GSR: Zugriffskontrolllisten empfangen

Inhalt

Einführung

In diesem Dokument wird eine neue Sicherheitsfunktion mit der Bezeichnung "Receive Access Control Lists (rACLs) [1]" beschrieben, und es werden Empfehlungen und Richtlinien für rACL-Bereitstellungen vorgestellt. Empfangszugriffskontrolllisten erhöhen die Sicherheit auf Cisco 1200-Routern, indem sie den Gigabit-Routingprozessor (GRP) des Routers vor unnötigem und potenziell schädlichem Datenverkehr schützen. Empfangszugriffskontrolllisten wurden als Sonderbefreiung zu der Wartungsdrosselung für die Cisco IOS ® Software Release 12.0.21S2 hinzugefügt und in Cisco IOS Software Release 12.0(22)S integriert.

GRP-Schutz

Die von einem Gigabit-Switch-Router (GSR) empfangenen Daten können in zwei große Kategorien unterteilt werden:

- Datenverkehr, der den Router über den Weiterleitungspfad passiert.
- Datenverkehr, der zur weiteren Analyse über den Empfangspfad an die GRP gesendet werden muss.

Im Normalbetrieb fließt der Großteil des Datenverkehrs einfach über einen GSR auf einer Route zu anderen Zielen. Die GRP muss jedoch bestimmte Datentypen verarbeiten, insbesondere Routing-Protokolle, Remote-Router-Zugriff und Netzwerkmanagement-Datenverkehr (z. B. Simple Network Management Protocol [SNMP]). Zusätzlich zu diesem Datenverkehr können andere Layer-3-Pakete die Verarbeitungsflexibilität des GRP erfordern. Dazu gehören bestimmte IP-Optionen und bestimmte Formen von ICMP-Paketen (Internet Control Message Protocol). Weitere Details zu rACLs und zum Empfangen von Pfaddatenverkehr im globalen Zugriffskontrolllisten

finden Sie im Anhang zum Empfang von Adjacencies und Paketen.

Ein Mitarbeiter der globalen Unterstützung verfügt über mehrere Datenpfade, von denen jeder verschiedene Datenverkehrsarten bedient. Der Transit-Datenverkehr wird von der Eingangs-Linecard (LC) an die Fabric und dann zur nächsten Hop-Bereitstellung an die Ausgangs-Karte weitergeleitet. Zusätzlich zum Datenpfad für den Transitverkehr verfügt ein GSR über zwei weitere Pfade für Datenverkehr, der eine lokale Verarbeitung erfordert: LC zu LC CPU und LC zu LC CPU zu Fabric zu GRP. Die folgende Tabelle zeigt die Pfade für mehrere häufig verwendete Features und Protokolle.

