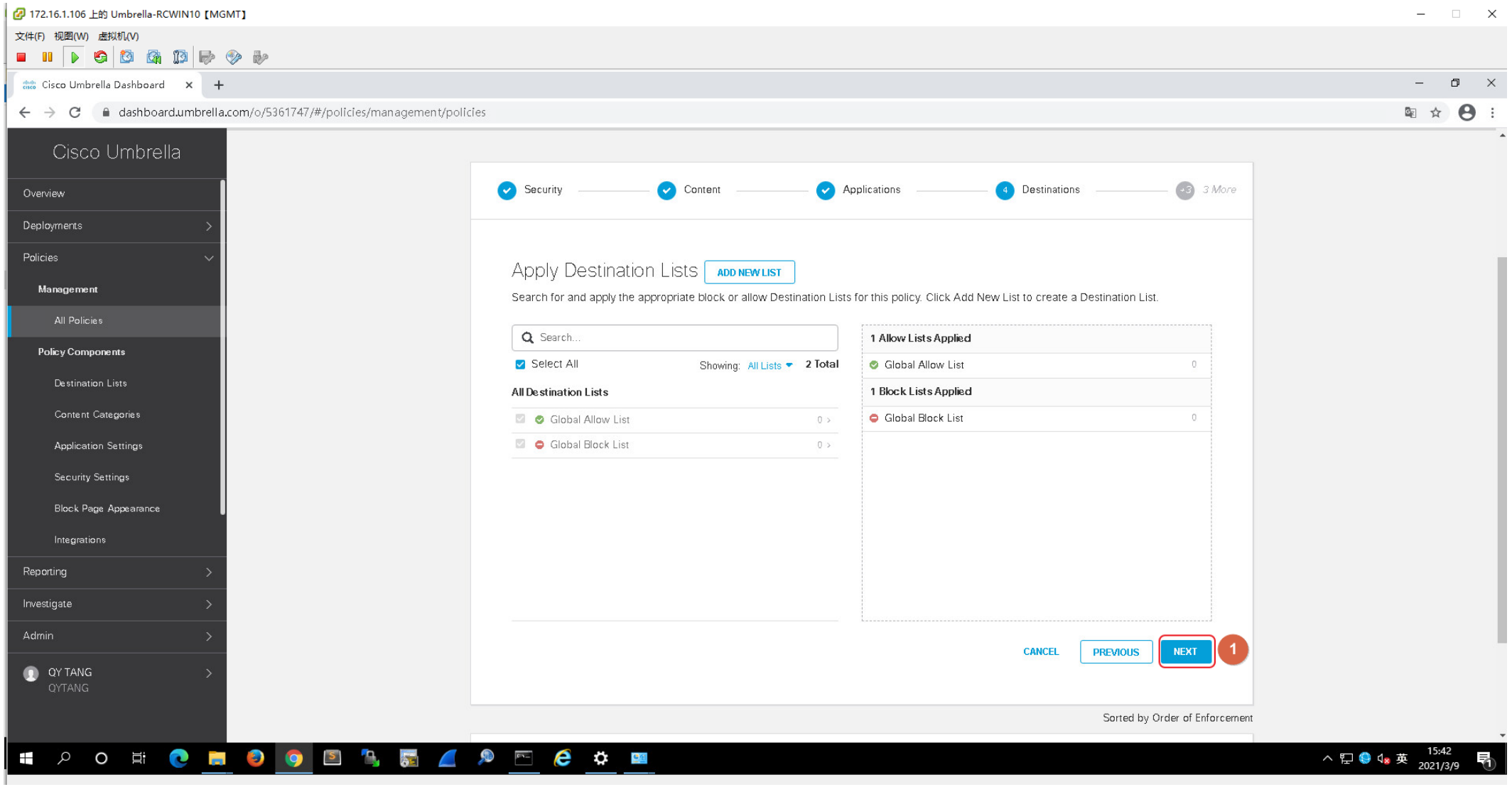
Cisco Umbrella部署（13）



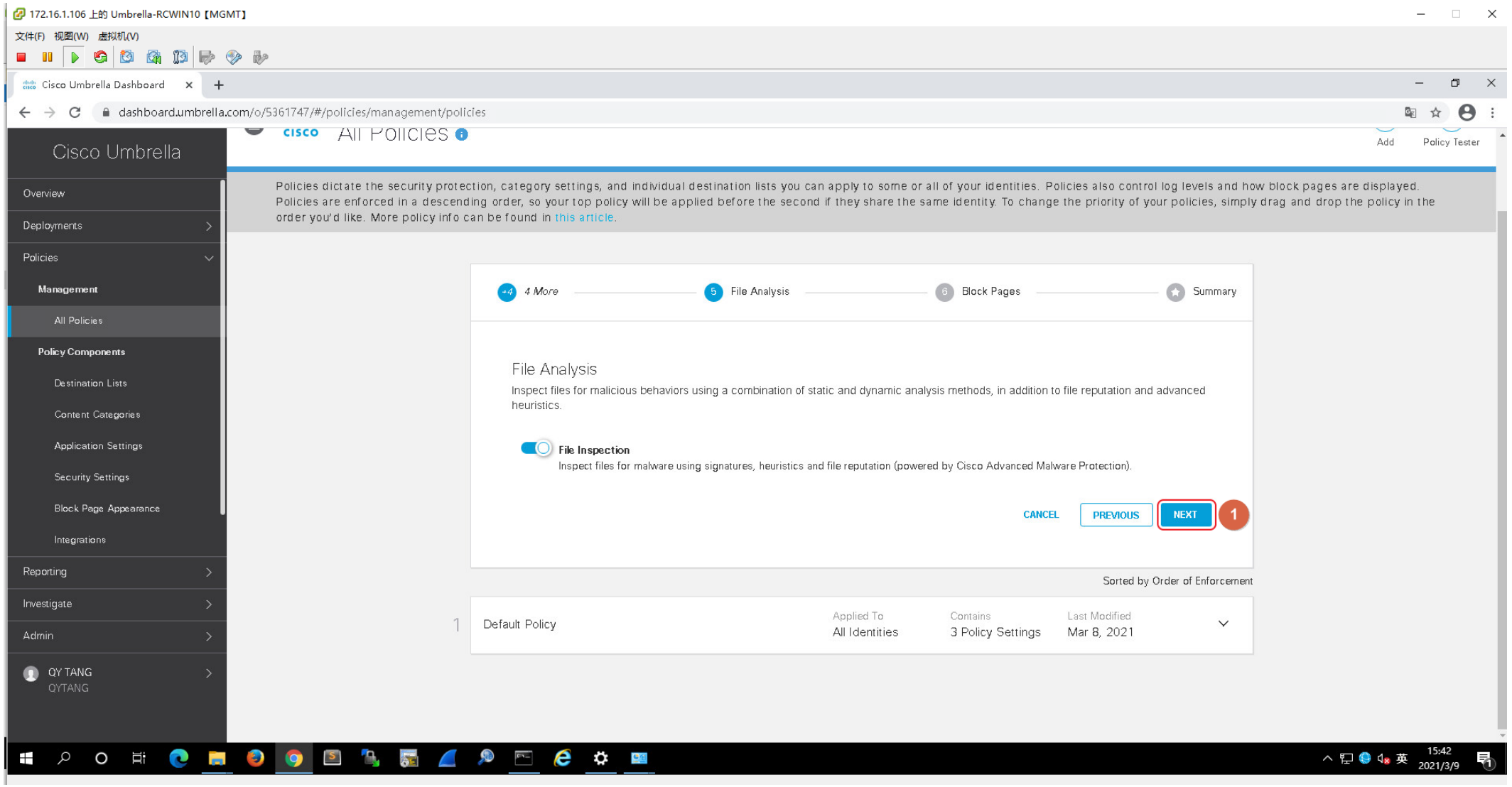
Cisco Umbrella部署（14）



