Schutz des Kerns: Zugriffskontrolllisten für Infrastrukturschutz

Inhalt

[Einführung](#)
[Infrastrukturschutz](#)
[Hintergrund](#)
[Techniken](#)
[ACL-Beispiele](#)
[Entwicklung einer Schutz-ACL](#)
[ACLs und fragmentierte Pakete](#)
[Risikobewertung](#)
[Anhänge](#)
[Unterstützte IP-Protokolle in der Cisco IOS-Software](#)
[Bereitstellungsrichtlinien](#)
[Bereitstellungsbeispiele](#)
[Zugehörige Informationen](#)

Einführung

Dieses Dokument enthält Richtlinien und empfohlene Bereitstellungsverfahren für Zugriffskontrolllisten (ACLs) zum Schutz der Infrastruktur. Infrastruktur-ACLs werden verwendet, um das Risiko und die Effektivität direkter Infrastrukturangriffe zu minimieren, indem explizit nur autorisierter Datenverkehr zu den Infrastrukturgeräten zugelassen und der gesamte andere Datenverkehr zugelassen wird.

Infrastrukturschutz

Hintergrund

Um Router vor verschiedenen Risiken - sowohl vor zufälliger als auch vor böswilliger - zu schützen, sollten Infrastrukturschutz-ACLs an den Netzwerk-Eingangspunkten bereitgestellt werden. Diese IPv4- und IPv6-ACLs verweigern den Zugriff von externen Quellen auf alle Infrastrukturadressen, z. B. Router-Schnittstellen. Gleichzeitig ermöglichen die ACLs einen unterbrechungsfreien Datenverkehr bei der Routine-Übertragung und bieten eine grundlegende RFC 1918 -, RFC 3330 - und Anti-Spoof-Filterung.

Die von einem Router empfangenen Daten können in zwei große Kategorien unterteilt werden:

- Datenverkehr, der über den Weiterleitungspfad durch den Router geleitet wird
- Datenverkehr, der für den Router über den Empfangspfad für die

Routingprozessorbehandlung bestimmt ist

Im Normalbetrieb fließt der Großteil des Datenverkehrs einfach über einen Router bis zum endgültigen Ziel.

Der Routingprozessor (RP) muss jedoch bestimmte Datentypen direkt verarbeiten, insbesondere Routing-Protokolle, Remote-Router-Zugriff (z. B. Secure Shell [SSH]) und Netzwerkmanagement-Datenverkehr wie Simple Network Management Protocol (SNMP). Darüber hinaus können Protokolle wie das Internet Control Message Protocol (ICMP) und IP-Optionen eine direkte Verarbeitung durch den RP erfordern. Häufig ist der direkte Zugriff auf Infrastruktur-Router nur von internen Quellen aus erforderlich. Zu den wichtigsten Ausnahmen gehören externes Border Gateway Protocol (BGP)-Peering, Protokolle, die auf dem eigentlichen Router enden (z. B. Generic Routing Encapsulation [GRE] oder IPv6 over IPv4-Tunnel), und möglicherweise eingeschränkte ICMP-Pakete für Verbindungstests wie Echoanfrage oder ICMP Unreachables und Time to Live (TTL)-abgelaufene Nachrichten für Traceroute.

Hinweis: Beachten Sie, dass ICMP häufig für einfache DoS-Angriffe (Denial-of-Service) verwendet wird und nur bei Bedarf von externen Quellen zugelassen werden sollte.

Alle RPs verfügen über einen Leistungsrahmen, in dem sie arbeiten. Der Router kann durch übermäßigen Datenverkehr, der für den RP bestimmt ist, überfordert werden. Dies führt zu einer hohen CPU-Auslastung und letztendlich zu einem Ausfall des Paket- und Routing-Protokolls, was zu einer Diensteverweigerung führt. Durch die Filterung des Zugriffs auf Infrastruktur-Router von externen Quellen werden viele der externen Risiken, die mit einem direkten Router-Angriff verbunden sind, verringert. Externe Angriffe können nicht mehr auf Infrastrukturgeräte zugreifen. Der Angriff wird auf Eingangs-Schnittstellen in das autonome System (AS) verworfen.