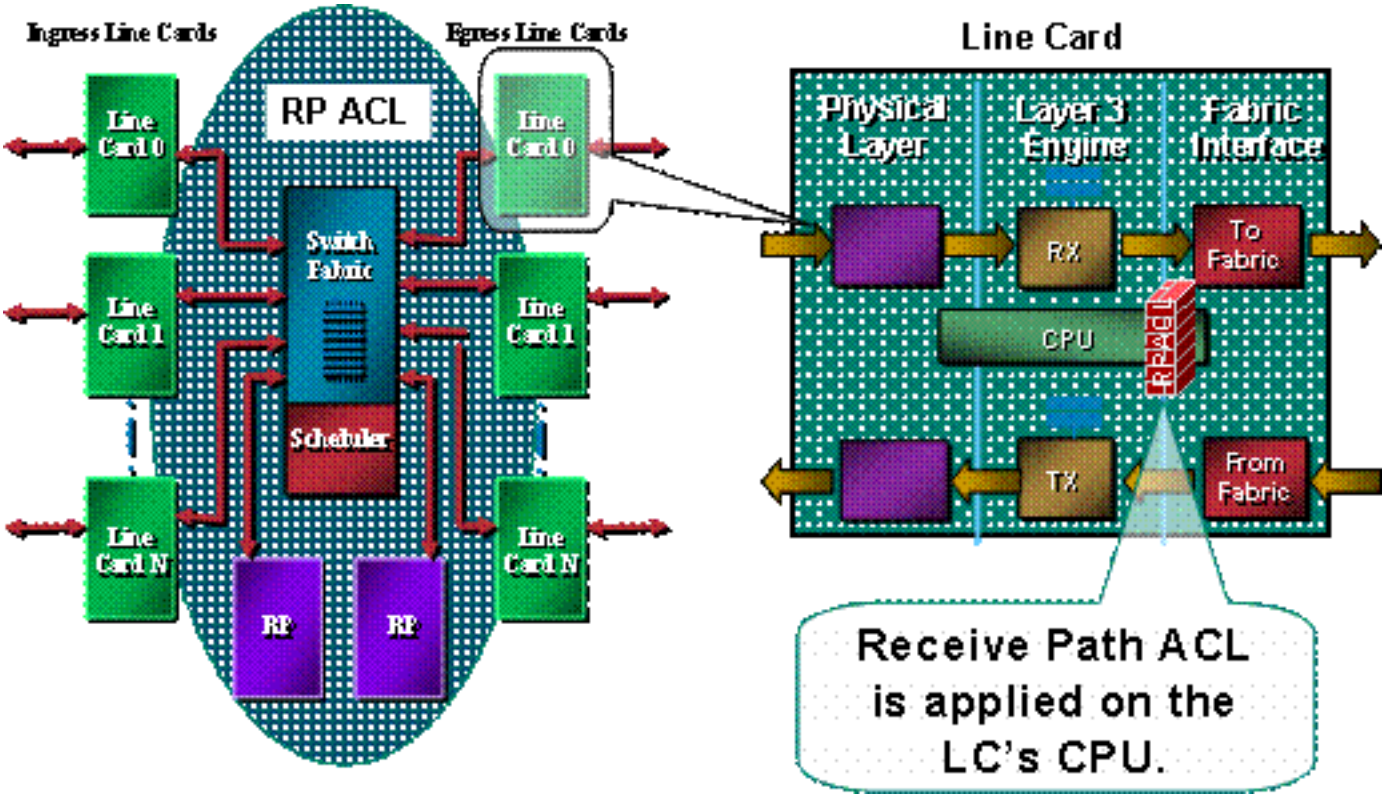
Datenverkehrstyp	Datenpfad
Normaler Datenverkehr (Transit)	LC zu Fabric zu LC
Routing-Protokolle/SSH/SNMP	LC zu LC CPU zu Fabric zu GRP
ICMP-Echo (Ping)	LC-LC-CPU
Protokollierung	

Der Routingprozessor für die GSR verfügt nur über eine begrenzte Kapazität zur Verarbeitung von Datenverkehr, der von den LCs für die GRP selbst bereitgestellt wird. Wenn für eine große Datenmenge ein Streichen auf die GRP erforderlich ist, kann dieser Datenverkehr die GRP überfordern. Dies führt zu einem effektiven Denial-of-Service (DoS)-Angriff. Die CPU der GRP kann mit der Paketprüfung nicht Schritt halten und beginnt, Pakete zu verwerfen, wodurch die Warteschlangen "Input Hold" und "Selective Packet Discard (SPD)" überflutet werden. [2] GSRs sollten vor drei Szenarien geschützt werden, die aus DoS-Angriffen auf eine GRP des Routers resultieren können.

- Paketverlust des Routing-Protokolls bei Flood mit normaler Priorität
- Management Session (Telnet, Secure Shell [SSH], SNMP) Paketverlust bei Flood mit normaler Priorität
- Paketverlust durch eine gefälschte Flut von hoher Priorität

Potenzieller Verlust von Routing-Protokolldaten während einer Flut mit normaler Priorität wird derzeit durch die statische Klassifizierung und die Ratenbeschränkung des Datenverkehrs von den LCs auf die GRP reduziert. Leider hat dieser Ansatz Einschränkungen. Die Ratenbegrenzung für normalen priorisierten Datenverkehr, der an die GRP gerichtet ist, reicht nicht aus, um den Schutz von Routing-Protokolldaten mit hoher Priorität zu gewährleisten, wenn ein Angriff über mehrere LCs erfolgt. Die Senkung des Grenzwerts, ab dem Daten mit normaler Priorität verworfen werden, um einen solchen Schutz zu gewährleisten, verschärft nur den Verlust des Managementverkehrs durch eine Flut mit normaler Priorität.