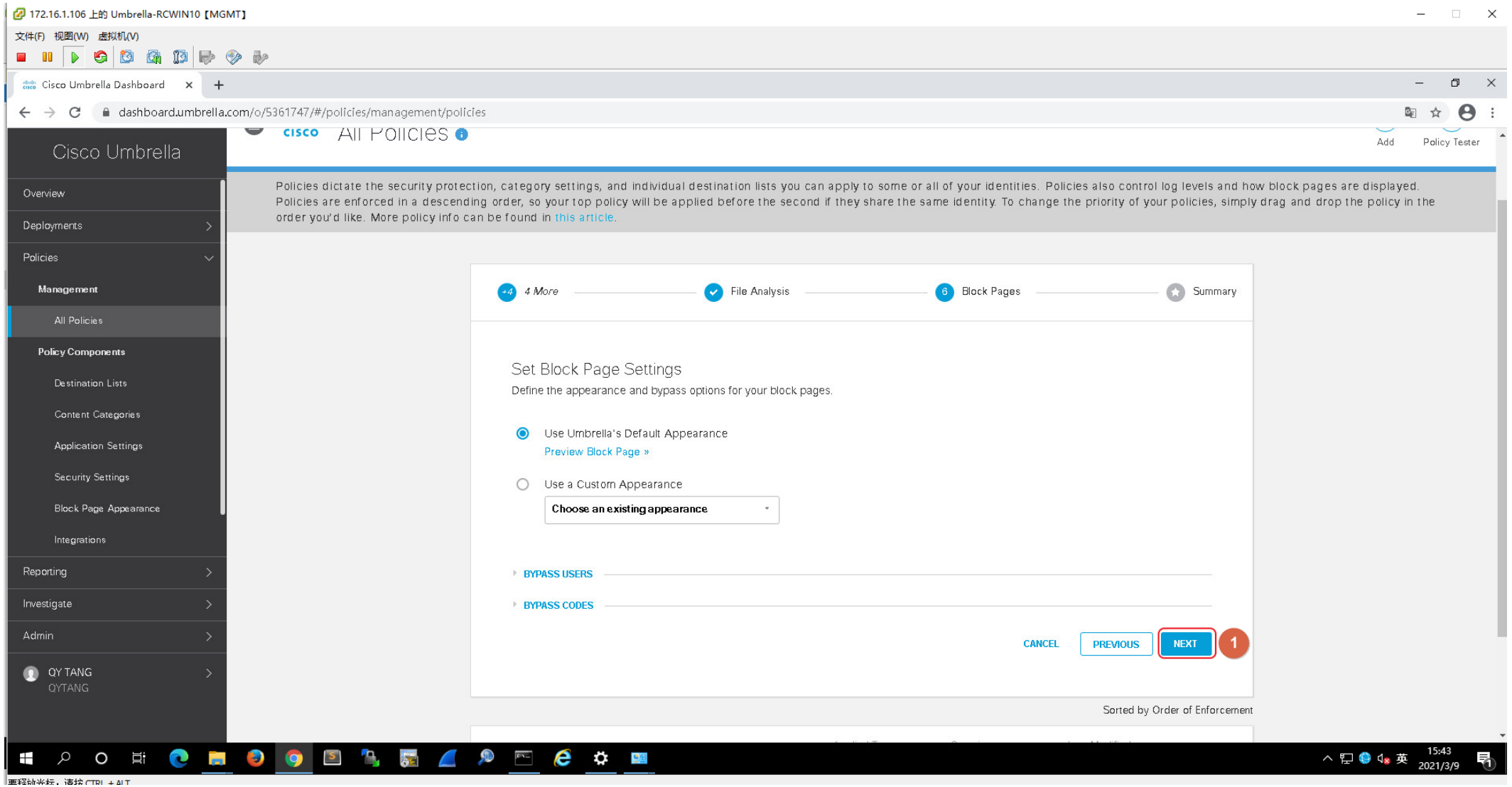
Cisco Umbrella部署（15）



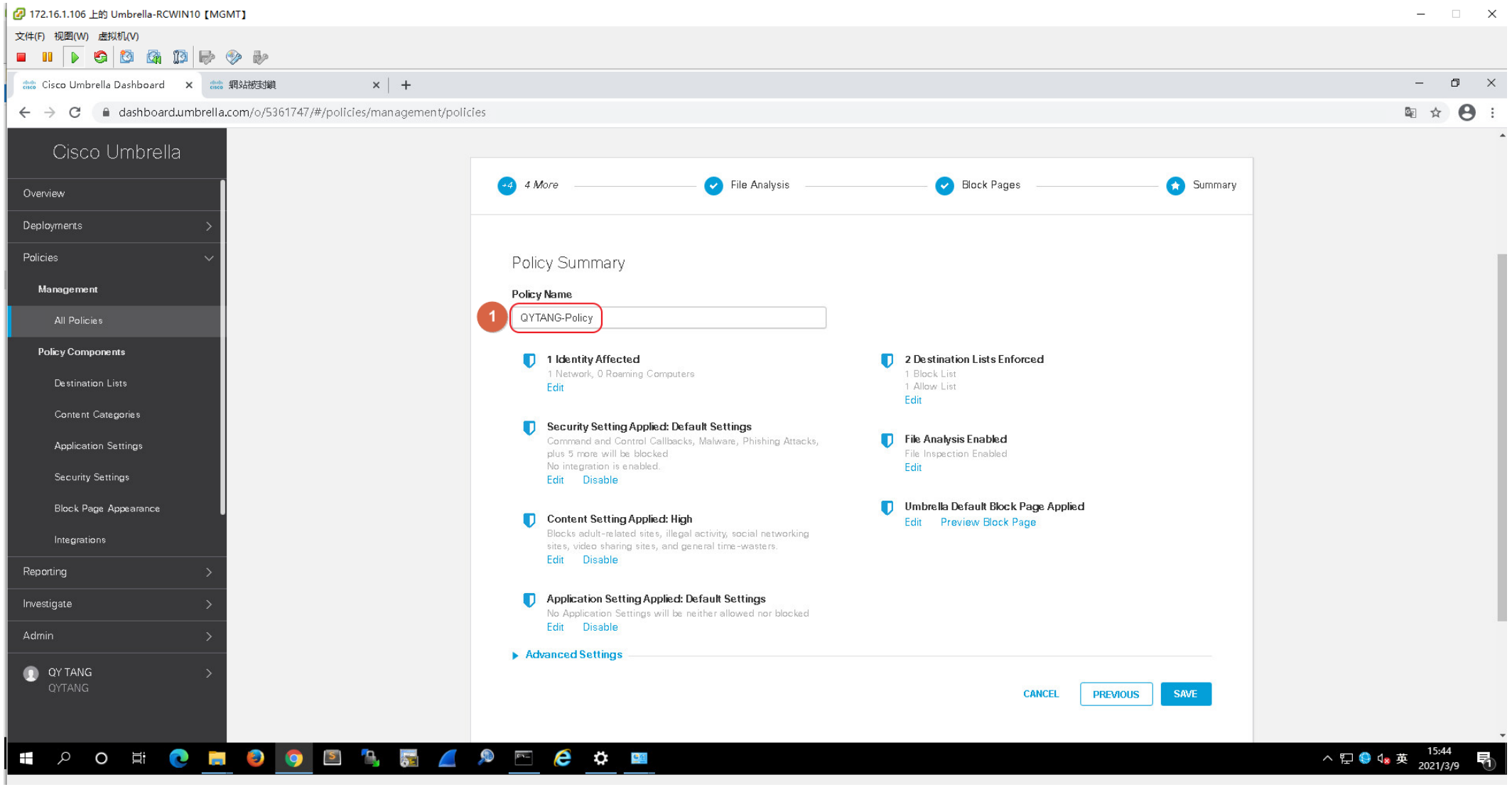
Cisco Umbrella部署（16）



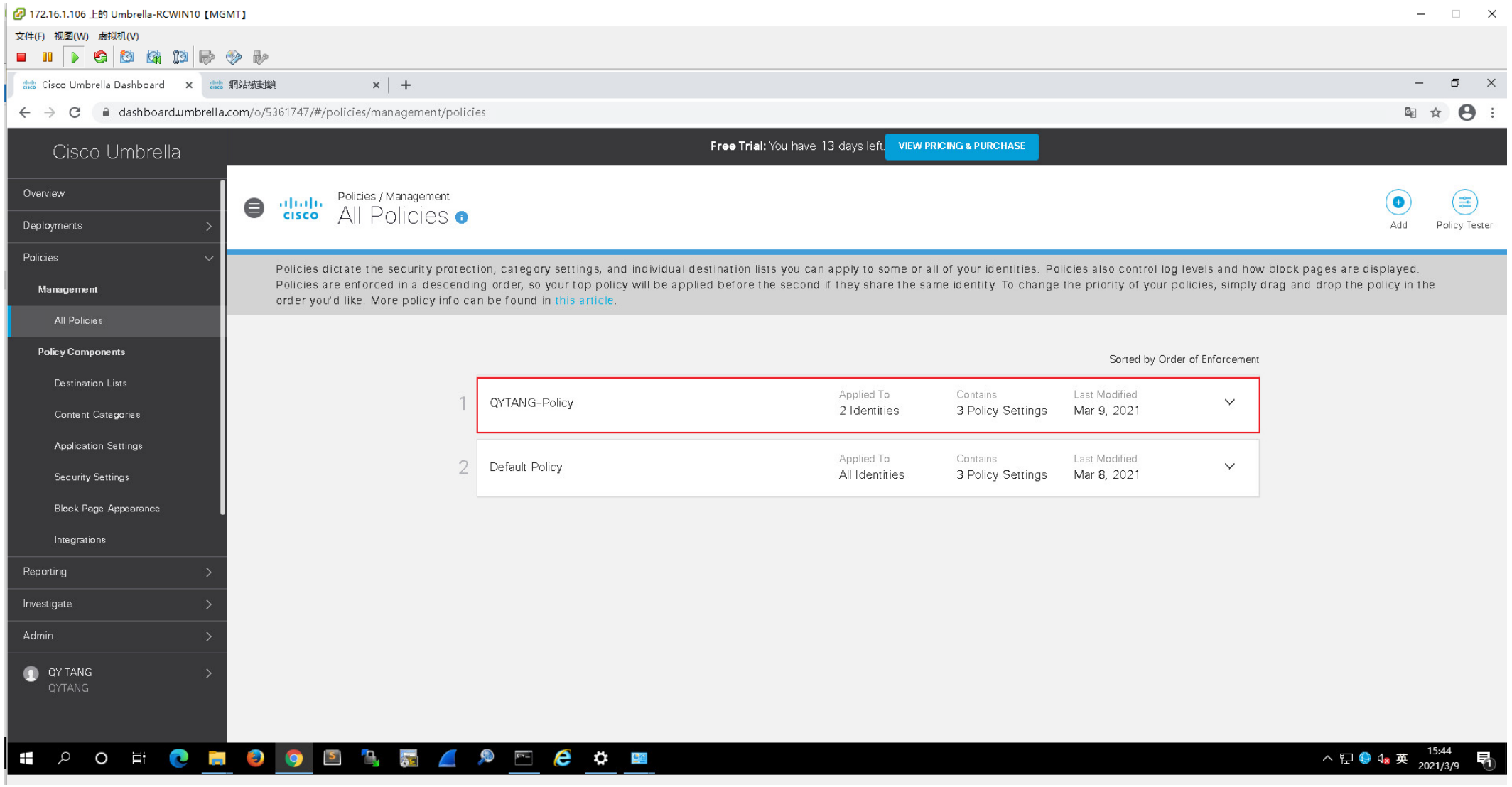