Die in diesem Dokument beschriebenen Filtertechniken dienen zum Filtern von Daten für Netzwerkinfrastrukturgeräte. Verwechseln Sie nicht die Infrastrukturfilterung mit einer allgemeinen Filterung. Die Zugriffskontrollliste für den Infrastrukturschutz soll genau festlegen, welche Protokolle und Quellen auf kritische Infrastrukturgeräte zugreifen dürfen.

Netzwerkinfrastrukturgeräte umfassen folgende Bereiche:

- Alle Router- und Switch-Managementadressen, einschließlich Loopback-Schnittstellen
- Alle internen Verbindungsadressen: Router-zu-Router-Verbindungen (Point-to-Point und Mehrfachzugriff)
- Interne Server oder Dienste, auf die nicht von externen Quellen zugegriffen werden sollte

In diesem Dokument wird der gesamte Verkehr, der nicht für die Infrastruktur bestimmt ist, häufig als Transitverkehr bezeichnet.

Techniken

Der Schutz der Infrastruktur kann durch eine Vielzahl von Techniken erreicht werden:

- **Empfangen von ACLs (rACLs)**Die Cisco 12000- und 7500-Plattformen unterstützen rACLs, die den gesamten für den RP bestimmten Datenverkehr filtern und den Transitverkehr nicht beeinträchtigen. Autorisierter Datenverkehr muss explizit zugelassen werden, und die rACL muss auf jedem Router bereitgestellt werden. Siehe GSR: Erhalten Sie Zugriffskontrolllisten für weitere Informationen.
- **Hop-by-Hop-Router-ACLs**Router können auch durch die Definition von ACLs geschützt werden, die nur autorisierten Datenverkehr zu den Schnittstellen des Routers zulassen. Alle

anderen Router außer dem Transit-Datenverkehr, der explizit zugelassen werden muss, werden abgelehnt. Diese ACL ähnelt logisch einer rACL, wirkt sich jedoch auf den Transitverkehr aus und kann daher negative Auswirkungen auf die Weiterleitungsrate eines Routers haben.

- **Edge-Filterung über Infrastruktur-ACLs**ACLs können am Netzwerk-Edge angewendet werden. Bei einem Service Provider (SP) ist dies der Edge des AS. Diese ACL filtert explizit den Datenverkehr, der für den Adressbereich der Infrastruktur bestimmt ist. Bei der Bereitstellung von Edge-Infrastruktur-ACLs müssen Sie den Infrastrukturraum und die erforderlichen/autorisierten Protokolle für den Zugriff auf diesen Bereich klar definieren. Die ACL wird beim Eingang in Ihr Netzwerk auf alle externen Verbindungen angewendet, z. B. Peering-Verbindungen, Kundenverbindungen usw.Im Mittelpunkt dieses Dokuments stehen die Entwicklung und Bereitstellung von Edge-Infrastrukturschutz-ACLs.

ACL-Beispiele

Diese IPv4- und IPv6-Zugriffslisten bieten einfache aber realistische Beispiele für typische Einträge, die für eine Schutz-ACL erforderlich sind. Diese grundlegenden ACLs müssen mit lokalen, standortspezifischen Konfigurationsdetails angepasst werden. In dualen IPv4- und IPv6-Umgebungen werden beide Zugriffslisten bereitgestellt.

IPv4-Beispiel

```
!--- Anti-spoofing entries are shown here. !--- Deny special-use address sources. !--- Refer to
RFC 3330 for additional special use addresses. access-list 110 deny ip host 0.0.0.0 any access-
list 110 deny ip 127.0.0.0 0.255.255.255 any access-list 110 deny ip 192.0.2.0 0.0.0.255 any
access-list 110 deny ip 224.0.0.0 31.255.255.255 any !--- Filter RFC 1918 space. access-list 110
deny ip 10.0.0.0 0.255.255.255 any access-list 110 deny ip 172.16.0.0 0.15.255.255 any access-
list 110 deny ip 192.168.0.0 0.0.255.255 any !--- Deny your space as source from entering your
AS. !--- Deploy only at the AS edge. access-list 110 deny ip YOUR_CIDR_BLOCK any !--- Permit
BGP. access-list 110 permit tcp host bgp_peer host router_ip eq bgp access-list 110 permit tcp
host bgp_peer eq bgp host router_ip !--- Deny access to internal infrastructure addresses.
access-list 110 deny ip any INTERNAL_INFRASTRUCTURE_ADDRESSES !--- Permit transit traffic.
access-list 110 permit ip any any
```