Wie dieses Bild zeigt, wird die rACL auf jedem LC ausgeführt, bevor das Paket an die GRP übertragen wird.



Ein Schutzmechanismus für die GRP ist erforderlich. rACLs wirken sich aufgrund von Empfangs-Adjacencies auf den an die GRP gesendeten Datenverkehr aus. Empfangs-Adjacencies sind Cisco Express Forwarding-Adjacencies für Datenverkehr, der an die IP-Adressen des Routers gerichtet ist, z. B. die Broadcast-Adresse oder die an den Schnittstellen des Routers konfigurierten Adressen. [3] Details zu Empfangsadjazenzen und getesteten Paketen finden Sie im Anhang.

Datenverkehr, der in einen LC eingeht, wird zuerst an die lokale CPU des LC gesendet, und Pakete, die vom GRP verarbeitet werden müssen, werden für die Weiterleitung an den Routingprozessor in die Warteschlange gestellt. Die Empfangs-ACL wird auf der GRP erstellt und dann auf die CPUs der verschiedenen LCs heruntergefahren. Bevor Datenverkehr von der LC-CPU an die GRP gesendet wird, wird der Datenverkehr mit der rACL verglichen. Wenn zulässig, wird der Datenverkehr an die GRP weitergeleitet, während der gesamte andere Datenverkehr abgelehnt wird. Die rACL wird vor der Funktion zur Ratenbegrenzung von LC zu GRP überprüft. Da die rACL für alle Empfangs-Adjacencies verwendet wird, werden auch einige Pakete, die von der LC-CPU verarbeitet werden (z. B. Echoanfragen), der rACL-Filterung unterzogen. Dies muss beim Entwerfen von rACL-Einträgen berücksichtigt werden.

Empfangszugriffskontrolllisten sind Teil eines mehrteiligen Programmbereichs von Mechanismen zum Schutz der Ressourcen in einem Router. Zukünftige Arbeiten werden eine Komponente zur Ratenbegrenzung in die rACL einschließen.

Performance-Auswirkungen

Es wird nur Speicher belegt, der für den einzelnen Konfigurationseintrag und die definierte Zugriffsliste selbst erforderlich ist. Die rACL wird auf jeden LC kopiert, sodass auf jedem LC ein leichter Speicherbereich vorhanden ist. Insgesamt sind die eingesetzten Ressourcen minimal, insbesondere im Vergleich zu den Vorteilen der Bereitstellung.

Eine Empfangs-ACL beeinträchtigt die Leistung des weitergeleiteten Datenverkehrs nicht. Die rACL gilt nur für den Empfang von Adjacency-Datenverkehr. Weitergeleiteter Datenverkehr unterliegt niemals der Zugriffskontrollliste (rACL). Der Transitverkehr wird mithilfe von

Schnittstellen-ACLs gefiltert. Diese "regulären" ACLs werden auf Schnittstellen in einer angegebenen Richtung angewendet. Der Datenverkehr wird vor der Verarbeitung von rACLs von den ACLs verarbeitet, sodass der von der ACLs der Schnittstelle abgelehnte Datenverkehr nicht von der rACL empfangen wird. [4]

Der LC, der die eigentliche Filterung durchführt (d. h. der LC, der den von der rACL gefilterten Datenverkehr empfängt), hat aufgrund der Verarbeitung der rACL eine höhere CPU-Auslastung. Diese erhöhte CPU-Auslastung ist jedoch auf ein hohes Datenverkehrsvolumen zurückzuführen, das für das GRP bestimmt ist. die Vorteile der GRP des rACL-Schutzes bei Weitem größer sind als die erhöhte CPU-Auslastung eines LC. Die CPU-Auslastung eines LCs variiert je nach LC-Modultyp. Beispielsweise kann ein LC der Engine 3 bei demselben Angriff eine niedrigere CPU-Auslastung aufweisen als ein LC der Engine 0.