Cisco Umbrella部署（17）



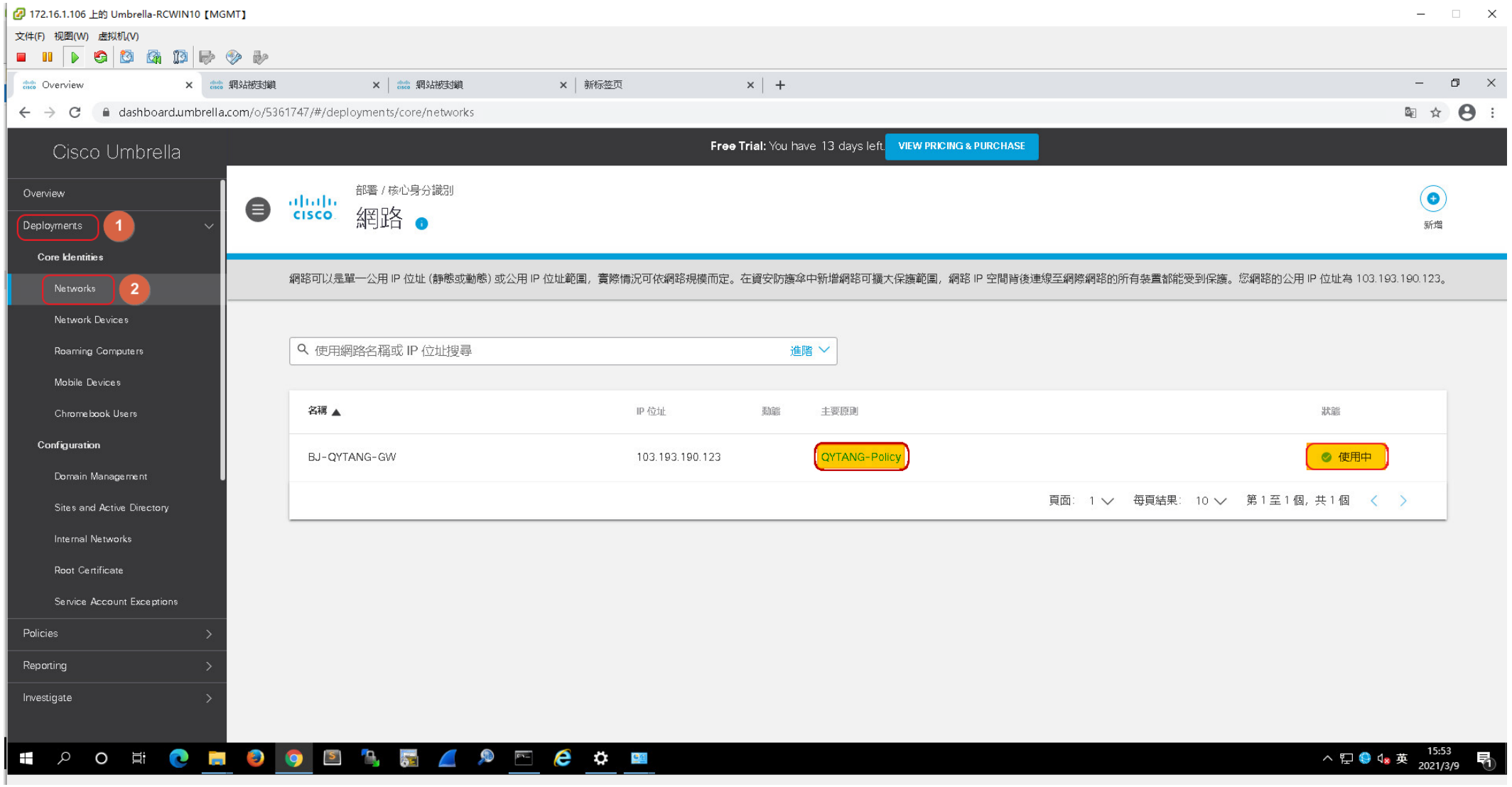
Cisco Umbrella部署（18）



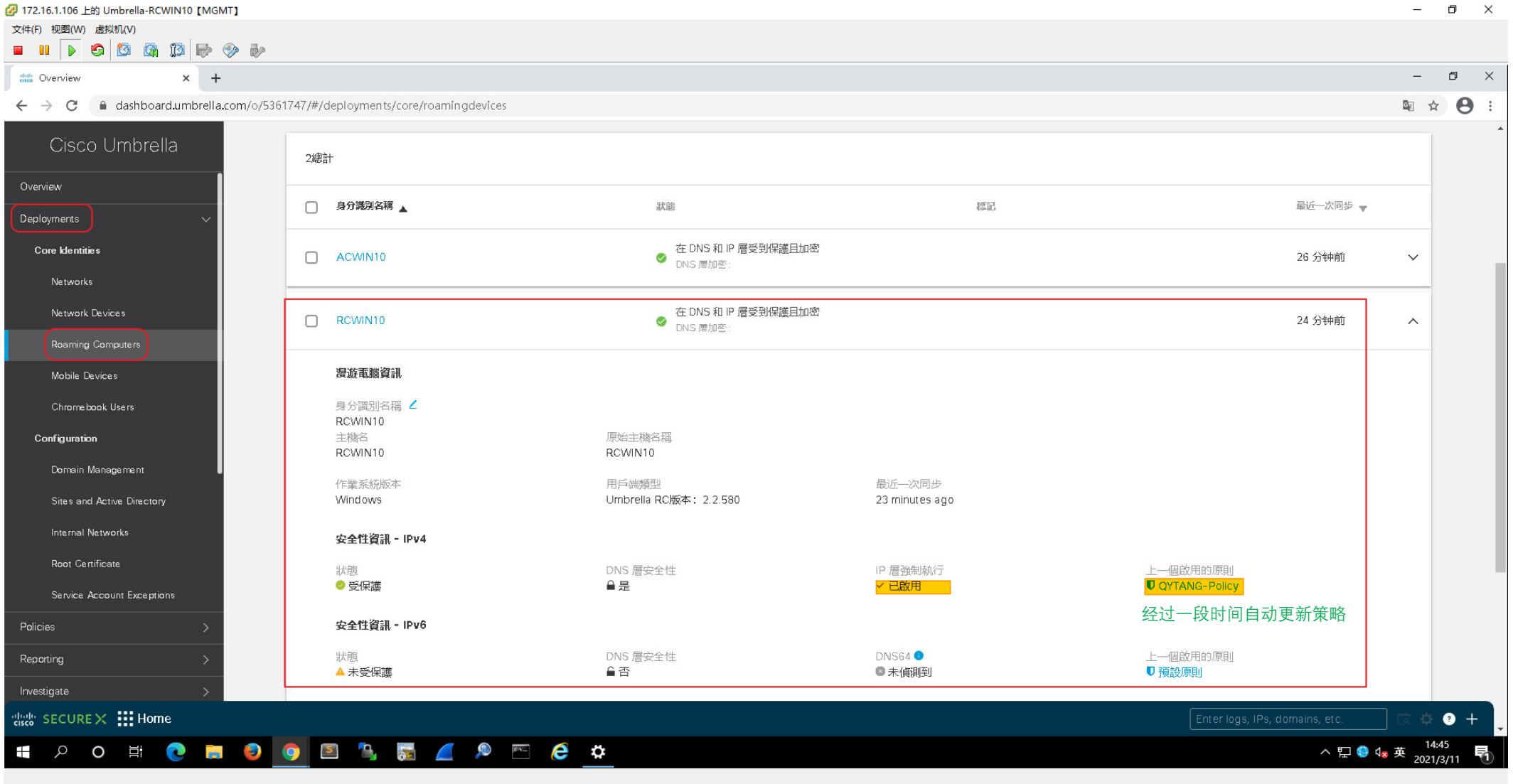
Cisco Umbrella部署（19）



