Cisco Secure Firewall ASA-防火墙服务

防火墙服务是指专注于控制网络访问的ASA功能，包括阻止流量的服务和在内外部网络之间启用流量数据流的服务。这些服务包括保护网络免受威胁（例如拒绝服务 [DoS] 及其他攻击）的服务。

以下主题概括介绍防火墙服务。

如何实施防火墙服务

以下操作步骤介绍实施防火墙服务的通用顺序。但每个步骤都是可选步骤，只有在您要为网络提供该服务时才需要使用。

开始之前

根据一般操作配置指南配置 ASA，包括最低基本设置、接口配置、路由和管理访问。

过程

步骤 1 实施网络访问控制。请参阅基本访问控制， 第 2 页。

步骤 2 实施 URL 过滤。请参阅URL 过滤， 第 2 页。

步骤 3 实施威胁防范。请参阅威胁防范， 第 2 页。

步骤 4 实施为虚拟环境定制的防火墙服务。请参阅面向虚拟环境的防火墙服务， 第 3 页。

步骤 5 实施网络地址转换 (NAT)。请参阅网络地址转换， 第 3 页。

步骤 6 实施应用检测（如果默认设置不能满足网络要求）。请参阅应用检测，第 4 页。

基本访问控制

访问规则是第一道防线，按接口或全局进行应用。可以在特定类型的流量进入后丢弃该流量，或者丢弃流出（或流入）特定主机或网络的流量。默认情况下，ASA 允许流量从内部网络（较高安全性级别）自由流向外部网络（较低安全性级别）。

可以应用访问规则，以限制从内部到外部的流量，或者允许从外部到内部的流量。

基本访问规则使用“5 元组”的源地址和端口、目标地址和端口以及协议控制流量。请参阅访问规则 和 访问控制列表。

可以通过对规则进行身份感知来扩充规则。要实施身份控制，请在单独的服务器上安装 Cisco Identity Services Engine (ISE)，以实施思科 Trustsec。然后，可以向访问规则添加安全组条件。请参阅 ASA 和思科 TrustSec。

URL 过滤

URL 过滤根据目标站点的 URL 拒绝或允许流量。

要实施 URL 过滤，请订用 Cisco Umbrellaa 服务，您将在其中配置企业安全策略基于完全限定域名 (FQDN) 来阻止恶意站点。对于被视为可疑的 FQDN，您可以将用户连接重定向至执行 URL 过滤的思科 Umbrella 智能代理。Umbrella 服务通过处理用户的 DNS 查询请求，返回阻止页面的 IP 地址或智能代理的 IP 地址发挥作用。该服务将为允许的域返回 FQDN 的真实 IP 地址。请参阅思科 Umbrella。

威胁防范

可以执行许多措施，来防御扫描、拒绝服务 (DoS) 及其他攻击。许多 ASA 功能可通过应用连接限制和丢弃异常 TCP 数据包来帮助防御攻击。某些功能是自动功能，某些功能可配置，但具有大多数情况下适用的默认设置，而其他功能则完全可选，如果要使用这些可选功能，必须进行配置。

下面是 ASA 中可用的威胁防范服务。

- IP 数据包分段保护 - ASA 完全重组所有 ICMP 错误消息，并虚拟重组通过 ASA 路由的剩余 IP 网段，丢弃未通过安全检查的网段。无需进行配置。

- 连接限制、TCP 规范化及其他连接相关的功能 - 配置连接相关的服务，例如 TCP 和 UDP 连接限制与超时、TCP 序列号随机化、TCP 规范化以及 TCP 状态绕行。TCP 规范化旨在丢弃出现异常的数据包。请参阅连接设置。

  例如，可以限制 TCP 和 UDP 连接及初期连接（源与目标之间尚未完成必要握手的连接请求）。限制连接和半开连接的数量可防止遭受 DoS 攻击。ASA 通过限制初期连接的数量来触发 TCP 拦截，从而防止内部系统受到 DoS 攻击（这种攻击使用 TCP SYN 数据包对接口发起泛洪攻击）。

- 威胁检测 - 在 ASA 上实施威胁检测，以便收集统计信息来帮助识别攻击。默认情况下启用基本威胁检测，但您可以实施高级统计和扫描威胁检测功能。可以避开标识为扫描威胁的主机。请参阅威胁检测。

面向虚拟环境的防火墙服务

虚拟环境将服务器部署为虚拟机，例如在 VMware ESXi 中。虚拟环境中的防火墙可以是传统硬件设备，也可以是虚拟机防火墙，例如 ASA Virtual。

传统和下一代防火墙服务应用于虚拟环境的方式与其应用于不使用虚拟机服务器的环境的方式相同。不过，因为在虚拟环境下易于创建和断开服务器，虚拟环境可提供更多挑战。

此外，数据中心内服务器之间的流量可能同数据中心与外部用户之间的流量需要相同程度的保护。例如，如果攻击者控制了数据中心内的某台服务器，则可能会对该数据中心的其他服务器发起攻击。