IPv6-Beispiel

Die IPv6-Zugriffsliste muss als erweiterte, benannte Zugriffsliste angewendet werden.

```
!--- Configure the access-list. ipv6 access-list iacl !--- Deny your space as source from
entering your AS. !--- Deploy only at the AS edge. deny ipv6 YOUR_CIDR_BLOCK_IPV6 any !---
Permit multiprotocol BGP. permit tcp host bgp_peer_ipv6 host router_ipv6 eq bgp permit tcp host
bgp_peer_ipv6 eq bgp host router_ipv6 !--- Deny access to internal infrastructure addresses.
deny ipv6 any INTERNAL_INFRASTRUCTURE_ADDRESSES_IPV6 !--- Permit transit traffic. permit ipv6
any any
```

Hinweis: Das **log-**Schlüsselwort kann verwendet werden, um zusätzliche Details über Quelle und Ziele für ein bestimmtes Protokoll bereitzustellen. Obwohl dieses Schlüsselwort wertvolle Einblicke in die Details von ACL-Treffern bietet, können übermäßige Treffer auf einen ACL-Eintrag, der das **log-**Schlüsselwort verwendet, die CPU-Auslastung erhöhen. Die Auswirkungen der Protokollierung auf die Leistung variieren je nach Plattform. Darüber hinaus deaktiviert die Verwendung des Schlüsselworts log das Cisco Express Forwarding (CEF)-Switching für Pakete, die der Anweisung der Zugriffsliste entsprechen. Diese Pakete werden stattdessen schnell geswitcht.

Entwicklung einer Schutz-ACL

Eine Infrastruktur-ACL besteht im Allgemeinen aus vier Abschnitten:

- Adressen- und Anti-Spoofing-Einträge für spezielle Zwecke, die verhindern, dass unberechtigte Quellen und Pakete mit Quelladressen, die in Ihrem AS enthalten sind, von einer externen Quelle in das AS gelangen**Hinweis:** RFC 3330 definiert IPv4-spezielle Verwendungsadressen, die ggf. gefiltert werden müssen. RFC 1918 definiert reservierten IPv4-Adressbereich, der keine gültige Quelladresse im Internet ist. RFC 3513 definiert die IPv6-Adressierungsarchitektur. RFC 2827 bietet Richtlinien für die Eingangsfilterung.
- Explizit erlaubter extern erfasster Datenverkehr, der an Infrastrukturadressen gerichtet ist
- **Ablehnen** von Aussagen für alle anderen extern bezogenen Datenverkehr an Infrastrukturadressen
- **permit**-Anweisungen für den gesamten anderen Datenverkehr für normalen Backbone-Datenverkehr auf Weiterleitung an Nicht-Infrastrukturziele

Die letzte Zeile der Infrastruktur-ACL erlaubt explizit den Transitverkehr: **ip any any any** for IPv4 und **permit ipv6 any any** for IPv6. Dieser Eintrag stellt sicher, dass alle IP-Protokolle über den Core hinweg zulässig sind und dass Kunden weiterhin problemlos Anwendungen ausführen können.

Der erste Schritt bei der Entwicklung einer Zugriffskontrollliste für den Infrastrukturschutz besteht darin, die erforderlichen Protokolle zu verstehen. Obwohl jeder Standort spezifische Anforderungen hat, werden in der Regel bestimmte Protokolle bereitgestellt und müssen verstanden werden. Externes BGP an externe Peers muss beispielsweise explizit zugelassen werden. Alle anderen Protokolle, die einen direkten Zugriff auf den Infrastruktur-Router erfordern, müssen ebenfalls explizit zugelassen werden. Wenn Sie beispielsweise einen GRE-Tunnel auf einem Core-Infrastruktur-Router beenden, muss auch Protokoll 47 (GRE) explizit zugelassen werden. Wenn Sie einen IPv6 over IPv4-Tunnel auf einem Core-Infrastruktur-Router terminieren, muss auch Protokoll 41 (IPv6 over IPv4) explizit zugelassen werden.