Cisco Umbrella部署（20）

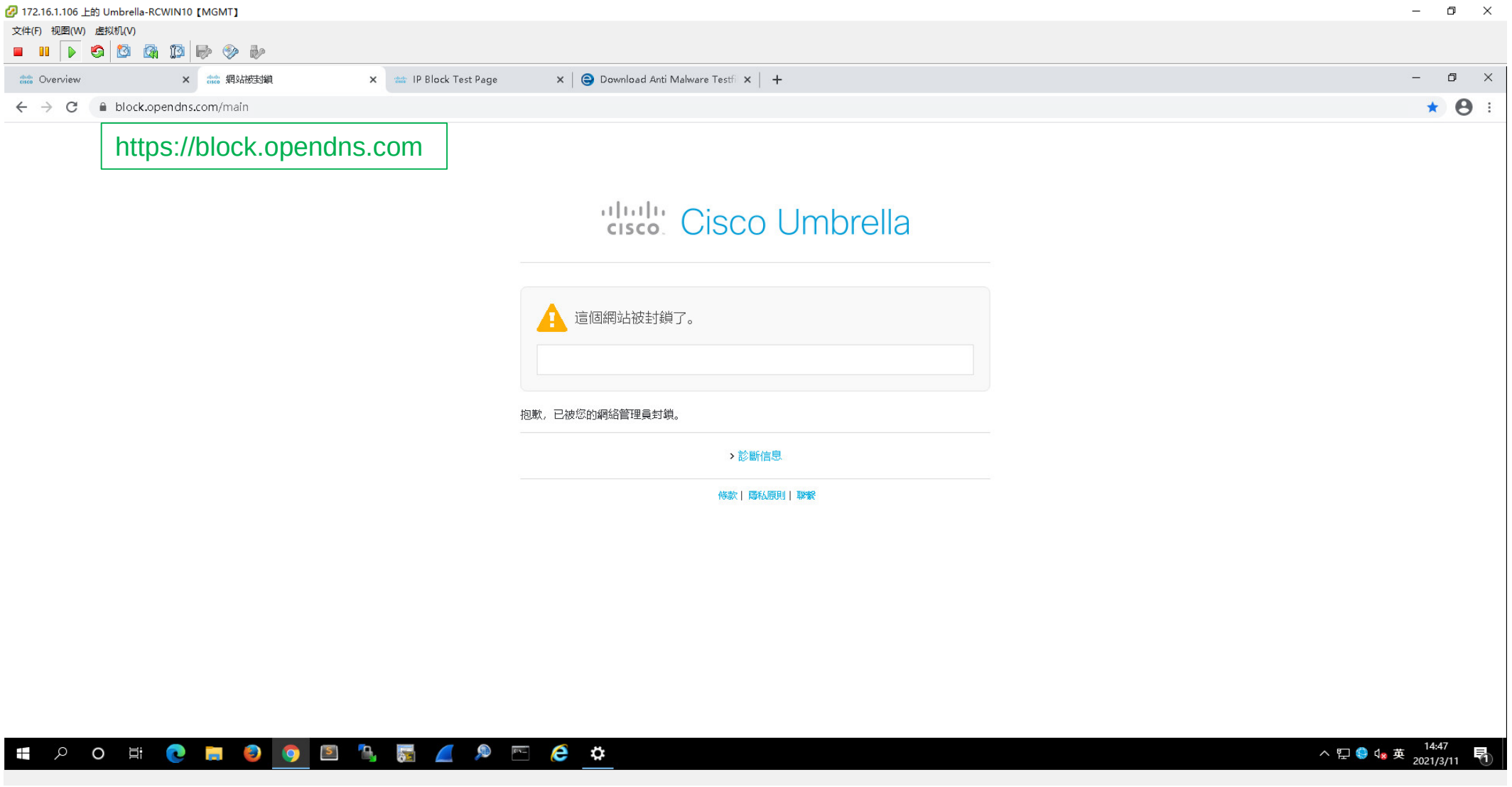


Cisco Umbrella部署（21）

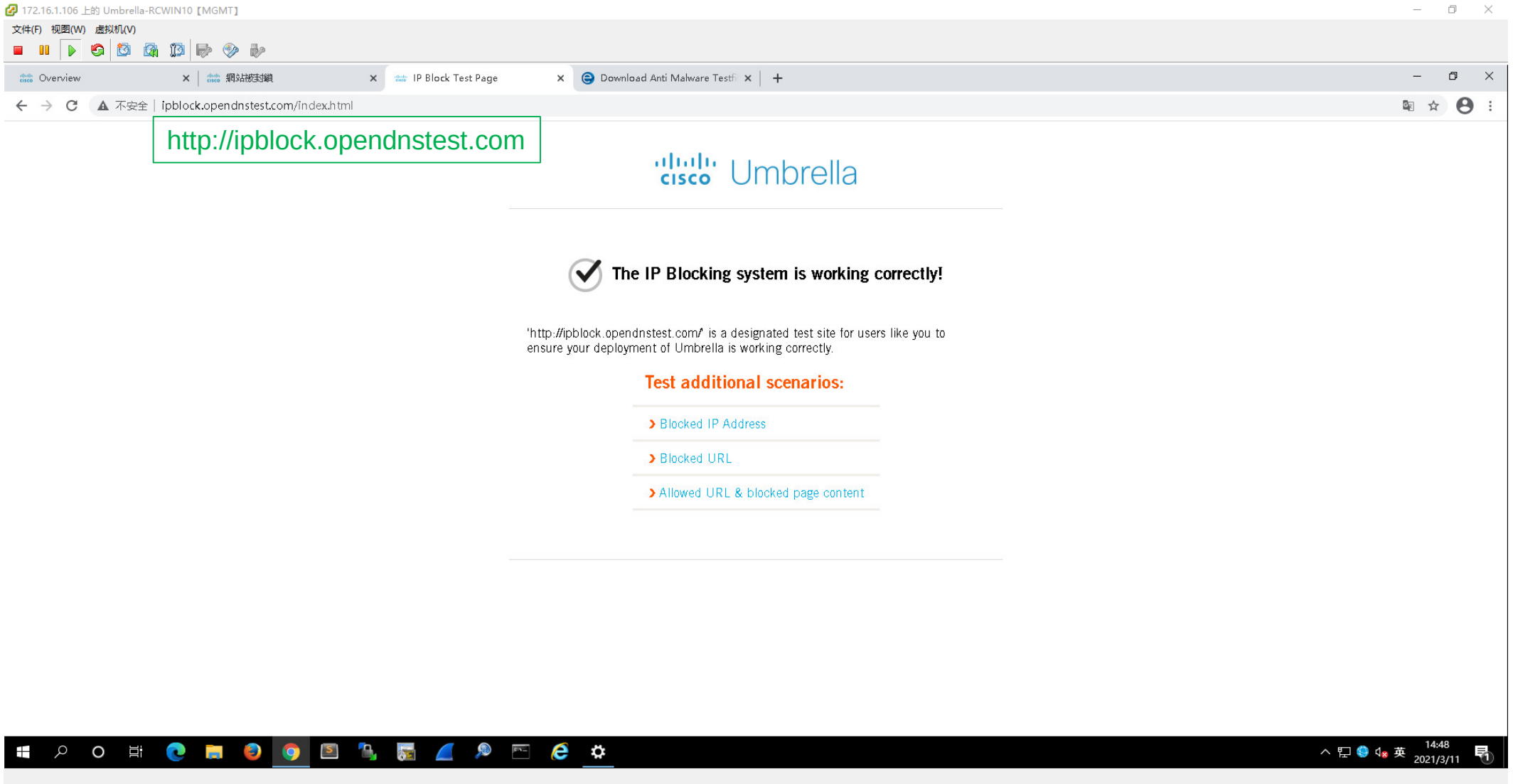