Durch die Aktivierung von Turbo-ACLs (mithilfe des Befehls **access-list compiled**) werden ACLs in eine äußerst effiziente Reihe von Suchtabelleneinträgen umgewandelt. Wenn Turbo-ACLs aktiviert sind, wirkt sich die rACL-Tiefe nicht auf die Leistung aus. Die Verarbeitungsgeschwindigkeit ist also unabhängig von der Anzahl der Einträge in der ACL. Wenn die rACL kurz ist, erhöhen Turbo-ACLs die Leistung nicht signifikant, verbrauchen aber Speicher. mit kurzen rACLs sind kompilierte ACLs wahrscheinlich nicht erforderlich.

Durch den Schutz der GRP trägt die rACL dazu bei, die Stabilität von Router und Netzwerk während eines Angriffs sicherzustellen. Wie oben beschrieben, wird die rACL auf der LC-CPU verarbeitet, sodass die CPU-Auslastung auf jedem LC steigt, wenn große Datenmengen an den Router gesendet werden. Bei E0/E1- und einigen E2-Paketen kann die CPU-Auslastung von 100+ % zu Routingprotokollen und Link-Layer-Verlusten führen. Diese Verwerfen werden auf die Karte lokalisiert, und die GRP-Routingprozesse sind geschützt, sodass Stabilität gewährleistet ist. E2-Karten mit Throttling-aktiviertem Mikrocode [5] aktivieren bei starker Auslastung den Throttling-Modus und leiten Datenverkehr nur mit der Priorität 6 und 7 an das Routing-Protokoll weiter. Andere Motortypen verfügen über Multi-Queue-Architekturen. E3-Karten verfügen beispielsweise über drei Warteschlangen zur CPU, wobei Routing-Protokollpakete (Rangfolge 6/7) in einer separaten Warteschlange mit hoher Priorität enthalten sind. Hohe LC-CPU, sofern keine Pakete mit hoher Priorität dies verursachen, führt nicht zu Verlusten des Routing-Protokolls. Pakete, die in Warteschlangen mit niedrigerer Priorität enthalten sind, werden als Tail-Drop verworfen. Schließlich verfügen E4-basierte Karten über acht Warteschlangen zur CPU, von denen eine für Routing-Protokollpakete reserviert ist.

Syntax

Mit dem folgenden globalen Konfigurationsbefehl wird eine Empfangs-ACL angewendet, um die rACL an alle LCs im Router zu verteilen.

```
[no] ip receive access-list
```

In dieser Syntax **wird** ***<num>*** wie folgt definiert:

```
<1-199> IP access list (standard or extended)
<1300-2699> IP expanded access list (standard or extended)
```

Grundlegende Vorlagen und ACL-Beispiele

Um diesen Befehl verwenden zu können, müssen Sie eine Zugriffsliste definieren, die den Datenverkehr identifiziert, der mit dem Router kommunizieren darf. Die Zugriffsliste muss sowohl Routing-Protokolle als auch Verwaltungsdatenverkehr (Border Gateway Protocol [BGP], Open Shortest Path First [OSPF], SNMP, SSH, Telnet) umfassen. Weitere Informationen finden Sie im Abschnitt zu den Bereitstellungsrichtlinien.