Mithilfe einer Klassifizierungs-ACL können die erforderlichen Protokolle identifiziert werden. Die Klassifizierungs-ACL besteht aus Genehmigungsanweisungen für die verschiedenen Protokolle, die für einen Infrastruktur-Router bestimmt sein können. Eine vollständige Liste finden Sie im Anhang zu unterstützten IP-Protokollen in der Cisco IOS® Software. Die Verwendung des Befehls **show access-list**, um die Anzahl der ACE-Treffer (Access Control Entry) anzuzeigen, identifiziert erforderliche Protokolle. Verdächtige oder überraschende Ergebnisse müssen untersucht und verstanden werden, bevor Sie für unerwartete Protokolle **zulässige** Anweisungen erstellen.

Diese IPv4-ACL beispielsweise hilft zu bestimmen, ob GRE-, IPsec (ESP)- und IPv6-Tunneling (IP Protocol 41) zugelassen werden müssen.

```
access-list 101 permit GRE any infrastructure_ips
access-list 101 permit ESP any infrastructure_ips
access-list 101 permit 41 any infrastructure_ips
access-list 101 permit ip any infrastructure_ips log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted.

access-list 101 permit ip any any

interface <int>
 ip access-group 101 in
```

Mit dieser IPv6-ACL kann bestimmt werden, ob GRE und IPsec (ESP) zugelassen werden müssen.

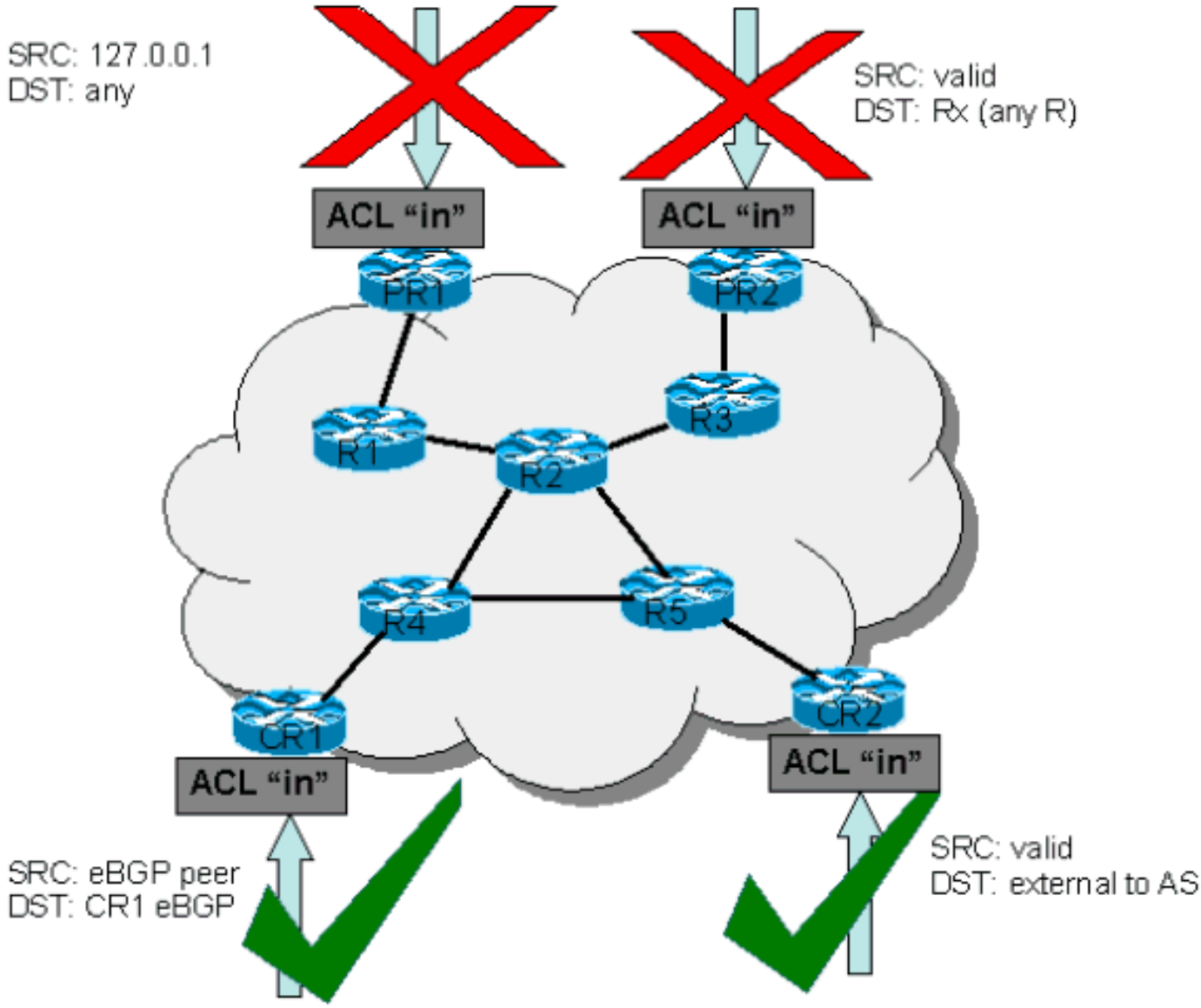
```
ipv6 access-list determine_protocols
 permit GRE any infrastructure_ips_ipv6
 permit ESP any infrastructure_ips_ipv6
 permit ipv6 any infrastructure_ips_ipv6 log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted. permit ipv6 any any interface <int> ipv6 traffic-filter determine_protocols in
```