3. Cisco Umbrella测试

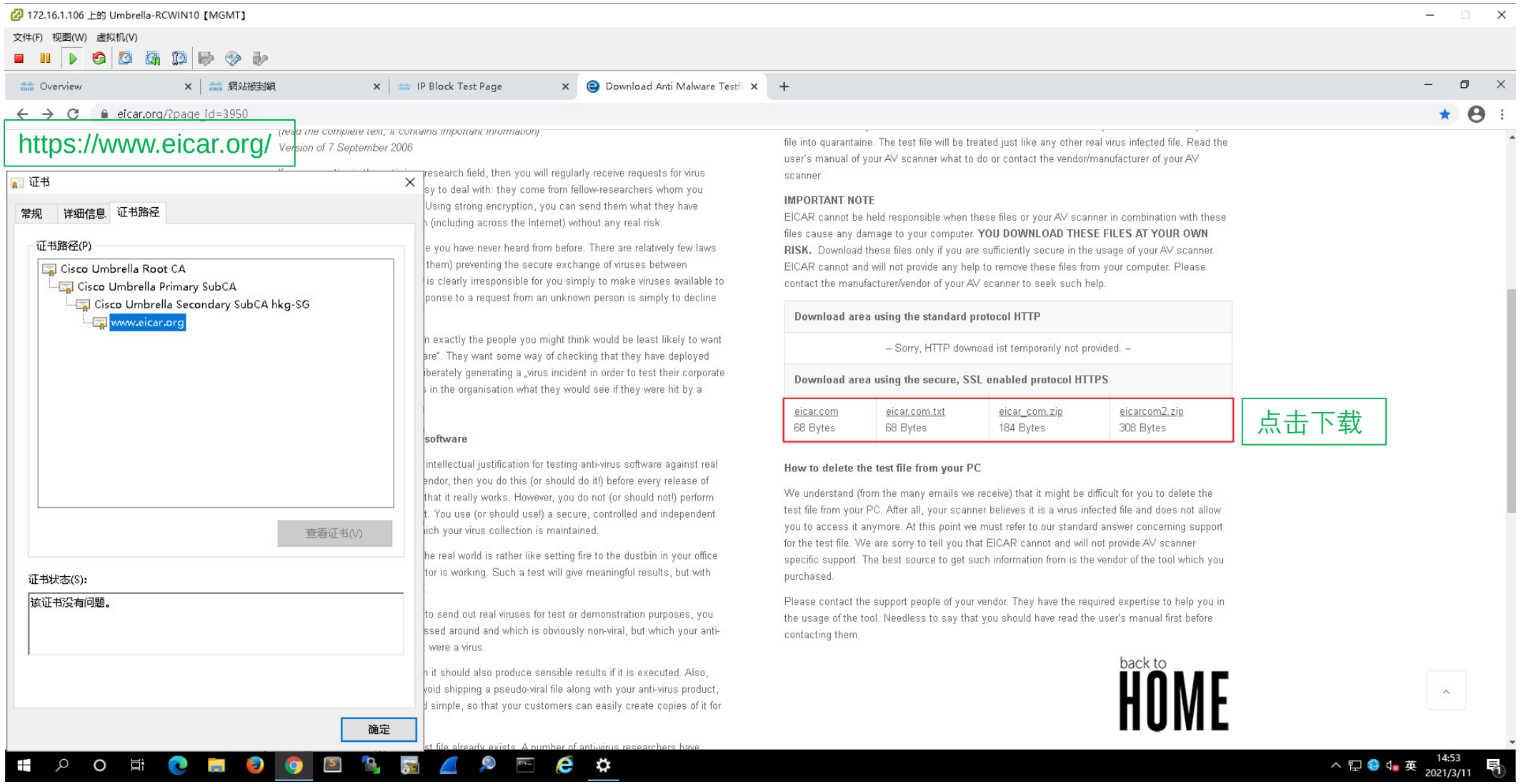
Cisco Umbrella测试（1）



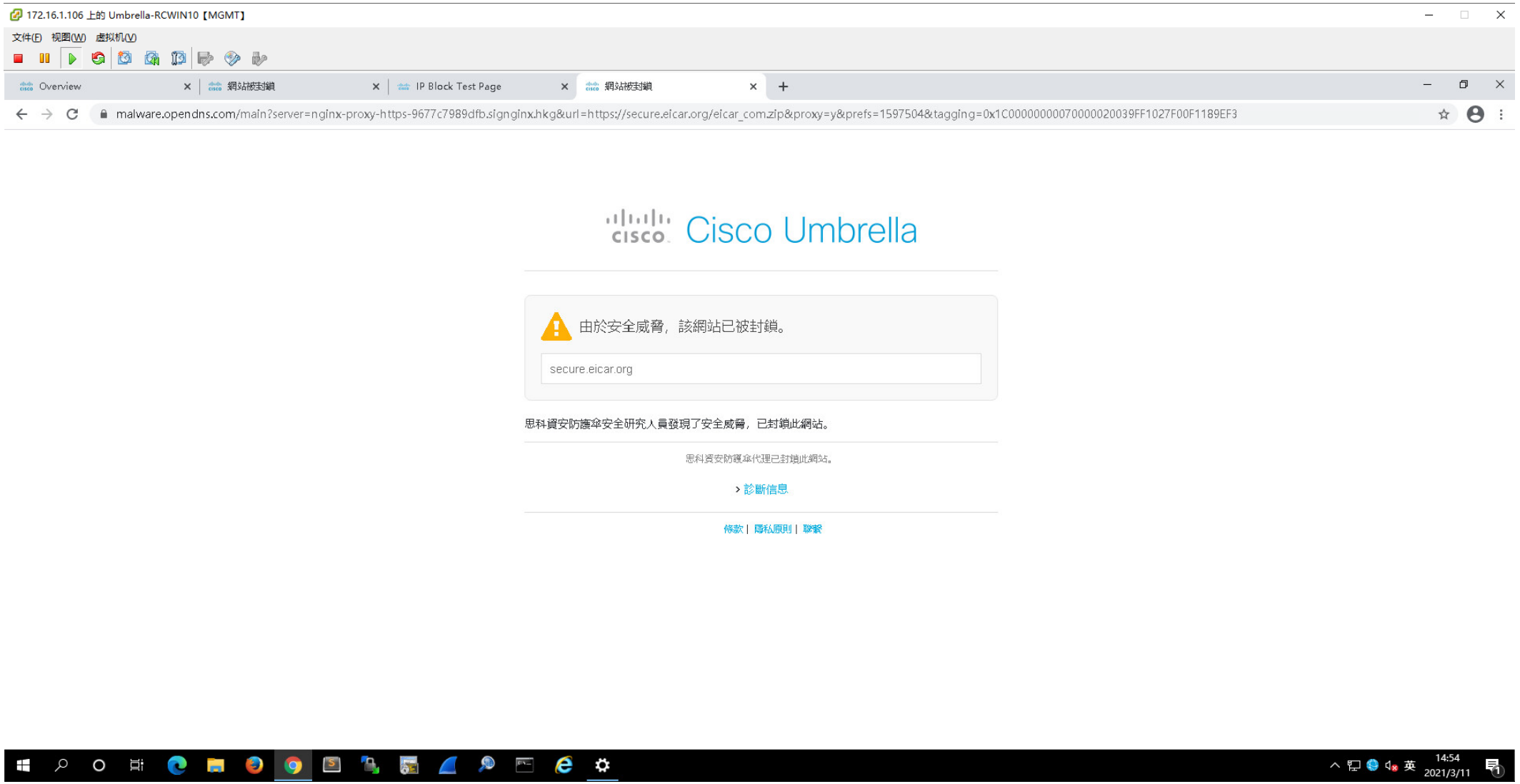
Cisco Umbrella测试（2）