Die folgende Beispiel-ACL bietet eine einfache Übersicht und enthält einige Konfigurationsbeispiele, die für bestimmte Verwendungszwecke angepasst werden können. Die ACL zeigt die erforderlichen Konfigurationen für mehrere häufig benötigte Services/Protokolle. Für SSH, Telnet und SNMP wird eine Loopback-Adresse als Ziel verwendet. Für die Routing-Protokolle wird die tatsächliche Schnittstellenadresse verwendet. Die Auswahl der in der rACL zu verwendenden Router-Schnittstellen hängt von den Richtlinien und Abläufen des lokalen Standorts ab. Wenn beispielsweise für alle BGP-Peering-Sitzungen Loopbacks verwendet werden, müssen in den **permit-**Anweisungen für BGP nur diese Loopbacks zugelassen werden.

```
!--- Permit BGP. access-list 110 permit tcp host bgp_peer host loopback eq bgp !--- Permit OSPF.
access-list 110 permit ospf host ospf_neighbor host 224.0.0.5 !--- Permit designated router
multicast address, if needed. access-list 110 permit ospf host ospf_neighbor host 224.0.0.6
access-list 110 permit ospf host ospf_neighbor host local_ip !--- Permit Enhanced Interior
Gateway Routing Protocol (EIGRP). access-list 110 permit eigrp host eigrp_neighbor host
224.0.0.10 access-list 110 permit eigrp host eigrp_neighbor host local_ip !--- Permit remote
access by Telnet and SSH. access-list 110 permit tcp management_addresses host loopback eq 22
access-list 110 permit tcp management_addresses host loopback eq telnet !--- Permit SNMP.
access-list 110 permit udp host NMS_stations host loopback eq snmp !--- Permit Network Time
Protocol (NTP). access-list 110 permit udp host ntp_server host loopback eq ntp !--- Router-
originated traceroute: !--- Each hop returns a message that time to live (ttl) !--- has been
exceeded (type 11, code 3); !--- the final destination returns a message that !--- the ICMP port
is unreachable (type 3, code 0). access-list 110 permit icmp any any ttl-exceeded access-list
110 permit icmp any any port-unreachable !--- Permit TACACS for router authentication. access-
list 110 permit tcp host tacacs_server router_src established !--- Permit RADIUS. access-list
110 permit udp host radius_server router_src log !--- Permit FTP for IOS upgrades. access-list
110 permit tcp host image_server eq ftp host router_ip_address access-list 110 permit tcp host
image_sever eq ftp-data host router_ip_address
```

Wie bei allen Cisco ACLs wird am Ende der Zugriffsliste eine implizite **Deny**-Anweisung ausgegeben, sodass Datenverkehr, der nicht mit einem Eintrag in der ACL übereinstimmt, abgelehnt wird.

Hinweis: Das **log-**Schlüsselwort kann verwendet werden, um Datenverkehr, der für die GRP bestimmt ist und nicht zulässig ist, zu klassifizieren. Obwohl das **log-**Schlüsselwort wertvolle Einblicke in die Details von ACL-Treffern bietet, können übermäßige Zugriffe auf einen ACL-Eintrag, der dieses Schlüsselwort verwendet, die LC-CPU-Auslastung erhöhen. Die Auswirkungen der Protokollierung auf die Leistung variieren je nach LC-Modultyp. Im Allgemeinen sollte die Protokollierung nur bei Bedarf an den Engines 0/1/2 verwendet werden. Bei den Engines 3/4/4+ führt die Protokollierung aufgrund der höheren CPU-Leistung und der Multi-Queue-Architektur zu deutlich geringeren Auswirkungen.

Die Detailgenauigkeit dieser Zugriffsliste richtet sich nach der lokalen Sicherheitsrichtlinie (z. B. der erforderlichen Filterebene für OSPF-Nachbarn).

rACLS und fragmentierte Pakete

ACLs verfügen über ein **fragments**-Schlüsselwort, das ein spezialisiertes, fragmentiertes Paketverarbeitungsverhalten ermöglicht. Im Allgemeinen werden nicht initiale Fragmente, die mit

den L3-Anweisungen übereinstimmen (unabhängig von den L4-Informationen) in einer ACL, von der **permit-** oder **deny-**Anweisung des zugeordneten Eintrags beeinflusst. Beachten Sie, dass die Verwendung des **Fragments**-Schlüsselworts ACLs zwingen kann, nicht initiale Fragmente mit höherer Genauigkeit abzulehnen oder zuzulassen.

Im rACL-Kontext fügen Filterfragmente eine zusätzliche Schutzschicht gegen DoS-Angriffe hinzu, bei denen nur nicht initiale Fragmente (wie FO > 0) verwendet werden. Die Verwendung einer **deny**-Anweisung für nicht initiale Fragmente am Anfang der rACL verhindert, dass alle nicht initialen Fragmente auf den Router zugreifen. In seltenen Fällen kann eine gültige Sitzung eine Fragmentierung erfordern und daher gefiltert werden, wenn eine **deny fragment-**Anweisung in der rACL vorhanden ist.