Neben den erforderlichen Protokollen muss auch der Adressraum der Infrastruktur identifiziert werden, da dies der von der ACL geschützte Bereich ist. Der Adressbereich der Infrastruktur umfasst alle Adressen, die für das interne Netzwerk verwendet werden und selten von externen Quellen wie Routerschnittstellen, Point-to-Point-Links-Adressierung und kritischen Infrastrukturservices genutzt werden. Da diese Adressen für den Zielteil der Infrastruktur-ACL verwendet werden, ist eine Zusammenfassung von entscheidender Bedeutung. Diese Adressen müssen, soweit möglich, in CIDR-Blöcken (Classless Interdomain Routing) gruppiert werden.

Mithilfe der identifizierten Protokolle und Adressen kann die Infrastruktur-ACL so erstellt werden, dass die Protokolle zugelassen und die Adressen geschützt werden. Neben dem direkten Schutz bietet die ACL auch eine erste Verteidigungslinie gegen bestimmte Typen von ungültigem Datenverkehr im Internet.

- Der RFC 1918-Platzhalter muss abgelehnt werden.
- Pakete mit einer Quelladresse, die in den in RFC 330 definierten Adressbereich für spezielle Zwecke fallen, müssen abgelehnt werden.
- Anti-Spoof-Filter müssen angewendet werden. (Der Adressbereich darf nie die Quelle für Pakete von außerhalb Ihres AS sein.)

Diese neu erstellte ACL muss eingehend auf alle Eingangsschnittstellen angewendet werden. Weitere Informationen finden Sie in den Abschnitten zu Bereitstellungsrichtlinien und Bereitstellungsbeispielen.



ACLs und fragmentierte Pakete

ACLs verfügen über ein **fragments**-Schlüsselwort, das ein spezialisiertes, fragmentiertes Paketverarbeitungsverhalten ermöglicht. Ohne dieses **fragments**-Schlüsselwort werden nicht initiale Fragmente, die den Layer-3-Anweisungen (unabhängig von den Layer-4-Informationen) in einer ACL entsprechen, durch die permit or deny-Anweisung des übereinstimmenden Eintrags beeinflusst. Wenn Sie jedoch das **fragments**-Schlüsselwort hinzufügen, können Sie ACLs zwingen, nicht initiale Fragmente mit höherer Genauigkeit abzulehnen oder zuzulassen. Dieses Verhalten ist für IPv4- und IPv6-Zugriffslisten gleich, mit der Ausnahme, dass IPv4-ACLs zwar die Verwendung des Fragments-Schlüsselworts in Layer-3- und Layer-4-Anweisungen zulassen, IPv6-ACLs jedoch nur die Verwendung des Fragments-Schlüsselworts in Layer-3-Anweisungen zulassen.

Die Filterung von Fragmenten bietet eine zusätzliche Schutzebene gegen DoS-Angriffe (Denial of Service), bei denen nicht initiale Fragmente (d. h. FO > 0) verwendet werden. Die Verwendung einer **deny-**Anweisung für nicht initiale Fragmente am Anfang der ACL verhindert, dass nicht initiale Fragmente auf den Router zugreifen. In seltenen Fällen kann eine gültige Sitzung fragmentiert werden, sodass sie gefiltert wird, wenn eine **deny fragment-**Anweisung in der ACL vorhanden ist.