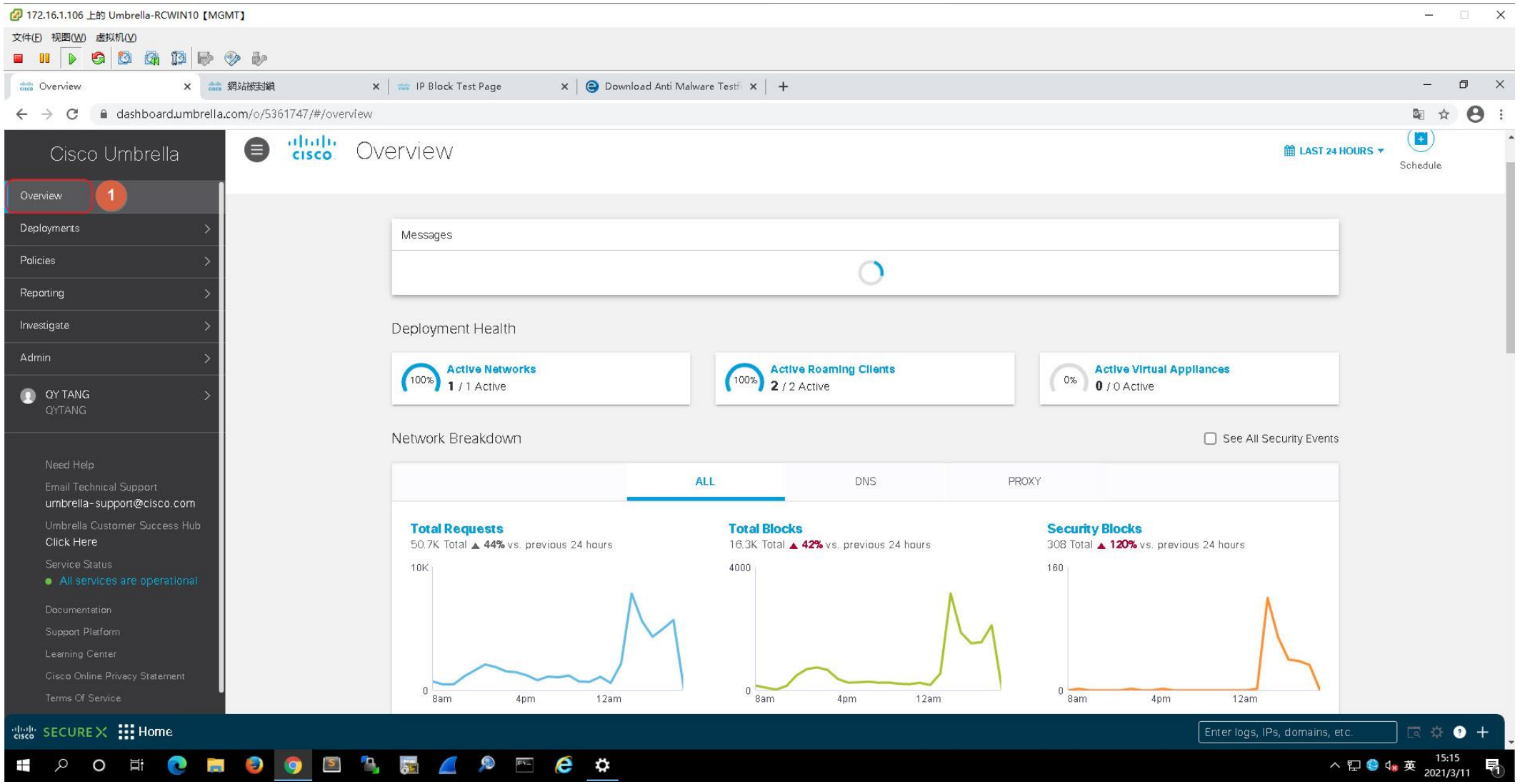
Cisco Umbrella测试（3）



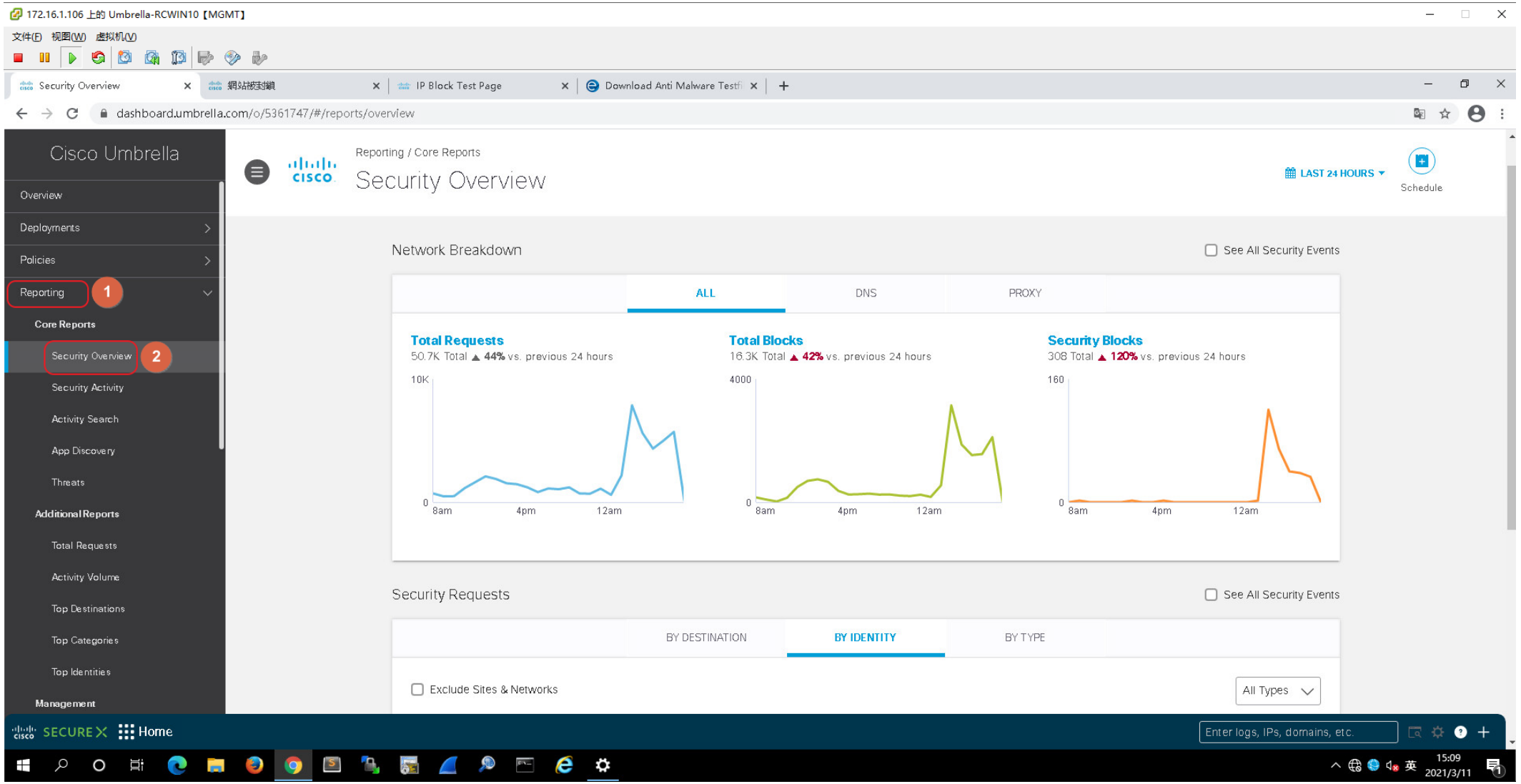
Cisco Umbrella测试（4）



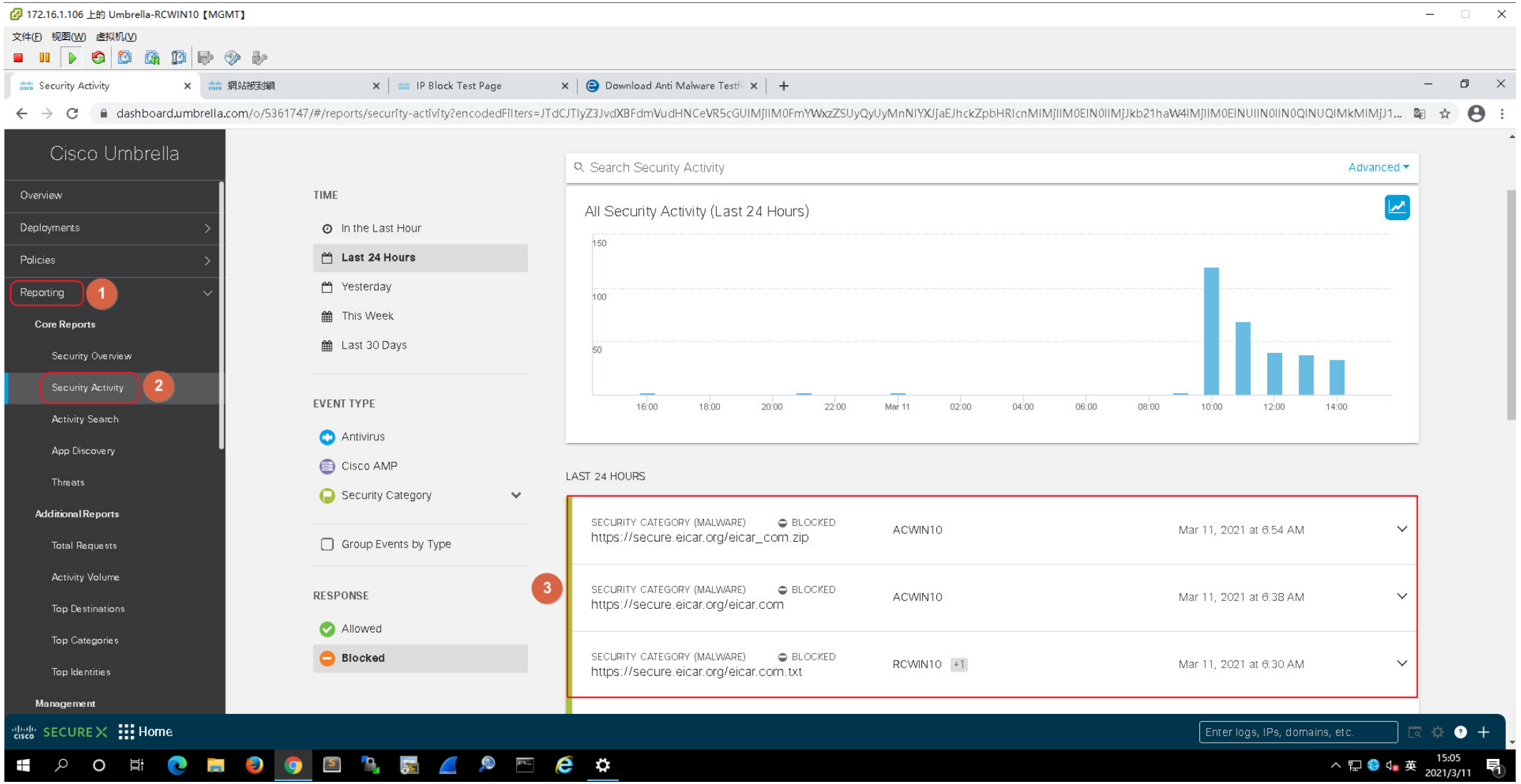