Betrachten Sie zum Beispiel die unten gezeigte partielle ACL.

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

Wenn diese Einträge zu Beginn einer rACL hinzugefügt werden, wird der nicht initiale Fragmentzugriff auf die GRP verweigert, während nicht fragmentierte Pakete oder initiale Fragmente an die nächsten Zeilen der rACL weitergeleitet werden, die von den **deny-Fragmentanweisungen** nicht beeinflusst werden. Der obige rACL-Ausschnitt erleichtert außerdem die Klassifizierung des Angriffs, da jedes Protokoll - Universal Datagram Protocol (UDP), TCP und ICMP - separate Zähler in der ACL erhöht.

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

Risikobewertung

Stellen Sie sicher, dass die rACL keinen kritischen Datenverkehr wie Routing-Protokolle oder interaktiven Zugriff auf die Router filtert. Die Filterung des erforderlichen Datenverkehrs kann dazu führen, dass der Remote-Zugriff auf den Router nicht möglich ist, sodass eine Konsolenverbindung erforderlich ist. Aus diesem Grund sollten Laborkonfigurationen die tatsächliche Bereitstellung so genau wie möglich nachahmen.

Wie immer empfiehlt Cisco, diese Funktion vor der Bereitstellung im Labor zu testen.

Anhänge und Notizen

Empfangen von Adjacencies und Punted-Paketen

Wie bereits zuvor in diesem Dokument beschrieben, erfordern einige Pakete eine GRP-Verarbeitung. Die Pakete werden von der Datenweiterleitungsebene zum GRP übertragen. Dies ist eine Liste der gängigen Formen von Layer-3-Daten, die GRP-Zugriff erfordern.

- Routing-Protokolle
- Multicast-Kontrolldatenverkehr (OSPF, Hot Standby Router Protocol [HSRP], Tag Distribution Protocol [TDP], Protocol Independent Multicast [PIM] usw.)

- MPLS-Pakete (Multiprotocol Label Switching), die fragmentiert werden müssen
- Pakete mit bestimmten IP-Optionen, z. B. Router-Warnmeldungen
- Erstes Paket von Multicast-Streams
- Fragmentierte ICMP-Pakete, die reassembliert werden müssen
- Gesamter Datenverkehr, der an den Router selbst gerichtet ist (mit Ausnahme des auf dem LC verarbeiteten Datenverkehrs)

Da rACLs auf Empfangsadjacencies angewendet werden, filtert die rACL einen Datenverkehr, der nicht an die GRP weitergeleitet wird, sondern eine Empfangs-Adjacency darstellt. Das häufigste Beispiel hierfür ist eine ICMP-Echoanfrage (Ping). ICMP-Echoanfragen, die an den Router gerichtet sind, werden von der LC-CPU verarbeitet. Da die Anfragen Adjacencies empfangen werden, werden sie auch durch die rACL gefiltert. Um daher Pings an die Schnittstellen (oder Loopbacks) des Routers zuzulassen, muss die rACL die Echo-Anforderungen explizit zulassen.

Empfangsadjacencies können mit dem Befehl **show ip cef** angezeigt werden.

```
12000-1#show ip cef
Prefix              Next Hop            Interface
0.0.0.0/0           drop                Null0 (default route handler entry)
1.1.1.1/32          attached            Null0
2.2.2.2/32          receive
64.0.0.0/30         attached            ATM4/3.300
...
```

Bereitstellungsrichtlinien

Cisco empfiehlt konservative Bereitstellungsverfahren. Um rACLs erfolgreich bereitstellen zu können, müssen die bestehenden Zugriffsanforderungen auf Kontroll- und Verwaltungsebene genau verstanden werden. In einigen Netzwerken kann es schwierig sein, das genaue Datenverkehrsprofil zu ermitteln, das zum Erstellen der Filterlisten erforderlich ist. Die folgenden Richtlinien beschreiben einen sehr konservativen Ansatz für die Bereitstellung von rACLs mithilfe iterativer rACL-Konfigurationen, um Datenverkehr zu identifizieren und schließlich zu filtern.