Betrachten Sie zum Beispiel folgende partielle IPv4ACL:

```
access-list 110 deny tcp any infrastructure_IP fragments
access-list 110 deny udp any infrastructure_IP fragments
access-list 110 deny icmp any infrastructure_IP fragments
<rest of ACL>
```

Durch Hinzufügen dieser Einträge zu Beginn einer ACL wird der nicht initiale Fragmentzugriff auf die Core-Router verweigert, während nicht fragmentierte Pakete oder anfängliche Fragmente an die nächsten Zeilen der ACL weitergeleitet werden, die von den **deny-Fragment-**Anweisungen nicht beeinflusst werden. Der vorangehende ACL-Befehl erleichtert außerdem die Klassifizierung des Angriffs, da jedes Protokoll - Universal Datagram Protocol (UDP), TCP und ICMP - separate Zähler in der ACL erhöht.

Dies ist ein vergleichbares Beispiel für IPv6:

```
ipv6 access-list iacl
   deny ipv6 any infrastructure_IP fragments
```

Wenn dieser Eintrag zu Beginn einer IPv6-ACL hinzugefügt wird, wird der nicht initiale Fragmentzugriff auf die Core-Router verweigert. Wie bereits erwähnt, erlauben IPv6-Zugriffslisten nur die Verwendung des Fragments-Schlüsselworts in Layer-3-Anweisungen.

Da viele Angriffe auf Flooding-Core-Router mit fragmentierten Paketen angewiesen sind, bietet das Filtern eingehender Fragmente in die Core-Infrastruktur einen zusätzlichen Schutz und hilft sicherzustellen, dass ein Angriff keine Fragmente infizieren kann, indem er einfach die Layer-3-Regeln in der Infrastruktur-ACLs vergleicht.

Unter Zugriffskontrolllisten und IP-Fragmente finden Sie eine ausführliche Erläuterung der Optionen.

Risikobewertung

Bei der Bereitstellung von Zugriffskontrolllisten für den Infrastrukturschutz sind folgende zwei Bereiche von besonderem Risiko zu berücksichtigen:

- Stellen Sie sicher, dass die entsprechenden **Zulassungs-/Ablehnungsanweisungen** vorhanden sind. Damit die Zugriffskontrollliste wirksam ist, müssen alle erforderlichen Protokolle zugelassen und der richtige Adressbereich durch die **deny-**Anweisungen geschützt werden.
- Die ACL-Leistung variiert von Plattform zu Plattform. Überprüfen Sie die Leistungsmerkmale Ihrer Hardware, bevor Sie ACLs bereitstellen.

Wie immer wird empfohlen, dieses Design vor der Bereitstellung in der Übung zu testen.

Anhänge

Unterstützte IP-Protokolle in der Cisco IOS-Software

Diese IP-Protokolle werden von der Cisco IOS-Software unterstützt:

- 1 - ICMP
- 2 - IGMP
- 3 - GGP
- 4 - IP in IP-Kapselung
- 6 - TCP
- 8 - EGP
- 9 - IGRP
- 17 - UDP
- 20 - HMP
- 27 - RDP
- 41 - IPv6-in-IPv4-Tunneling
- 46 - RSVP
- 47 - GRE
- 50 - ESP
- 51 - AH
- 53 - SWIPE
- 54 - NARP
- 55 - IP-Mobilität
- 63 - jedes lokale Netzwerk
- 77 - Sun ND
- 80 - ISO IP
- 88 - EIGRP
- 89 - OSPF
- 90 - Sprite RPC
- 91 - LARP
- 94 - KA9Q/NOS-kompatible IP over IP
- 103 - PIM
- 108 - IP-Komprimierung
- 112 - VRRP
- 113 - GVO
- 115 - L2TP
- 120 - UTI
- 132 - SCTP

Bereitstellungsrichtlinien

Cisco empfiehlt konservative Bereitstellungsverfahren. Um Infrastruktur-ACLs erfolgreich bereitstellen zu können, müssen die erforderlichen Protokolle genau verstanden und der Adressbereich klar identifiziert und definiert werden. Diese Richtlinien beschreiben eine sehr konservative Methode für die Bereitstellung von Schutz-ACLs mithilfe eines iterativen Ansatzes.