虚拟环境的防火墙服务添加了专门面向虚拟机应用防火墙保护的功能。下面是可用于虚拟环境的防火墙服务：

- 基于属性的访问控制 - 您可以将网络对象配置为基于属性匹配流量，并在访问控制规则中使用这些对象。这样便可以从网络拓扑中将防火墙规则分离出来。例如，您可以允许具有 Engineering 属性的所有主机访问具有 Lab Server 属性的主机。然后，可以添加/删除具有这些属性的主机并自动应用防火墙策略，而无需更新访问规则。有关详细信息，请参阅基于属性的访问控制。

网络地址转换

网络地址转换 (NAT) 的主要功能之一是使专用 IP 网络可以连接到互联网。NAT 用公用 IP 地址替换专用 IP 地址，将内部专用网络中的专用地址转换为可在公用互联网上使用的合法可路由地址。通过这种方式，NAT 即可保存公用地址，因为您至少可以为整个网络向外部网络通告一个公用地址。

NAT 的其他功能包括：

- 安全 - 隐藏内部 IP 地址可以阻止直接攻击。
- IP 路由解决方案 - 使用 NAT 时不会出现重叠 IP 地址。
- 灵活性 - 可以更改内部 IP 寻址方案，而不影响外部的可用公用地址；例如，对于可以访问互联网的服务器，可以维护供互联网使用的固定 IP 地址，但在内部，可以更改服务器地址。
- 在 IPv4 和 IPv6 之间转换（仅路由模式）- 如果想将 IPv6 网络连接到 IPv4 网络，可以利用 NAT 在两种类型的地址之间转换。

不需要 NAT。如果不为一组给定流量配置 NAT，将不转换这些流量，但会正常应用所有安全策略。

请参阅：

- 网络地址转换 (NAT)
- NAT 示例和参考

应用检测

对于在用户数据包中嵌入 IP 寻址信息的服务或在动态分配端口上打开辅助信道的服务，需要使用应用检测引擎。这些协议需要 ASA 执行深度数据包检测，以便打开所需的针孔及应用网络地址转换 (NAT)。

默认 ASA 策略已对许多常见协议（例如 DNS、FTP、SIP、ESMTP、TFTP 等）全局应用检测。默认检测可能满足您对网络的所有需求。

但是，您可能需要启用其他协议的检测，或者优化检测。许多检测都包含详细的选项，您可以根据这些选项的内容来控制数据包。如果非常熟悉某个协议，可以对该流量应用精细控制。

使用服务策略配置应用检测。可以配置全局服务策略，还可以向每个接口应用服务策略，或者同时使用这两种方式。

请参阅：

- 服务策略
- 应用层协议检测入门
- 基本互联网协议检测
- 语音和视频协议检测
- 移动网络检测。

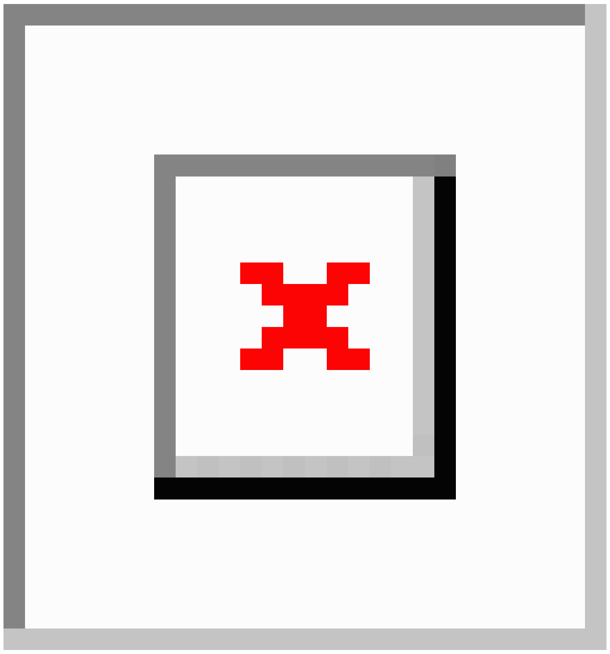
应用场景：面向公众显示服务器

可以在公共网络上显示服务器上的某些应用服务。例如，可以开放 Web 服务器，以便用户可以连接到网页，但不与服务器建立任何其他连接。

要在公共网络上开放服务器，通常需要创建允许连接和 NAT 规则的访问规则，以在服务器的内部 IP 地址与公共网络可以使用的外部地址之间转换。此外，如果不希望外部开放的服务使用与内部服务器相同的端口，可以使用端口地址转换 (PAT) 将内部端口映射到外部端口。例如，如果内部 Web 服务器不在 TCP/80 上运行，可以将其映射到 TCP/80，以方便外部用户进行连接。

以下示例实现了内部专用网络上某台 Web 服务器的公共访问。

图 *1:* 面向内部 ***Web*** 服务器的静态 ***NAT***



过程

步骤 1 为内部 Web 服务器创建网络对象。

```
hostname(config)# object network myWebServ
hostname(config-network-object)# host 10.1.2.27
```

步骤 2 配置对象的静态 NAT：

```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10
```

步骤 3 向与外部接口关联的访问组添加访问规则，以允许对服务器进行 Web 访问。

```
hostname(config)# access-list outside_access_in line 1 extended
permit tcp any4 object myWebServ eq http
```

步骤 4 如果外部接口上没有访问组，请使用 access-group 命令应用该访问组：

```
hostname(config)# access-group outside_access_in in interface outside
```

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。