1. **Identifizieren Sie im Netzwerk verwendete Protokolle mit einer Klassifizierungs-ACL.**Stellen Sie eine rACL bereit, die alle bekannten Protokolle zulässt, die auf die GRP zugreifen. Bei dieser "Discovery"-rACL sollten Quell- und Zieladressen auf **alle** festgelegt sein. Die Protokollierung kann verwendet werden, um eine Liste von Quelladressen zu entwickeln, die den **zulässigen** Protokollanweisungen entsprechen. Zusätzlich zur Protokoll-**permit**-Anweisung kann **jede Protokoll-**Zeile am Ende der rACL verwendet werden, um andere Protokolle zu identifizieren, die von der rACL gefiltert werden und die möglicherweise Zugriff auf die GRP erfordern.Ziel ist es zu bestimmen, welche Protokolle das spezifische Netzwerk verwendet. Die Protokollierung sollte für die Analyse verwendet werden, um festzustellen, "was sonst noch 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. 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 die GRP zu filtern.**Sobald die in Schritt 1 mithilfe der rACL gefilterten Pakete identifiziert und geprüft wurden, stellen Sie eine rACL mit einer **beliebigen** Anweisung für die zulässigen Protokolle bereit. Wie in Schritt 1 kann das **log-**Schlüsselwort weitere Informationen zu Paketen

bereitstellen, die den **permit-**Einträgen entsprechen. Wenn Sie **ein Protokoll** am Ende **ablehnen**, können Sie unerwartete Pakete identifizieren, die für die GRP bestimmt sind. Diese rACL bietet grundlegenden Schutz und ermöglicht es Netzwerktechnikern, sicherzustellen, dass der gesamte erforderliche Datenverkehr zulässig ist.Das Ziel besteht darin, den Bereich der Protokolle zu testen, die mit dem Router kommunizieren müssen, ohne über den expliziten Bereich der IP-Quell- und -Zieladressen zu verfügen.

3. **Beschränken Sie einen Makrobereich von Quelladressen.**Lassen Sie nur zu, dass der gesamte Bereich Ihres CIDR-Blocks (Associated Classless Interdomain Routing) als Quelladresse zulässig ist. Wenn Sie beispielsweise 171.68.0.0/16 für Ihr Netzwerk zugewiesen haben, lassen Sie Quelladressen von nur 171.68.0.0/16 zu.Mit diesem Schritt wird das Risiko verringert, ohne dass Services unterbrochen werden. Es stellt auch Datenpunkte von Geräten/Personen außerhalb Ihres CIDR-Blocks bereit, die möglicherweise auf Ihre Geräte zugreifen. Alle externen Adressen werden gelöscht.Externe BGP-Peers erfordern eine Ausnahme, da die zulässigen Quelladressen für die Sitzung außerhalb des CIDR-Blocks liegen.Diese Phase kann einige Tage lang fortgesetzt werden, um Daten für die nächste Phase der Eingrenzung der rACL zu sammeln.
4. **Schränken Sie die Anweisungen zur rACL-Zulassung so ein, dass nur bekannte autorisierte Quelladressen zugelassen werden.**Zunehmend begrenzen Sie die Quelladresse, um nur Quellen zuzulassen, die mit der GRP kommunizieren.
5. **Begrenzen Sie die Zieladressen auf der rACL. (*optional*)**Einige Internet-Service-Provider (ISP) dürfen nur bestimmten Protokollen gestatten, bestimmte Zieladressen auf dem Router zu verwenden. Diese letzte Phase soll den Bereich der Zieladressen begrenzen, die Datenverkehr für ein Protokoll akzeptieren. [6]

Bereitstellungsbeispiel

Das nachfolgende Beispiel zeigt eine Empfangs-ACL zum Schutz eines Routers, der auf der folgenden Adressierung basiert.

- Der Adressblock des ISP lautet 169.223.0.0/16.
- Der Infrastrukturblock des ISP lautet 169.223.252.0/22.
- Das Loopback für den Router lautet 169.223.253.1/32.
- Da der Router ein Core-Backbone-Router ist, sind nur interne BGP-Sitzungen aktiv.

Angesichts dieser Informationen könnte die erste empfangene ACL etwa wie im Beispiel unten aussehen. Da wir den Infrastruktur-Adressblock kennen, wird zunächst der gesamte Block zugelassen. Später werden detailliertere Zugriffskontrolleinträge (ACEs) hinzugefügt, wenn die spezifischen Adressen für alle Geräte abgerufen werden, die Zugriff auf den Router benötigen.

```
!
no access-list 110
!
!--- This ACL is an explicit permit ACL. !--- The only traffic permitted will be packets that !-
-- match an explicit permit ACE.

!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 - Explicit Permit !--- Permit only applications whose destination address !--- is
the loopback and whose source addresses !--- come from an valid host.

!
```

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

!
!--- Permit BGP. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq bgp
! !--- Permit OSPF. ! access-list 110 permit ospf 169.223.252.0 0.0.3.255 host 224.0.0.5 ! !---
Permit designated router multicast address, if needed. ! access-list 110 permit ospf
169.223.252.0 0.0.3.255 host 224.0.0.6 access-list 110 permit ospf 169.223.252.0 0.0.3.255 host
169.223.253.1 ! !--- Permit EIGRP. ! access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host
224.0.0.10 access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host 169.223.253.1 ! !--- Permit
remote access by Telnet and SSH. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255 host
169.223.253.1 eq 22 access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq
telnet ! !--- Permit SNMP. ! access-list 110 permit udp 169.223.252.0 0.0.3.255 host
169.223.253.1 eq snmp ! !--- Permit NTP. ! access-list 110 permit udp 169.223.252.0 0.0.3.255
host 169.223.253.1 eq ntp ! !--- Router-originated traceroute: !--- Each hop returns a message
that ttl !--- has been exceeded (type 11, code 3); !--- the final destination returns a message
that !--- the ICMP port is unreachable (type 3, code 0). ! access-list 110 permit icmp any
169.223.253.1 ttl-exceeded access-list 110 permit icmp any 169.223.253.1 port-unreachable ! !---
Permit TACACS for router authentication. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255
host 169.223.253.1 established ! !--- Permit RADIUS. ! ! access-list 110 permit udp
169.223.252.0 0.0.3.255 169.223.253.1 log ! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !---
Phase 2 - Explicit Deny and Reaction !--- Add ACEs to stop and track specific packet types !---
that are destined for the router. This is the phase !--- where you use ACEs with counters to
track and classify attacks.

!
!--- SQL WORM Example - Watch the rate of this worm. !--- Deny traffic destined to UDP ports
1434 and 1433. !--- from being sent to the GRP. This is the SQL worm. ! access-list 110 deny udp
any any eq 1433 access-list 110 deny udp any any eq 1434 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 - Explicit Denies for
Tracking !--- Deny all other traffic, but count it for tracking.

!
access-list 110 deny udp any any
access-list 110 deny tcp any any range 0 65535
access-list 110 deny ip any any
```

Hinweise

1. Informationen zur Erhöhung der DoS-Resistenz finden Sie unter Understanding Selective Packet Discard (SPD) SPD and Hold Queue Guidelines.
2. Weitere Informationen zu Cisco Express Forwarding und Adjacencies finden Sie unter Übersicht über Cisco Express Forwarding.
3. Eine detaillierte Beschreibung der ACL-Bereitstellungsrichtlinien und der zugehörigen Befehle finden Sie unter Implementieren von ACLs auf Cisco Internet Routern der Serie 12000.
4. Dies bezieht sich auf Pakete mit Vanilla, Border Gateway Protocol Policy Accounting (BGPPA), Per Interface Rate Control (PIRC) und Frame Relay Traffic Policing (FRTP).
5. Phase II des Empfangspfad-Schutzes ermöglicht die Erstellung einer Verwaltungsschnittstelle und begrenzt automatisch, welche IP-Adresse eingehende Pakete abhört.

Zugehörige Informationen

- Support-Seite für Zugriffslisten
- Technischer Support - Cisco Systems