1. **Identifizieren Sie im Netzwerk verwendete Protokolle mit einer Klassifizierungs-ACL.**Stellen Sie eine ACL bereit, die alle bekannten Protokolle zulässt, die auf Infrastrukturgeräte zugreifen. Diese Erkennungs-ACL verfügt über eine Quell-Adresse für **beliebige** Adressen und ein Ziel, das den Infrastruktur-IP-Raum umfasst. Die Protokollierung kann verwendet werden, um eine Liste von Quelladressen zu entwickeln, die den **zulässigen** Protokollanweisungen entsprechen. Eine letzte Zeile, die **IP any any** (IPv4) oder **ipv6 any** (IPv6) ermöglicht, ist erforderlich, um den Datenverkehrsfluss zu ermöglichen.Ziel ist es zu

bestimmen, welche Protokolle das spezifische Netzwerk verwendet. Die Protokollierung dient der Analyse, um festzustellen, was sonst mit dem Router kommuniziert.**Hinweis:** Obwohl das **log-**Schlüsselwort wertvolle Einblicke in die Details von ACL-Treffern bietet, können übermäßige Zugriffe auf einen ACL-Eintrag, der dieses Schlüsselwort verwendet, zu einer überwältigenden Anzahl von Protokolleinträgen und möglicherweise zu einer hohen CPU-Nutzung des Routers führen. Darüber hinaus deaktiviert die Verwendung des **log-**Schlüsselworts das Cisco Express Forwarding (CEF)-Switching für Pakete, die der Zugriffslistenanweisung entsprechen. Diese Pakete werden stattdessen schnell geswitcht. Verwenden Sie das **log-**Schlüsselwort für kurze Zeiträume und nur, wenn dies zur Klassifizierung des Datenverkehrs erforderlich ist.

2. **Überprüfen Sie identifizierte Pakete und beginnen Sie, den Zugriff auf den Routingprozessor-RP zu filtern.**Nachdem die in Schritt 1 von der ACL gefilterten Pakete identifiziert und geprüft wurden, stellen Sie eine ACL mit der **Genehmigung** einer **beliebigen Quelle** für Infrastrukturadressen der zulässigen Protokolle bereit. Wie in Schritt 1 kann das **log-**Schlüsselwort weitere Informationen zu Paketen bereitstellen, die den **permit-**Einträgen entsprechen. Die Verwendung von **Deny Any** am Ende kann dabei helfen, unerwartete Pakete zu identifizieren, die für die Router bestimmt sind. Bei der letzten Zeile dieser ACL muss es sich um eine **permit ip any** (IPv4) oder **permit ipv6 any** (IPv6) statement handeln, um den Fluss des Transitverkehrs zu ermöglichen. Diese ACL bietet grundlegenden Schutz und ermöglicht es Netzwerktechnikern, sicherzustellen, dass der gesamte erforderliche Datenverkehr zulässig ist.
3. **Quelladressen einschränken.**Sobald Sie die Protokolle, die zugelassen werden müssen, verstanden haben, können weitere Filter durchgeführt werden, um nur autorisierte Quellen für diese Protokolle zuzulassen. Beispielsweise können Sie externe BGP-Nachbarn oder bestimmte GRE-Peer-Adressen explizit zulassen.Mit diesem Schritt wird das Risiko verringert, ohne dass Services unterbrochen werden, und Sie können eine präzise Kontrolle auf Quellen anwenden, die auf Ihre Infrastrukturgeräte zugreifen.
4. **Begrenzen Sie die Zieladressen auf der ACL. (*optional*)**Einige Internet-Service-Provider (ISP) entscheiden sich möglicherweise dafür, bestimmten Protokollen die Verwendung bestimmter Zieladressen auf dem Router zu gestatten. Diese letzte Phase soll den Bereich der Zieladressen begrenzen, die Datenverkehr für ein Protokoll akzeptieren können.

Bereitstellungsbeispiele

IPv4-Beispiel

Dieses IPv4-Beispiel zeigt eine Infrastruktur-ACL zum Schutz eines Routers, der auf der folgenden Adressierung basiert:

- Der ISP-Adressblock lautet 169.223.0.0/16.
- Der ISP-Infrastrukturblock lautet 169.223.252.0/22.
- Das Loopback für den Router lautet 169.223.253.1/32.
- Der Router ist ein Peering-Router und Peers mit 169.254.254.1 (für Adresse 169.223.252.1).

Die angezeigte Infrastruktur-Schutz-ACL wird auf der Grundlage der vorherigen Informationen entwickelt. Die ACL ermöglicht das externe BGP-Peering zum externen Peer, bietet Anti-Spoof-Filter und schützt die Infrastruktur vor jeglichem externen Zugriff.