Cisco Umbrella测试（5）



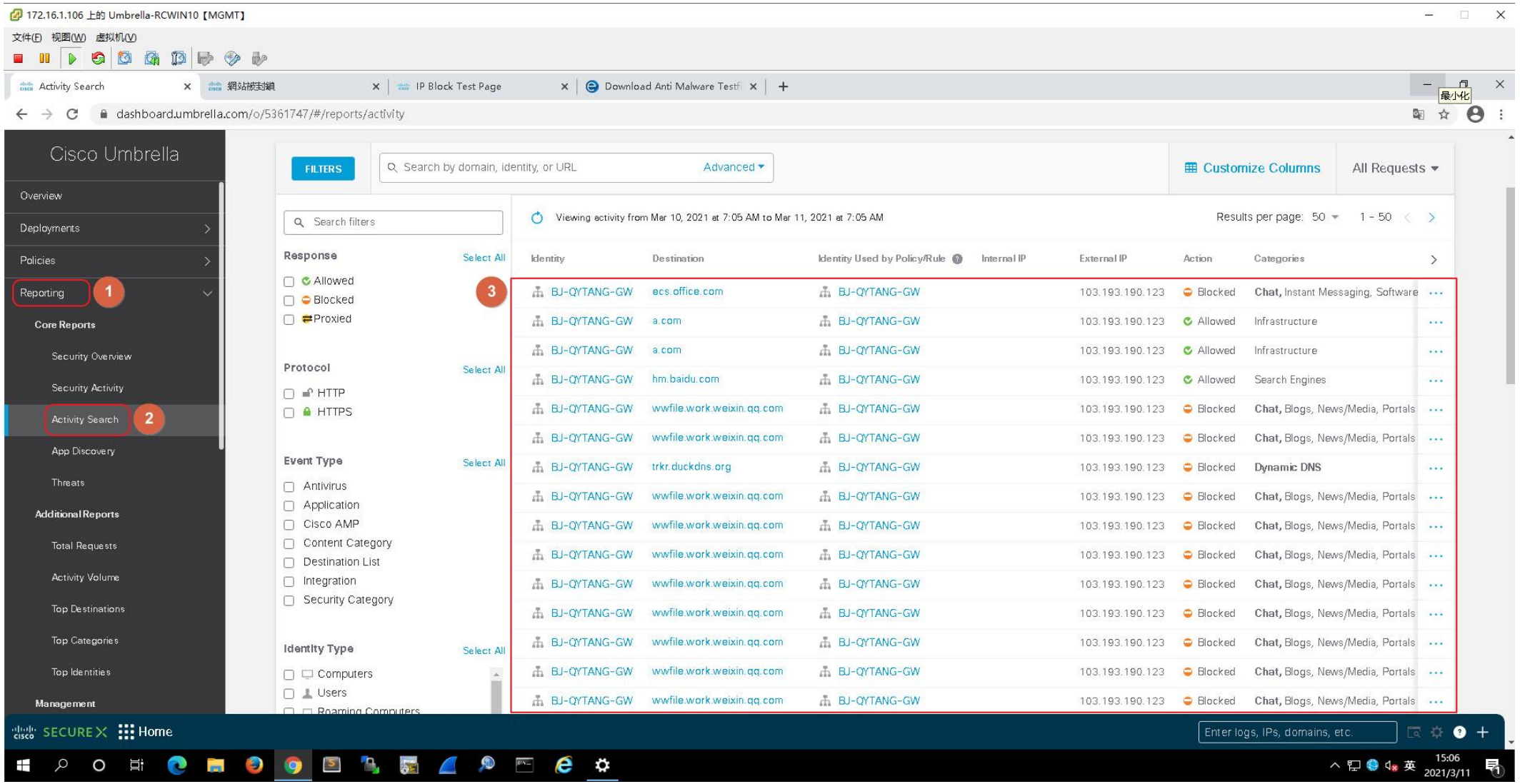
Cisco Umbrella测试（6）



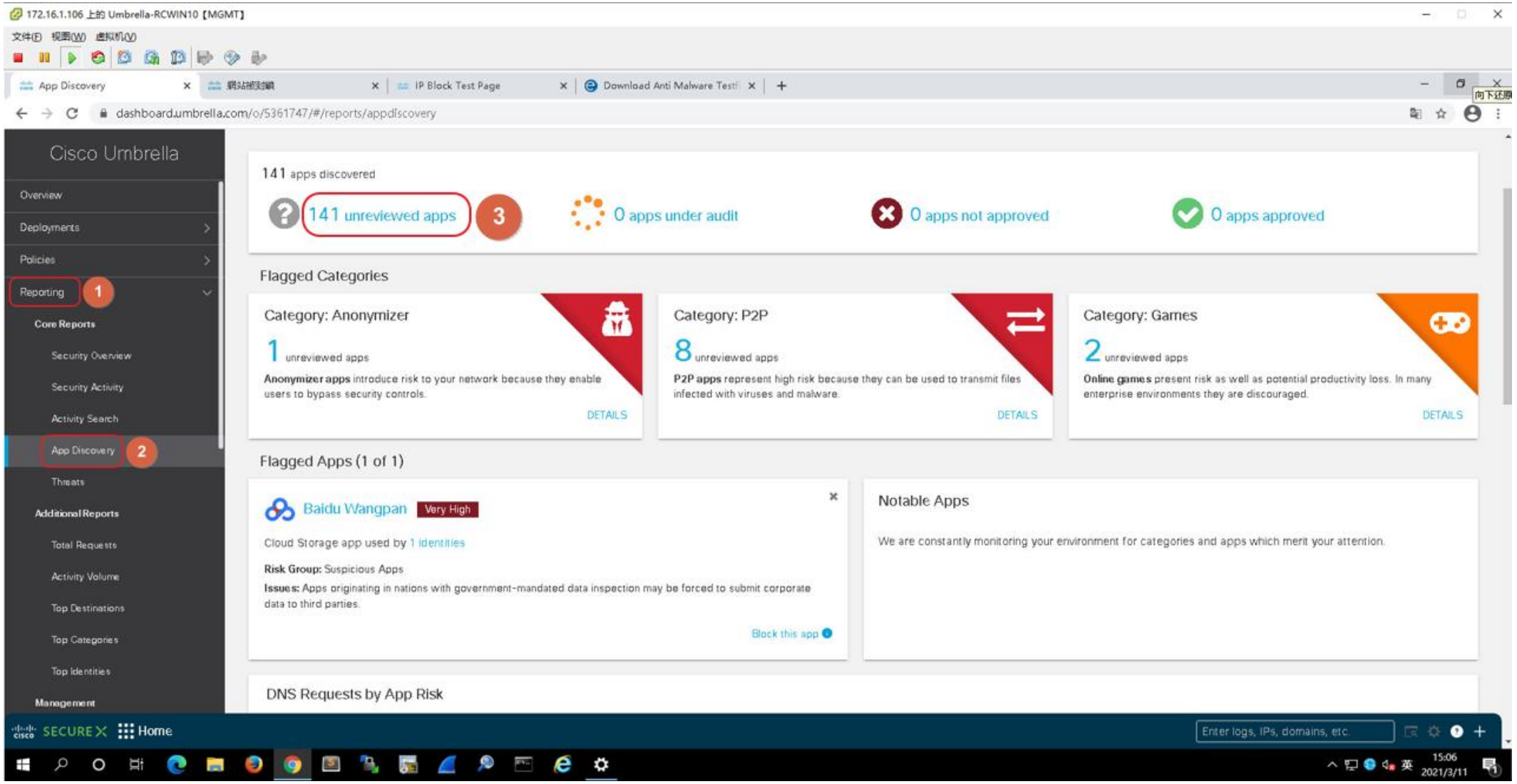
Cisco Umbrella测试（7）



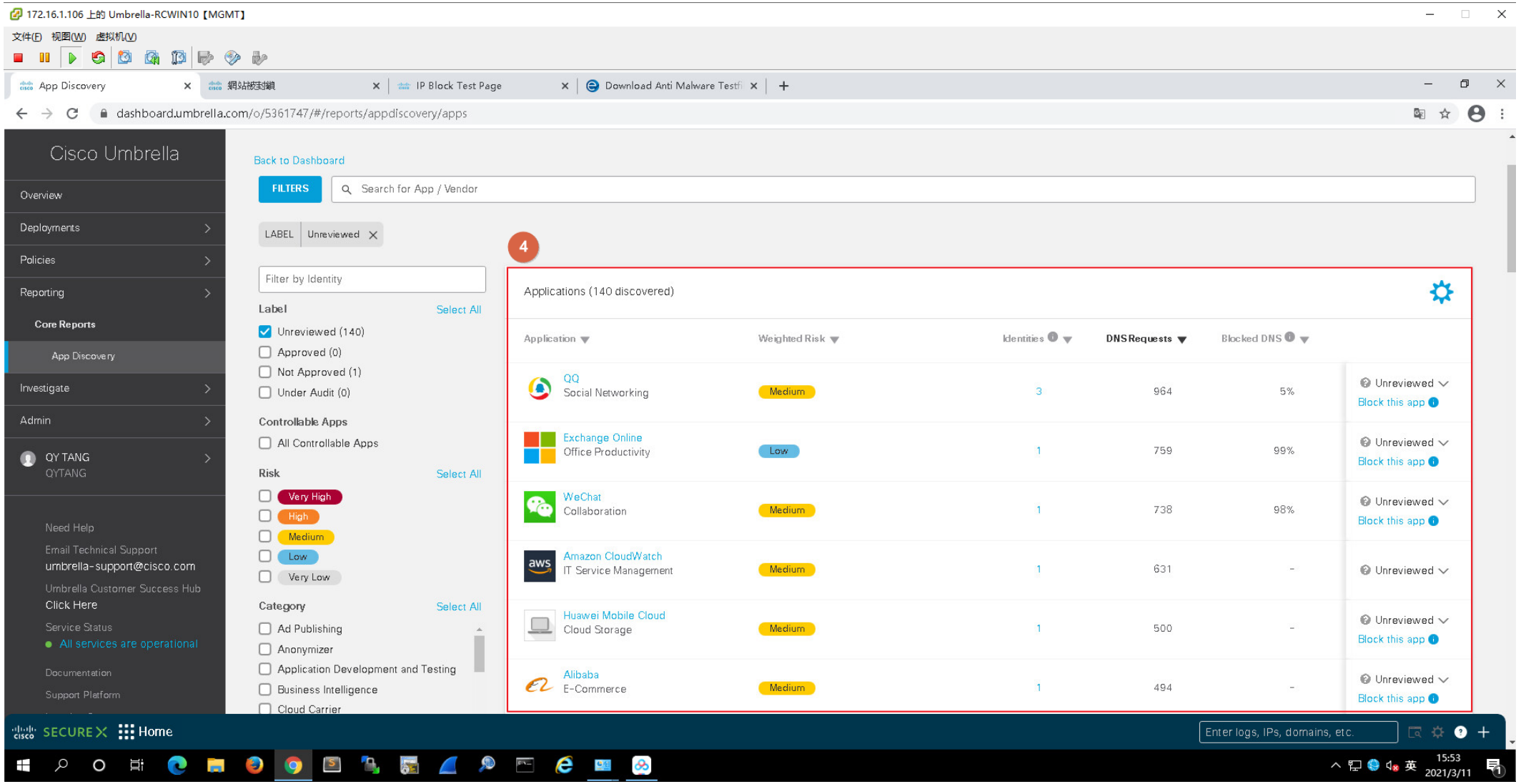
Cisco Umbrella测试（8）



Cisco Umbrella测试（9）



Cisco Umbrella测试（9）



Cisco Umbrella测试（10）