!

```
no access-list 110
!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 - Anti-spoofing Denies !--- These ACEs deny fragments, RFC 1918 space, !--- invalid
source addresses, and spoofs of !--- internal space (space as an external source).

!
!--- Deny fragments to the infrastructure block. access-list 110 deny tcp any 169.223.252.0
0.0.3.255 fragments access-list 110 deny udp any 169.223.252.0 0.0.3.255 fragments access-list
110 deny icmp any 169.223.252.0 0.0.3.255 fragments !--- Deny special-use address sources. !---
See RFC 3330 for additional special-use addresses. access-list 110 deny ip host 0.0.0.0 any
access-list 110 deny ip 127.0.0.0 0.255.255.255 any access-list 110 deny ip 192.0.2.0 0.0.0.255
any access-list 110 deny ip 224.0.0.0 31.255.255.255 any !--- Filter RFC 1918 space. access-list
110 deny ip 10.0.0.0 0.255.255.255 any access-list 110 deny ip 172.16.0.0 0.15.255.255 any
access-list 110 deny ip 192.168.0.0 0.0.255.255 any !--- Deny our internal space as an external
source. !--- This is only deployed at the AS edge access-list 110 deny ip 169.223.0.0
0.0.255.255 any !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 2 - Explicit Permit !--
- Permit only applications/protocols whose destination !--- address is part of the
infrastructure IP block. !--- The source of the traffic should be known and authorized.

!
!--- Note: This template must be tuned to the network's !--- specific source address
environment. Variables in !--- the template need to be changed.

!--- Permit external BGP. access-list 110 permit tcp host 169.254.254.1 host 169.223.252.1 eq
bgp access-list 110 permit tcp host 169.254.254.1 eq bgp host 169.223.252.1 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 - Explicit Deny to
Protect Infrastructure

access-list 110 deny ip any 169.223.252.0 0.0.3.255
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 4 - Explicit Permit for Transit Traffic

access-list 110 permit ip any any
```

IPv6-Beispiel

Dieses IPv6-Beispiel zeigt eine Infrastruktur-ACL zum Schutz eines Routers, der auf der folgenden Adressierung basiert:

- Der dem ISP zugewiesene gesamte Präfixblock ist 2001:0DB8:/32.
- Der vom ISP für Adressen der Netzwerkinfrastruktur verwendete IPv6-Präfixblock lautet 2001:0DB8:C18::/48.
- Es gibt einen BGP-Peering-Router mit der Quell-IPv6-Adresse 2001:0DB8:C18:2:1:1, der Peers auf die Ziel-IPv6-Adresse 2001:0DB8:C19:2:1::F stellt.

Die angezeigte Infrastruktur-Schutz-ACL wird auf der Grundlage der vorherigen Informationen entwickelt. Die ACL ermöglicht ein externes Multiprotocol-BGP-Peering mit dem externen Peer, bietet Anti-Spoof-Filter und schützt die Infrastruktur vor jeglichem externen Zugriff.

```
no ipv6 access-list iacl
ipv6 access-list iacl
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 - Anti-spoofing and Fragmentation Denies !--- These ACEs deny fragments and spoofs
of !--- internal space as an external source. !--- Deny fragments to the infrastructure block.
deny ipv6 any 2001:0DB8:C18::/48 fragments !--- Deny our internal space as an external source.
!--- This is only deployed at the AS edge. deny ipv6 2001:0DB8::/32 any
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 2 - Explicit Permit !--- Permit only
applications/protocols whose destination !--- address is part of the infrastructure IP block. !-
```

```
-- The source of the traffic should be known and authorized. !--- Note: This template must be
tuned to the !--- specific source address environment of the network. Variables in !--- the
template need to be changed. !--- Permit multiprotocol BGP. permit tcp host 2001:0DB8:C19:2:1::F
host 2001:0DB8:C18:2:1::1 eq bgp permit tcp host 2001:0DB8:C19:2:1::F eq bgp host
2001:0DB8:C18:2:1::1 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 –
Explicit Deny to Protect Infrastructure deny ipv6 any 2001:0DB8:C18::/48
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 4 – Explicit Permit for
Transit Traffic permit ipv6 any any
```

Zugehörige Informationen

- Support-Seite für Zugriffslisten
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems